CISM Review Manual 2006

Information Systems
Audit and Control
Association®

Information Systems Audit and Control Association®

With more than 50,000 members in more than 140 countries, the Information Systems Audit and Control Association® (ISACA®) (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 44,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 5,500 professionals in its first two years.

Disclaimer

ISACA has produced this publication as an educational resource to assist individuals preparing to take the CISM certification exam. It was produced independently from the CISM Certification Board, which has had no input into or responsibility for its content. Copies of past examinations are not released to the public and are not made available to ISACA for preparation of this publication. ISACA makes no representations or warranties whatsoever with regard to these or other ISACA/ITGI publications assuring candidates' passage of the CISM examination.

Disclosure

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Web site: *www.isaca.org*

ISBN 1-933284-38-2
2006 CISM Review Manual
Printed in the United States of America

Foreword

The Information Systems Audit and Control Association is pleased to offer this third edition of the *CISM Review Manual*. The purpose of this manual is to provide CISM candidates with updated technical information and references to assist in preparation and study for the Certified Information Security Manager examination. Please note that the manual has been written using standard American English.

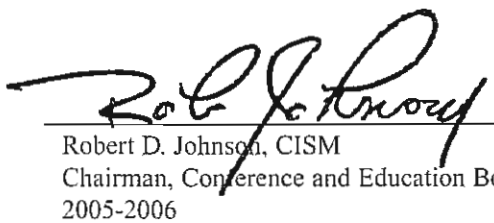
The *CISM Review Manual* will be updated annually to keep pace with the rapid changes in the management, design, oversight and assessment of information security. As such, your comments and suggestions regarding this manual are welcome. A feedback questionnaire is included at the back of the manual. After the examination is over, please take a moment to complete and return the questionnaire to ISACA. Your observations are extremely valuable for the preparation of the 2007 edition.

No representations or warranties are made by ISACA in regard to these or other association/IT Governance Institute® (ITGI) publications assuring candidates' passage of the CISM examination. This publication was produced independently from the CISM Certification Board, which has no responsibility for its content.

Copies of examinations will not be released to the public. The sample questions contained in this manual are designed to depict the type of question format typically found on the CISM examination.

Certification has provided a positive effect on many careers. CISM is designed to provide executive management with assurance that those earning the designation have the required knowledge and ability to provide effective information security management and consulting. While its central focus is information security management, all those in the IT profession with security experience will certainly find value in CISM. We wish you success with the CISM examination.

Everett C. Johnson Jr.
International President
2005-2006



Robert D. Johnson, CISM
Chairman, Conference and Education Board
2005-2006

Acknowledgments

The Information Systems Audit and Control Association wishes to recognize:

The technical content project leaders

Eugene Schultz, Ph.D., CISM, CISSP
Chief Technology Officer
High Tower Software

Krag Brotby, CISM
Senior Security Consultant

The reviewers

Rogelio Aguilar Alamilla
Mexico City Chapter, Mexico

Christopher Chukwuemeka Anoruo, CISM
Vee Networks Limited (Vmobile Nigeria)
Lagos Chapter, Nigeria

Evelyn Susana Anton, CISA, CISM
UTE
Montevideo Chapter, Uruguay

Osman Abdel Halim Azab, CISA, CISM
Arab African International Bank
Egypt (chapter in formation)

Sunil Bhaskar Bakshi, CISA, CISM
State Bank of India
Pune Chapter, India

Jennifer Bayuk, CISA, CISM
Bear Stearns & Co. Inc.
New Jersey Chapter, USA

Juan de Dios Bel, CISA, CISM
AzimuT, Ltd.
Buenos Aires Chapter, Argentina

Mark Edward Stirling Bernard, CISM
EDS Advanced Solutions
Ottawa Chapter, Canada

Endre Paul Bihari, CISM
Performance Resources
Melbourne Chapter, Australia

Ulises Castillo Hernández, CISA, CISM
SCITUM, S.A. de C.V.
Mexico City Chapter, Mexico

Milthon Chávez
MCH Consultoria Integral, CA
Caracas Chapter, Venezuela

Richard Hon-Mon Chew, CISM
Los Angeles Chapter, USA

Mark T. Edmead, CISA
MTE Software Inc.
San Diego Chapter, USA

Jesús Leonardo García Rojas, CISM
Innovaciones Telemáticas, S.A. de C.V.
Mexico City Chapter, Mexico

Adam Geller, CISM
New York Metro Chapter, USA

Venugopal R. Iyengar, CISA, CISM
Tata Consultancy Services
Mumbai Chapter, India

Avinash W. Kadam, CISA, CISM
MIEL e-Security Pvt., Ltd.
Mumbai Chapter, India

Srinivasan S. Krishnaswamy, CISA, CISM
Bangalore Chapter, India

Charles Koerwer, CISM
CIGNA
Philadelphia Chapter, USA

María Cristina Ledesma, CISA, CISM
Citibank NA Sucursal Uruguay
Montevideo Chapter, Uruguay

Joe W. Livingston, CISM
Roundy's Supermarkets Inc.
Kettle Morraine Chapter, USA

James W.S. Ludwig, CISM
Anacomp Inc.
San Diego Chapter, USA

Dr. Orillo Narduzzo, CISA, CISM
SEC Servizi ScPA
Milano Chapter, Italy

Joseph Ponnoly, CISA, CISM
Nationwide Financial
Central Ohio Chapter, USA

Vernon Richard Poole, CISM
Sapphire Technologies Ltd.
Northern England Chapter, UK

Delphine Pramotton, CISA, CISM
Ernst & Young Toulouse
Paris Chapter, France

Marc Sel, CISA, CISM
PricewaterhouseCoopers
Belux Chapter, Belgium

Barbara Soldano, CISM
NYS Office for Technology
New York Metro Chapter, USA

Marcel Paul Sorouni, CISA, CISM
Deloitte & Touche Tohmatsu
Sydney Chapter, Australia

Jason L. Stradley, CISM
Corn Products International Inc.
Chicago Chapter, USA

Allen E. Stokes, CISA, CISM
Tennessee Valley Authority
USA

Marguerite E. Surat, CISA,CISM
EDS
Phoenix Chapter, USA

Bhavani Suresh, CISA, CISM
Adnoc Distribution
UAE Chapter, United Arab Emirates

Jason B. Taule, CISM
ViPS
Central Maryland Chapter, USA

Ghassan Toufik Youssef, CISM
Banque Audi, SAL
Lebanon Chapter, Lebanon

Raymond Tee Meng Wee, CISA, CISM
Senyum International
Singapore Chapter, Singapore

Bruce R. Wilkins, CISA, CISM
TWM Associates Inc.
National Capital Chapter, USA

CISM®
CERTIFIED INFORMATION SECURITY MANAGER®

Table of Contents

ORGANIZATION xi

CHAPTER 1: INFORMATION SECURITY GOVERNANCE 1
1.1 Definition 1
1.2. Objectives 1
1.3. Tasks 1
1.3.1 Knowledge Statements 2
1.3.2 Relationship of Tasks to Knowledge Statements 2
1.4 Information Security Governance Overview 4
1.4.1 Importance of Information Security Governance 6
1.4.2 Outcomes of Security Governance 7
1.5 Effective Information Security Governance 7
1.5.1 Roles and Responsibilities of Senior Management and Boards of Directors 8
1.5.2 Matrix of Outcomes and Responsibilities 9
1.6 Information Security Concepts 10
1.7 Information Security Manager 10
1.7.1 Responsibilities 10
1.7.2 Senior Management Commitment 11
1.8 Scope and Charter of Information Security Governance 12
1.8.1 Convergence 12
1.9 Information Security Governance Metrics 12
1.9.1 Strategic Alignment 13
1.9.2 Risk Management 13
1.9.3 Business Process Assurance 14
1.9.4 Value Delivery 14
1.9.5 Resource Management 14
1.9.6 Performance Measurement 14
1.10 Defining an Information Security Strategy 15
1.10.1 An Alternate View of Strategy 15
1.11 Challenges in Developing an Information Security Strategy 16
1.11.1 Common Pitfalls 16
1.12 Information Security Strategy Objectives 17
1.12.1 The Goal 17
1.12.2 Defining Objectives 18
1.12.3 The Desired State 20
1.12.4 Risk Objectives 23
1.13 Determining Current State of Security 24
1.13.1 Current Risk 24
1.14 Developing an Information Security Strategy 24
1.14.1 Elements of a Strategy 25
1.14.2 Strategy Resources and Constraints 25

1.15 Strategy Resources 26
1.15.1 Policies and Standards 26
1.15.2 Architecture 27
1.15.3 Controls 28
1.15.4 Countermeasures 30
1.15.5 Technologies 30
1.15.6 Personnel 30
1.15.7 Roles and Responsibilities 31
1.15.8 Skills 31
1.15.9 Awareness and Education 31
1.15.10 Audits 33
1.15.11 Compliance Enforcement 33
1.15.12 Threat Analysis 33
1.15.13 Vulnerability Analysis 33
1.15.14 Risk Assessment 34
1.15.15 Business Impact Assessment 34
1.15.16 Resource Dependency Analysis 34
1.15.17 Outsourced Security Providers 34
1.15.18 Other Organizational Support and Assurance Providers 35
1.16 Strategy Contraints 35
1.16.1 Legal and Regulatory Requirements 35
1.16.2 Physical and Environmental Factors 36
1.16.3 Ethics 36
1.16.4 Culture/Regional Variances 36
1.16.5 Costs 36
1.16.6 Personnel 37
1.16.7 Resources 37
1.16.8 Capabilities 37
1.16.9 Time 37
1.16.10 Risk Tolerance 37
1.17 Implementing Information Security Governance 37
1.17.1 Gap Analysis—Basis for an Action Plan 37
1.17.2 Policy Development 38
1.17.3 Standards Development 39
1.17.4 Training and Awareness 39
1.17.5 Action Plan Metrics 39
1.18 Intermediate Implementation Goals 40
1.19 Information Security Program Objectives 40
1.20 Chapter 1 Glossary 42
1.21 Chapter 1 Sample Questions 45
1.22 Chapter 1 Answers to Sample Questions 47
1.23 Chapter 1 References 48

CISM®
CERTIFIED INFORMATION SECURITY MANAGER®

CHAPTER 2: RISK MANAGEMENT 51
2.1 Definition 51
2.2 Objective 51
2.3 Tasks 51
2.3.1 Knowledge Statements 51
2.3.2 Relationship of Tasks to Knowledge Statements 52
2.4 Risk Management Overview 53
2.4.1 The Importance of Risk Management 55
2.4.2 Outcomes of Risk Management 55
2.5 Effective Information Security Risk Management 55
2.5.1 Roles and Responsibilities 56
2.6 Information Security Risk Management Concepts 56
2.6.1 Concepts 56
2.6.2 Technologies 57
2.7 Implementing Risk Management 57
2.7.1 Risk Management Process 58
2.7.2 Threats 60
2.7.3 Vulnerabilities 60
2.7.4 Risks 61
2.7.5 Impact 64
2.7.6 Controls and Countermeasures 64
2.7.7 Information Resource Valuation 65
2.7.8 Information Asset Classification 66
2.7.9 Recovery Time Objectives 68
2.7 10 Third-party Service Providers 68
2.7.11 Integration Into Life Cycle Processes 69
2.7.12 Baselines 70
2.7.13 Monitoring and Communication 71
2.7.14 Documentation 71
2.8 Chapter 2 Glossary 73
2.9 Chapter 2 Sample Questions 75
2.10 Chapter 2 Answers to Sample Questions 77
2.11 Chapter 2 References 78

CHAPTER 3: INFORMATION SECURITY PROGRAM(ME) MANAGEMENT 81
3.1 Definition 81
3.2 Objective 81
3.3 Tasks 81
3.3.1 Knowledge Statements 81
3.3.2 Relationship of Tasks to Knowledge Statements 82
3.4 Information Security Program Management Overview 84
3.4.1 Importance of Information Security Program Management 84
3.4.2 Outcomes of Information Security Program Management 84
3.4.3 Key Elements 85
3.4.4 Summary of Tasks 86

CISM
CERTIFIED INFORMATION SECURITY MANAGER®

3.5 Planning 87
3.5.1 Creating and Maintaining Plans 87
3.5.2 Methods to Develop an Implementation Plan 87
3.5.3 Project Management Methods and Techniques 87
3.5.4 Budgets 88
3.5.5 Scheduling 89
3.6 Security Baselines 89
3.6.1 Developing Information Security Baselines 89
3.6.2 Security Baselines and Configuration Management 90
3.7 Business Processes 90
3.7.1 Ensuring Business Processes Address Information Security Risk 90
3.7.2 Security Procedures and Guidelines 91
3.8 Infrastructure 91
3.8.1 IT Infrastructure Activities to Ensure Compliance With Information Security Policies 91
3.8.2 Information Security Architectures 92
3.8.3 Information Security Technologies 92
3.8.4 Key Concepts for Architecture and Technologies 92
3.8.5 Firewalls 106
3.8.6 Intrusion Detection Systems 108
3.8.7 Encryption 109
3.8.8 Malicious Code (Malware) 114
3.9 Life Cycles 116
3.9.1 Integrating Information Security Program Requirements 116
3.9.2 Systems Development Life Cycle Methodologies 117
3.9.3 Compliance With the Information Security Governance Framework 118
3.10 Impact on End Users 118
3.10.1 Meeting Information Security Policy Requirements and Recognizing the Impact on End Users 118
3.10.2 Planning, Conducting, Reporting and Following Up on Security Testing 119
3.10.3 Physical, Administrative and Technical Controls 119
3.11 Accountability 119
3.11.1 Promoting Accountability in Managing Information Security Risks 119
3.11.2 Integrate Security Program Into the Enterprise 120
3.11.3 Integrating Information Security Requirements Into the Business Processes 121
3.12 Security Metrics 121
3.12.1 Establishing Metrics to Manage the Security Program 121
3.12.2 Security Metrics Design, Development and Implementation 121
3.13 Managing Internal and External Resources 122
3.13.1 Identify, Appropriate and Manage Information Security Resources 122
3.13.2 Acquisition Management Methods and Techniques 122
3.14 Chapter 3 Glossary 123
3.15 Chapter 3 Sample Questions 134
3.16 Chapter 3 Answers to Sample Questions 139
3.17 Chapter 3 References 142

CHAPTER 4: INFORMATION SECURITY MANAGEMENT 149
4.1 Definition 149
4.2 Objective 149
4.3 Tasks 149
4.3.1 Knowledge Statements 149
4.3.2 Relationship of Tasks to Knowledge Statements 150
4.4 Information Security Management Overview 151
4.4.1 Management Commitment 152
4.4.2 IT Security and Information Security 152
4.4.3 The Importance of Information Security Management 152
4.4.4 Outcomes of Information Security Management 153
4.5 Effective Information Security Management 153
4.5.1 Scope of Responsibilities 153
4.5.2 Roles and Responsibilities 154
4.6 Information Security Management Concepts 154
4.6.1 Concepts 154
4.6.2 Technologies 155
4.7 Implementing Information Security Management 156
4.7.1 Integrating Assurance Activities 156
4.7.2 Controls 157
4.7.3 Security Policies 159
4.7.4 General Rules of Use/Acceptable Use Policy 159
4.7.5 Security Standards 159
4.7.6 Security Procedures 160
4.7.7 Assignment of Roles and Responsibilities 161
4.7.8 Trading Partners and Security Providers 162
4.7.9 Security Metrics and Monitoring 162
4.7.10 The Change Management Process 164
4.7.11 Vulnerability Assessments 165
4.7.12 Due Diligence 166
4.7.13 Resolution of Noncompliance Issues 167
4.7.14 Culture, Behavior and Security Awareness 168
4.8 Chapter 4 Glossary 171
4.9 Chapter 4 Sample Questions 175
4.10 Chapter 4 Answers to Sample Questions 177
4.11 Chapter 4 References 178

CHAPTER 5: RESPONSE MANAGEMENT 181
5.1 Definition 181
5.2 Objective 181
5.3 Tasks 181
5.3.1 Knowledge Statements 181
5.3.2 Relationship of Tasks and Knowledge Statements 182
5.4 Introduction to Response Management 182
5.4.1 Response Management Overview 182
5.4.2 Importance of Response Management 183

CISM®
CERTIFIED INFORMATION SECURITY MANAGER®

5.4.3 Outcomes of Response Management 184
5.4.4 Key Elements 184
5.5 Performing a Business Impact Analysis 184
5.5.1 Definition of BIA 184
5.5.2 Elements of BIAs 185
5.5.3 Benefits of Conducting BIAs 185
5.6 Developing Response and Recovery Plans 186
5.6.1 Organizing, Training and Equipping the Response Staff 186
5.6.2 Recovery Planning and Business Recovery Processes 186
5.6.3 Understand Response and Recovery Practices 194
5.7 Incident Response Processes 194
5.7.1 Detecting, Identifying and Analyzing Security-related Events 194
5.7.2 Components of an Incident Response Capability 195
5.8 Testing Response and Recovery Plans 196
5.8.1 Periodic Testing of the Response and Recovery Plans 196
5.8.2 Testing for Infrastructure and Critical Business Applications 196
5.9 Executing Response and Recovery Plans 198
5.9.1 Ensuring the Execution as Required 198
5.9.2 Escalation Process for Effective Security Management 199
5.9.3 Intrusion Detection Policies and Processes 200
5.9.4 Help Desk Processes for Identifying Security Incidents 201
5.9.5 The Notification Process 201
5.10 Documenting Events 201
5.10.1 Establishing Procedures 201
5.10.2 Requirements for Evidence 202
5.11 Postevent Reviews 202
5.11.1 Identifying Causes and Corrective Actions 202
5.11.2 Postincident Reviews and Follow-up Procedures 203
5.12 Chapter 5 Glossary 204
5.13 Chapter 5 Sample Questions 212
5.14 Chapter 5 Answers to Sample Questions 215
5.15 Chapter 5 Reference 217

GENERAL INFORMATION 219

Organization

The 2006 CISM Review Manual is divided into five chapters covering the CISM content areas:

1. **Information Security Governance**
2. **Risk Management**
3. **Information Security Program(me) Management**
4. **Information Security Management**
5. **Incident Response Management**

The manual is organized by major topics with reference to the relevant task and knowledge statements.


CISM
CERTIFIED INFORMATION
SECURITY MANAGER®

Chapter 1:

INFORMATION SECURITY GOVERNANCE

1.1 DEFINITION

The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly

1.2 OBJECTIVES

The objective of this job practice area is to ensure that the information security manager (ISM) understands the broad requirements for effective information security governance, the elements and actions required to develop an information security strategy and a plan of action to implement it.

An extension of the governance definition will include the "structure through which the objectives of the enterprise are set, and the means of attaining those objectives and monitoring performance are determined."[1] Structure and means will include strategy; policies and their corresponding standards, procedures and guidelines; strategic and operational plans; awareness and training; risk management; controls; and audits and other assurance activities.

The *2006 CISM Review Manual* is written from a practical perspective required for the implementation of effective governance with focus on the CISM function. Information security governance is just beginning to get the attention of organizational leaders and it may well fall to the ISM to play a critical role in many aspects of achieving good information security governance. With this consideration, information security governance is covered extensively in this chapter.

Governance is not presented from a purely theoretical perspective, but rather from an implementation viewpoint. As a result, elements of management will be included in the governance section when it serves to illuminate understanding of implementation requirements. Information security management functions are covered in detail in chapter 4.

This job practice area represents **21** percent percent of the CISM examination (approximately **42** questions).

1.3 TASKS

There are eight (8) tasks within this job practice area that a CISM candidate must know how to do:
1) Develop the information security strategy in support of business strategy and direction.
2) Obtain senior management commitment and support for information security throughout the enterprise.
3) Ensure that definitions of roles and responsibilities throughout the enterprise include information security governance activities.
4) Establish reporting and communication channels that support information security governance activities.
5) Identify current and potential legal and regulatory issues affecting information security and assess their impact on the enterprise.
6) Establish and maintain comprehensive information security policies that support business goals and objectives.
7) Develop standards to govern procedures and guidelines that support information security policies.
8) Develop business case and enterprise value analysis that supports information security program investments.

[1] Organisation for Economic Co-operation and Development, "OECD Principles of Corporate Governance," 1999, *www.ecgi.org/codes/country_documents/oecd/principles_en.pdf.* Organisation for Economic Co-operation and Development "OECD Principles of Corporate Governance: 2004," 2004, *www.oecd.org/document/49/0,2340,en_2649_34813_31530865_1_1_1_1,00.html*

1.3.1 Knowledge Statements

The CISM candidate must have a good understanding of each of the 20 areas delineated by the knowledge statements. These statements are the basis for the examination:

1) Knowledge of information security concepts
2) Knowledge of the relationship between information security and business operations
3) Knowledge of techniques used to secure senior management commitment and support of information security management
4) Knowledge of methods of integrating information security governance into the overall enterprise governance framework
5) Knowledge of practices associated with an overall policy directive that capture senior management-level direction and expectations for information security in laying the foundation for information security management within an organization
6) Knowledge of an information security steering group function
7) Knowledge of information security management roles, responsibilities and organizational structure
8) Knowledge of areas of governance (e.g., risk management, data classification management, network security, system access)
9) Knowledge of centralized and decentralized approaches to coordinating information security
10) Knowledge of legal and regulatory issues associated with Internet businesses, global transmissions and transborder data flows (e.g., privacy, tax laws and tariffs, data import/export restrictions, restrictions on cryptography, warranties, patents, copyrights, trade secrets, national security)
11) Knowledge of common insurance policies and imposed conditions (e.g., crime or fidelity insurance, business interruptions)
12) Knowledge of the requirements for the content and retention of business records and compliance
13) Knowledge of the process for linking policies to enterprise business objectives
14) Knowledge of the function and content of essential elements of an information security program (e.g., policy statements, procedures, guidelines)
15) Knowledge of techniques for developing an information security process improvement model for sustainable and repeatable information security policies and procedures
16) Knowledge of information security process improvement and its relationship to traditional process management
17) Knowledge of information security process improvement and its relationship to security architecture development and modeling
18) Knowledge of information security process improvement and its relationship to security infrastructure
19) Knowledge of generally accepted international standards for information security management and related process improvement models
20) Knowledge of the key components of cost-benefit analysis and enterprise transformation/migration plans (e.g., architectural alignment, organizational positioning, change management, benchmarking, market/competitive analysis)
21) Knowledge of methodology for business case development and computing enterprise value proposition

1.3.2 Relationship of Tasks to Knowledge Statements

The task statements reflect what the CISM candidate is expected to know how to do. The knowledge statements delineate what the CISM candidate is expected to know to perform the tasks.

The task and knowledge statements are approximately mapped in the table below insofar as it is possible to do so. Note that there is often overlap. Each task statement will generally map to several knowledge statements as shown in **figure 1.1**.

Figure 1.1—Knowledge and Task Statements Mapping	
Task Statements	**Knowledge Statements**
1. Develop the information security strategy in support of business strategy and direction.	1. Knowledge of information security concepts 2. Knowledge of the relationship between information security and business operations 3. Knowledge of techniques used to secure senior management commitment and support of information security management 4. Knowledge of methods of integrating information security governance into the overall enterprise governance framework 8. Knowledge of areas of governance 13. Knowledge of the processes for linking policies to enterprise business objectives 14. Knowledge of the function and content of essential elements of an information security program
2. Obtain senior management commitment and support for information security throughout enterprise.	2. Knowledge of the relationship between information the security and business operations 3. Knowledge of techniques used to secure senior management commitment and support of information security management 4. Knowledge of methods of integrating information security governance into the overall enterprise governance framework 13. Knowledge of the processes for linking policies to enterprise business objectives
3. Ensure that definitions of roles and responsibilities throughout the enterprise include information security governance activities.	4. Knowledge of methods of integrating information security governance into the overall enterprise governance framework 5. Knowledge of practices associated with an overall policy directive that captures senior management level direction and expectations for information security in laying the foundation for information security management within an organization 7. Knowledge of information security management roles, responsibilities and organizational structure 9. Knowledge of centralized and decentralized approaches to coordinating information security
4. Establish reporting and communication channels that support information security governance activities.	2. Knowledge of the relationship between information security and business operations 13. Knowledge of the processes for linking policies to enterprise business objectives 20. Knowledge of the key components of cost benefit analysis and enterprise transformation/migration plans 21. Knowledge of methodology for business case development and computing enterprise value proposition
5. Identify current and potential legal and regulatory issues affecting information security and assess their impact on the enterprise.	10. Knowledge of legal and regulatory issues associated with Internet business, global transmissions and transborder data flows 12. Knowledge of the requirements for the content and retention of business records and compliance

Figure 1.1—Knowledge and Task Statements Mapping (*cont.*)	
Task Statements	**Knowledge Statements**
6. Establish and maintain information security policies that support business goals and objectives.	1. Knowledge of information security concepts 2. Knowledge of the relationship between information security and business operations 4. Knowledge of methods of integrating information security governance into the overall enterprise governance framework 5. Knowledge of practices associated with an overall policy directive that captures senior management level direction and expectations for information security in laying the foundation for information security management within an organization 14. Knowledge of the function and content of essential elements of an information security program 15. Knowledge of techniques for developing an information security process improvement model for sustainable and repeatable information security policies and procedures
7. Ensure the development of procedures and guidelines that support information security policies.	1. Knowledge of information security concepts 2. Knowledge of the relationship between information security and business operations 4. Knowledge of methods of integrating information security governance into the overall enterprise governance framework 5. Knowledge of practices associated with an overall policy directive that captures senior management level direction and expectations for information security in laying the foundation for information security management within an organization 14. Knowledge of the function and content of essential elements of an information security program 15. Knowledge of techniques for developing an information security process improvement model for sustainable and repeatable information security policies and procedures
8. Develop business case and enterprise value analysis that support information security program investments.	2. Knowledge of the relationship between information security and business operations 10. Knowledge of legal and regulatory issues associated with Internet business, global transmissions and transborder data flows 20. Knowledge of key components of cost benefit analysis and enterprise transformation./ migration plans 21. Knowledge of methodology for business case development and computing enterprise value proposition

1.4 INFORMATION SECURITY GOVERNANCE OVERVIEW

Information can be defined as "data endowed with meaning and purpose." Today, it plays an increasingly important role in all aspects of our lives. Information has become an indispensable component of conducting business for virtually all organizations. In a growing number of companies, information is the business. This includes major players of the emerging knowledge society such as Google, eBay, Microsoft and countless others large and small. Some might not think of software as information, but it is simply information for computers on how to operate or process something.

Traditional organizations have undergone radical transformations in the "information age" as well. The graphic arts and printing industry, for example, today deal almost entirely with information in digital form. Artwork and masters are no longer physical drawings or pieces of film but blocks of information stored on hard disks.

It would be difficult to find a business that has not been touched by information technology and dependent on the information it processes. Information systems have become pervasive in global society and business, and the dependence on these systems and the information they handle is arguably absolute.

The increasing dependency on information was apparent over a decade ago when Peter Drucker stated, "The diffusion of technology and the commodification of information transforms the role of information into a resource equal in importance to the traditionally important resources of land, labor and capital."[2]

During the intervening 12 years, the trend of escalating value of, and dependence on, information has increased exponentially. There is every indication that this quickening pace will continue unabated into the foreseeable future. Gartner recently estimated that in less than a decade, organizations will typically deal with 30 times more information than they do today. Yet, with the chaos, glaring vulnerabilities and perpetual crisis-mode activities observed in most information technology operations, that is not a reassuring notion.

During the same 12-year period, information crime and vandalism have become the choice of a growing cadre of prudent crooks. Terrorists and others with enmity toward society have brazenly embraced the very information technology they claim to despise to herald their view and advertise their horrid acts.

Approximately 80 percent of critical infrastructures in the developed world are controlled by the private sector. Coupled with often ineffective bureaucracies, countless conflicting jurisdictions and aging institutions unable to adapt to dealing with burgeoning global "information" crime, a preponderance of the task of protecting the information resources critical to survival falls squarely on corporate shoulders.

To accomplish the task of adequate protection for information resources, the issue must be raised to a board-level activity as are other critical governance functions. The complexity, relevance and criticality of information security and its governance mandate that it be addressed and supported at the highest organizational levels.

Increasingly, those that understand the scope and depth of risks to information take the position that, as a critical resource, information must be treated with the same care, caution and prudence that any other asset essential to the survival of the organization and perhaps society itself would receive.

Until recently, the focus of protection has been on the IT systems that process and store the vast majority of information rather than the information itself. But this approach is too narrow to accomplish the level of integration, process assurance and overall security that is now required. Information security takes the larger view that the content, information and the knowledge based on it, must be adequately protected regardless of how it is handled, processed, transported or stored.

IT security addresses the security of the technology and is typically driven from the CIO level. Information security addresses the universe of risks, benefits and processes involved with information and must be driven by executive management and supported by the board of directors.

The relentless advance of information technology and the unparalleled ability to access, manipulate and use information has brought enormous benefits and opportunities to the global economy. It has also brought unparalleled new risks and a confounding patchwork of existing and pending laws and regulations.

Executive management is increasingly confronted by the need to stay competitive in the global economy and heed the promise of greater gains from the deployment of more information resources. But even as organizations reap those gains, the twin specters of increasing dependence on information and the systems that support it and advancing risks from a host of threats are forcing management to face difficult decisions about how to effectively address information security. In addition, scores of new and existing laws and regulations are increasingly demanding compliance and higher levels of accountability.

[2] Drucker, Peter; "Management Challenges for the 21st Century," *Harpers Business*, 1993

Information security governance is the responsibility of the board of directors and executive management. It must be an integral and transparent part of enterprise governance. It consists of the leadership, organizational structures and processes that safeguard information.

1.4.1 Importance of Information Security Governance

From an organization's perspective, information security governance is increasingly critical as dependence on IT grows. One reason is because, "A man's judgment cannot be better than the information on which he has based it."[3]

Information defined as "data endowed with meaning and purpose" is the substance of knowledge. Knowledge is in turn captured, transported and stored as organized information. "Knowledge is fast becoming the sole factor of productivity, sidelining both capital and labor."[4]

For most organizations, information and the knowledge based on it, has become increasingly one of their most important assets without which conducting business would not be possible. The systems and processes that handle this information have become truly pervasive throughout business and governmental organizations globally. This growing dependence of organizations on information and the systems that handle it, coupled with the risks, benefits and opportunities these resources present, have made information security governance an increasingly critical facet of overall governance. In addition to addressing legal and regulatory requirements, effective information security governance is simply good business. Prudent management has come to understand that it provides a series of significant benefits including:

- Addressing the increasing exposure the organization and its management have to civil or legal liability as a result of inaccurate information provided to the public or to regulators as well as the consequences of not exercising due care in the protection of private information
- Providing assurance of policy compliance
- Increasing predictability and reducing uncertainty of business operations by lowering risks to definable and acceptable levels
- Providing the structure and framework to optimize allocations of limited security resources
- Providing a level of assurance that critical decisions are not based on faulty information
- Providing a firm foundation for efficient and effective risk management, process improvement, and rapid incident response
- Providing accountability for safeguarding information during critical business activities such as mergers and acquisitions, business process recovery, and regulatory response

And finally, because new information technology provides the potential for dramatically enhanced business performance, effective information security can add significant value to the organization by:

- Providing greater reliance on interactions with trading partners
- Improved trust in customer relationships
- Protecting the organization's reputation
- Enabling new and better ways to process electronic transactions

Information security (infosec) covers all information processes, physical and electronic, regardless of whether they involve people and technology or relationships with trading partners, customers and third parties. It is concerned with all aspects of information and its protection at all points of its life cycle within the organization.

[3] Hays Sulzberger, Arthur; *New York Times*, March 1947
[4] *Op. cit.*, Drucker

1.4.2 Outcomes of Security Governance

The five basic outcomes of effective security governance should include:

1. **Strategic alignment**—Align information security with business strategy to support organizational objectives. Components include:
   - Security requirements driven by enterprise requirements thoroughly developed to provide guidance on what must be done and a measure of when it has been achieved
   - Security solutions fit for enterprise processes that take into account the culture, governance style, technology, and structure of the organization
   - Investment in information security aligned with the enterprise strategy and well defined threat, vulnerability and risk profile
2. **Risk management**—Manage and execute appropriate measures to mitigate risks and reduce potential impacts on information resources to an acceptable level. Components include:
   - Collective understanding of the organizations threat, vulnerability and risk profile
   - Understanding of risk exposure and potential consequences of compromise
   - Awareness of risk management priorities based on potential consequences
   - Risk mitigation sufficient to achieve acceptable consequences form residual risk
   - Risk acceptance/deference based on an understanding of the potential consequences of residual risk
3. **Value delivery**—Optimize security investments in support of business objectives. Components include:
   - A standard set of security practices, i.e., baseline security requirements following adequate and sufficient practices proportionate to risk
   - Properly prioritized and distributed effort to areas with greatest impact and business benefit
   - Institutionalized and commoditized standards-based solutions
   - Complete solutions, covering organization and process as well as technology based on an understanding of the end to end business of the organization
   - A continuous improvement culture based on the understanding that security is a process, not an event
4. **Resource management**—Utilize information security knowledge and infrastructure efficiently and effectively. Components include:
   - Ensure knowledge is captured and available
   - Document security processes and practices
   - Develop security architecture(s) to define and utilize infrastructure resources efficiently
5. **Performance measurement**—Measure, monitor and report on information security processes to ensure objectives are achieved. Components include:
   - Defined, agreed-upon, and meaningful set of metrics properly aligned with strategic objectives
   - Measurement process that will help identify shortcomings and provide feedback on progress made resolving issues
   - Independent assurance provided by external assessments and audits

1.4.2.1 Emerging Concept of Business Process Assurance

This concept consists of integrating all relevant assurance factors to ensure processes operate as intended from end to end:

- Determine all organizational assurance functions.
- Develop formal relationships with other assurance functions.
- Coordinate all assurance functions for more complete security.
- Ensure roles and responsibilities between assurance functions overlap.

1.5 EFFECTIVE INFORMATION SECURITY GOVERNANCE

Corporate governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

The strategic direction of the business will be defined by business goals and objectives. Information security must support business activities to be of value to the organization.

Information security governance is a subset of corporate governance that provides strategic direction for security activities and ensures objectives are achieved. It ensures that information security risks are appropriately managed and enterprise information resources are used responsibly.

To achieve effective information security governance, management must establish and maintain a framework to guide the development and management of a comprehensive information security program that supports business objectives.

The governance framework will generally consist of:
- A comprehensive security strategy intrinsically linked with business objectives
- Governing security policies that address each aspect of strategy, controls and regulation
- A complete set of standards for each policy to ensure procedures and guidelines comply with policy
- An effective security organizational structure void of conflicts of interest
- Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness

This framework in turn provides the basis for the development of a cost-effective information security program that supports the organization's business goals. Implementing a security program is covered in chapter 3. The objective of the program is a set of activities which provide assurance that information assets are given a level of protection commensurate with their value or with the risk their compromise poses to the organization.

Although 28 percent of all companies are operating security programs at best in class levels, Aberdeen Group research shows that less than 10 percent operate best-in-class security governance programs.[5]

> *Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management—including boards of directors, senior executives and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieve, or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability and resources to act and enforce compliance.*[6]

"Firms operating at best-in-class (security) levels are lowering financial losses to less than 1 [percent] of revenue, whereas other organizations are experiencing loss rates that exceed 5 [percent]."[7]

1.5.1 Roles and Responsibilities of Senior Management and Boards of Directors

1.5.1.1 Boards of Directors/Senior Management

Information security governance requires strategic direction and impetus. It requires commitment, resources and assigning responsibility for information security management, as well as a means for the board to determine that its intent has been met. Effective information security governance can be accomplished only by involvement in approving policy, and appropriate monitoring and metrics coupled with reporting and trend analysis.

[5] Aberdeen Group, "Best Practices in Security Governance," USA, 2005
[6] Allen, Julia; "Governing for Enterprise Security," Carnegie Mellon University, USA, 2005
[7] *Op. cit.*, Aberdeen Group

Members of the board need to be aware of the organization's information assets and their criticality to ongoing business operations. This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analysis (BIA). It may also be accomplished by business dependency assessments of information resources. A result of these activities should include board members validating/ratifying the key assets they want protected and that protection levels and priorities are appropriate to a standard of due care.

The tone at the top must be conducive to effective security governance. It is unreasonable to expect lower-level personnel to abide by security measures if they are not exercised by senior management. Executive management endorsement of intrinsic security requirements provides the basis for ensuring security expectations are met at all levels of the enterprise. Penalties for noncompliance must be defined, communicated and enforced from the board level down.

1.5.1.2 Executive Management

Implementing effective security governance and defining the strategic security objectives of an organization is a complex, arduous task. As with any other major initiative, it must have leadership and ongoing support from executive management to succeed. Developing an effective information security strategy requires integration with and cooperation of business process owners. A successful outcome is the alignment of information security activities in support of business objectives. To the extent this is achieved will determine the cost-effectiveness of the information security program in achieving the desired objective of providing a predictable, defined level of assurance for business processes and an acceptable level of impact from adverse events.

1.5.1.3 Steering Committee

To some extent, security affects all aspects of an organization. To be effective, it must be pervasive throughout the enterprise. To ensure that all stakeholders impacted by security considerations are involved, many organizations use a steering committee comprised of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives. It can also be instrumental in achieving modification of behavior toward a culture more conducive to good security.

1.5.1.4 CISO

All organization have a chief information security officer (CISO) whether anyone holds that title or not. It may be the CIO, CFO or, in some cases, the CEO—even when there is an information security office or director in place. The scope and breadth of information security today is such that the authority required and the responsibility taken will inevitably end up with a C-level officer or executive management. Legal responsibility will by default extend up the command structure and ultimately reside with senior management and the board of directors. Failure to recognize this and implement appropriate governance structures can result in senior management being unaware of this responsibility and the attendant liability. It also usually results in a lack of effective alignment of business objectives and security activities. Increasingly, prudent management is elevating the position of information security officer to a C-level or executive position, as organizations begin to understand their dependence on information and the growing threats to it.

1.5.2 Matrix of Outcomes and Responsibilities

The relationship between the outcomes of effective security governance and management responsibilities are shown in **figure 1.2**. These are not meant to be comprehensive but merely indicate some primary tasks and level for which management is responsible.

Figure 1.2—Relationships of Security Governance Outcomes to Management Responsibilities						
Management Level	**Strategic Alignment**	**Risk Management**	**Value Delivery**	**Performance Measurement**	**Resource Management**	**Process Assurance**
Board of directors	Require demonstrable alignment.	Institute a policy of risk management in all activities and ensure regulatory compliance.	Require reporting of security activity costs.	Require reporting of security effectiveness.	Institute a policy of knowledge management and resource utilization.	Institute a policy of assurance process integration.
Executive management	Institute processes to integrate security with business objectives.	Ensure roles and responsibilities include risk management in all activities and monitor regulatory compliance.	Require business case studies of security initiatives.	Require monitoring and metrics for security activities.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all assurance functions and plans for integration.
Steering committee	Review security strategy and integration efforts, and ensure business owners support integration.	Identify emerging risks, promote business unit security practices and identify compliance issues.	Review adequacy of security initiatives to serve business functions.	Review and advise *vis-a-vis* security initiatives and ensure they meet business objectives.	Review processes for knowledge capture and dissemination.	Identify critical business processes and assurance providers, and direct assurance integration efforts.
Chief information security officer	Develop security strategy, oversee the security program and initiatives, and liaise with business process owners for ongoing alignment.	Ensure risk and business impact assessments, develop risk mitigation strategies, and enforce policy and regulatory compliance.	Monitor utilization and effectiveness of security resources.	Develop and implement monitoring and metrics approaches, and direct and monitor security activities.	Develop methods for knowledge capture and dissemination, and develop metrics for effectiveness and efficiency.	Liaise with other assurance providers, and ensure that gaps and overlaps are identified and addressed.

1.6 INFORMATION SECURITY CONCEPTS

There are a number of business and technology related concepts that the ISM is expected to thoroughly understand to implement effective security governance and perform the other required tasks. These include knowledge of budgeting, reporting, personnel management, technology and business law, forensics and investigative procedures, organization management, and managing change within an organization. Often the success of an ISM and his/her recognition as a contributor to the success of an enterprise is more related to the manager's business skills and expertise than to the technical security knowledge that the ISM brings. The ISM is expected to bring a comprehensive understanding of security technology and methods to the executive conference table. What distinguishes an effective information security executive is the ability to translate security concepts and directions into business language as well as the ability to integrate security technologies and processes into business processes.

There are a variety of security technologies of which it is important for the ISM to have a thorough conceptual understanding. These will be addressed in later sections of this review manual.

1.7 INFORMATION SECURITY MANAGER

1.7.1 Responsibilities

The responsibilities and authority of ISMs vary dramatically between organizations, although they are on the rise globally. This can be attributed to the growing awareness of the importance of this function driven by increasingly spectacular failures of security and the growing losses that result. These responsibilities currently range from the CISO that reports to the CEO to system administrators who have part-time responsibility for security management.

Reporting structures for ISMs vary widely. In several recent surveys conducted by the International Development Corp. (IDC) and CMP Media, a significant majority—approximately 30 percent—of all ISMs report directly or indirectly to the CIO. While this is often functionally adequate, it constitutes a structural deficiency that must eventually be rectified. There are several reasons why this is the case. One is that the increasingly broad requirements of information security transcends the purview of the typical CIO. Another reason is the inherent conflict of interest. Information security, due to efforts to ensure security, is often perceived as a constraint on IT operations. CIOs and their IT departments are usually under pressure to increase performance and cut costs. Security is often the victim of these pressures. Finally, it must be considered that information security, to be effective, must be more aligned with business than with technology.

1.7.2 Senior Management Commitment

As with any organization's initiatives, without senior management commitment and support, enterprise information security activities are unlikely to be successful. Information security spans every division and department in a company to some extent. Any initiative that affects so many people and so many business processes cannot be successful without senior management support and commitment. It is imperative that senior management views security as a serious subject and allocates appropriate resources.

Once an ISM has developed the security strategy with input from key business units, approval of the strategy by senior management is required. Since this is typically a complicated subject, the ISM may need to first educate senior managers on the high-level aspects of information security and submit the overall strategy for review. A presentation to senior management describing the various aspects of the security strategy usually will take place to support and explain the documentation that the ISM submitted. Unfortunately, in many organizations, the true value of IT systems does not become apparent until they fail. Senior management will be in a better position to support security initiatives if they are educated on how critical IT systems are to the continued operation of the enterprise. In addition, there is often significant confusion about which regulations apply to the organization. It will be helpful to provide an overview of pertinent regulations, compliance requirements and possible sanctions, if the organization is out of compliance.

Senior management (board-level directors or equivalent) should have a high level of commitment to:
- Achieving high standards of corporate governance
- Treating information security as a critical business issue and creating a positive security environment
- Demonstrating to third parties that the organization deals with information security in a professional manner
- Applying fundamental principles such as assuming ultimate responsibility for information security, implementing controls that are proportionate to risk and achieving individual accountability

Senior management should demonstrate their commitment to information security by:
- Becoming directly involved in high-level information security arrangements, such as information security policy
- Providing high-level control
- Allocating sufficient resource to information security
- Reviewing information security effectiveness periodically

1.7.2.1 Obtaining Senior Management Commitment

The most widely used technique ISMs can use to secure senior management commitment and support of information security management policies, procedures and strategy is a formal presentation.

The formal presentation to senior management is used as a means to educate and communicate key aspects of the overall security program. Acceptance is facilitated by the ISM applying common business case aspects throughout the acceptance process. These can include:
- Aligning security objectives with business objectives enabling senior management to understand and apply the security policies and procedures
- Identifying potential consequences of failing to achieve certain security-related objectives and regulatory compliance.
- Identifying budget items so senior management can quantify the costs of the security program
- Utilizing commonly accepted project risk/benefit models, such as total cost of ownership (TCO) or the cost/benefit to quantify the benefits and costs of the security program

- Defining the monitoring and auditing measures that will be included in the security program
- Defining compliance processes
- Utilizing methods such as balanced business scorecards providing senior management a means of analyzing the progress of the security program
- Requiring that risk management be integrated into the operation of the security program
- Ensuring that clear accountabilities and responsibilities are defined
- Approving training and awareness programs
- Attending departmental staff meetings and making presentations. Staff will note the commitment of departmental heads during such meetings.

It also should be noted that while senior management may support the security program, it is imperative that all employees understand and abide by the security parameters defined and put into place. Without employee acceptance, it is unlikely that the security program will be successful and meet its objectives. It is important for senior management to be seen complying with security requirements. For example, if a physical access control system is implemented in the organization, senior management should lead by example and not be "out of the system" when it is implemented.

1.8 SCOPE AND CHARTER OF INFORMATION SECURITY GOVERNANCE

Information security deals with all aspects of information whether spoken, written, printed, electronic or relegated to any other medium regardless of whether it is being created, viewed, transported, stored or destroyed. This is contrasted with IT security, which is concerned with security of information within the boundaries of the technology domain. Typically, confidential information disclosed in an elevator conversation or sent via the mail would be outside the scope of IT security. From an information security perspective, however, the nature and type of compromise is not important, the fact that security has been breached is.

In the context of information security governance, it is important that the scope and responsibilities of information security are clearly set forth in the information security strategy.

1.8.1 Convergence

For several decades, it has been clear that the arbitrary division of security-related activities into physical security, IT security, risk management, privacy, compliance, information security and other disciplines has not been conducive to achieving optimal results. The increasingly dire consequences of disintegrated security efforts has caused this separation to increasingly be reconsidered by professionals and management. It is becoming more common to see CISOs being elevated to CSO to better integrate the main security elements. Physical security for many organizations has become fairly routine and is more easily integrated into information security than the other way around. The recent alliance of ISACA with ISSA and ASIS International is an indication of the trend in this direction.

Since it is not possible to effectively deliver information security without a number of physical considerations, the evolution is natural. It is reasonable to expect that the integration of many security activities will center around information security in the coming decade. As a result, aspects of physical security and other assurance functions will increasingly be relevant for the ISM to consider.

1.9 INFORMATION SECURITY GOVERNANCE METRICS

Quantitatively, effectiveness of security governance may be difficult to measure with accuracy if at all. Clearly, it can be argued that good security governance must be gauged by how effectively and efficiently the security machinery performs and what the trends indicate. In practice, key goal indicators (KGIs) may be one of the most effective measures of the success of governance and the security strategy employed.

If the aforementioned six outcomes of effective security governance are the hallmark of success, then there will be specific indicators that the objectives have been achieved. Each of the six expected outcomes of good security governance is discussed below with some suggested KGIs that might be employed. There are certain to be others that may be more useful to specific organizations. The point is to determine what KGIs are important, whether trends are in the right direction and when objectives have been achieved.

1.9.1 Strategic Alignment

Strategic alignment of information security in support of business objectives is an increasingly critical element of effective information security governance.

Indicators of alignment can include a subjective evaluation by business process owners indicating that:
- Security activities do not materially hinder business
- The security program enables business activities
- Security activities have provided predictable, robust operations
- Security incidents have not significantly impacted business operations
- Trends for adverse impacts are continuously improving
- The security organization is responsive to business requirements
- The cost of security measures are appropriate and generally track the degree of risk and value of assets
- The security group understands the business objectives

1.9.2 Risk Management

Executing appropriate measures to mitigate risks and reduce potential impacts on information resources to an acceptable level is the goal of risk management. An understanding of acceptable risk must be achieved and a comprehensive risk assessment is the requisite precursor. Additional risk assessments will be required to determine if residual risks are acceptable.

KGIs can include:
- Cost-effectiveness of risk mitigation
- Reductions in residual risk
- Reduction in open vulnerabilities
- Reduction of significant risks
- Reduction in adverse impacts
- Improved response time to new risks
- Systematic, continuous risk management
- Periodic risk assessments
- Tested business continuity planning (BCP)/disaster recovery (DR)
- Completeness of asset valuation and assignment of ownership
- Meeting RTO objectives during tests

The overarching goal of information security is to reduce adverse impacts on the organization's business operations to an acceptable level.

A key metric is, therefore, the extent of impacts to the organization. An effective security program will show a trend in impact reduction both in frequency and cost. A quantitative measure can include a trend analysis of impacts quarter over quarter.

1.9.3 Business Process Assurance

Most organizations have a number of assurance functions that have different reporting structures and are poorly integrated if at all. This often results in gaps in security with unexpected consequences and impacts. These assurance "silos" can include risk management, change management, internal and external audit, privacy offices, insurance offices, human resources, legal and others. Integration of all relevant assurance functions is an important objective to preclude unintended gaps in security and to ensure business processes operate as intended from end to end.

KGIs can include:
- No gaps exist in information asset protection.
- All assurance activities are demonstrably integrated.
- Roles and responsibilities that are well defined with concise interfaces
- Responsibility and accountability are clearly defined.
- The steering committee has representatives of all assurance functions.

1.9.4 Value Delivery

Optimizing security investments in support of business objectives is the goal of assuring the best return on security investments. Security activities consume resources. Optimal investment levels occur when strategic goals for security are achieved at the lowest cost.

KGIs can include:
- Security activities that achieve strategic objectives on budget
- The cost of security is proportional to the value of assets.
- Security resources are allocated by degree of assessed risk.
- Aggregate protection costs that are a function of revenues or asset valuation
- Utilization of controls—rarely used controls are not likely to be cost-effective.
- The number of controls to achieve acceptable risk and impact levels. Fewer effective controls can be expected to be more cost-effective than more less-effective controls.
- The effectiveness of controls as determined by testing. Marginal controls are not likely to be cost-effective.

1.9.5 Resource Management

Using information security knowledge and infrastructure efficiently and effectively is the objective of effective resource management.

KGIs can include:
- The frequency of problem rediscovery
- The effectiveness of knowledge capture and dissemination
- Clearly defined roles and responsibilities for IT security functions
- IT security functions that are incorporated into every project plan
- Information assets and related threats that are covered by security resources

1.9.6 Performance Measurement

Monitoring and reporting on information security processes to ensure that objectives are achieved is a requirement of effective management. It is difficult or impossible to manage what is not being measured.

KGIs can include:
- The time it takes to detect and report incidents
- The number and frequency of unreported incidents
- Benchmarking security costs against comparable organizations

- Effectiveness/efficiency of controls
- Trends in audit findings
- Compliance metrics
- Times for variance resolution
- Trends in impacts
- Down time for critical systems

1.10 DEFINING AN INFORMATION SECURITY STRATEGY

There are a number of definitions of strategy. While they all generally point in the same direction, they vary widely in scope, emphasis and detail. One that is representative of what is required for an information security strategy definition is:

> *Corporate strategy is the pattern of decisions in a company that determines and reveals its objectives, purposes, or goals, produces the principal policies and plans for achieving those goals, and defines the range of business the company is to pursue, the kind of economic and human organization it is or intends to be, and the nature of the economic and non-economic contribution it intends to make to its shareholders, employees, customers, and communities.*[8]

Adding security in the appropriate places to the foregoing statement provides a good working definition of a security strategy. The term "to ensure prosperity" is unusual, but obviously the end goal of all organizations whatever form "prosperity" takes.

1.10.1 An Alternate View of Strategy

A recent report from McKinsey poses the caution that often the "approach to strategy involves the mistaken assumption that a predictable path to the future can be paved from the experience of the past."[9] It goes on to suggest that strategic outcomes canot be predetermined given today's turbulent business environment.

As a result, McKinsey proposes to define strategy as "a coherent and evolving portfolio of initiatives to drive shareholder value and long-term performance." This change in thinking requires management to develop a "you are what you do" perspective as opposed to "you are what you say." In other words, companies are defined by the initiatives they prioritize and drive, not merely by mission and vision statements.

The report goes on to say "Strategy approached in this way is by its very nature more adaptive and less dependent upon 'big bets.' A carefully managed portfolio of initiatives is balanced across activities of adapting the core businesses to meet future challenges, shaping the portfolio in an ongoing way to respond to a changing environment, and building the next generation of businesses. By creating a portfolio of initiatives around a unifying theme, reinforced by brands, value proposition to customers, and solid operational skills, a company can successfully set the stage to drive shareholder value."

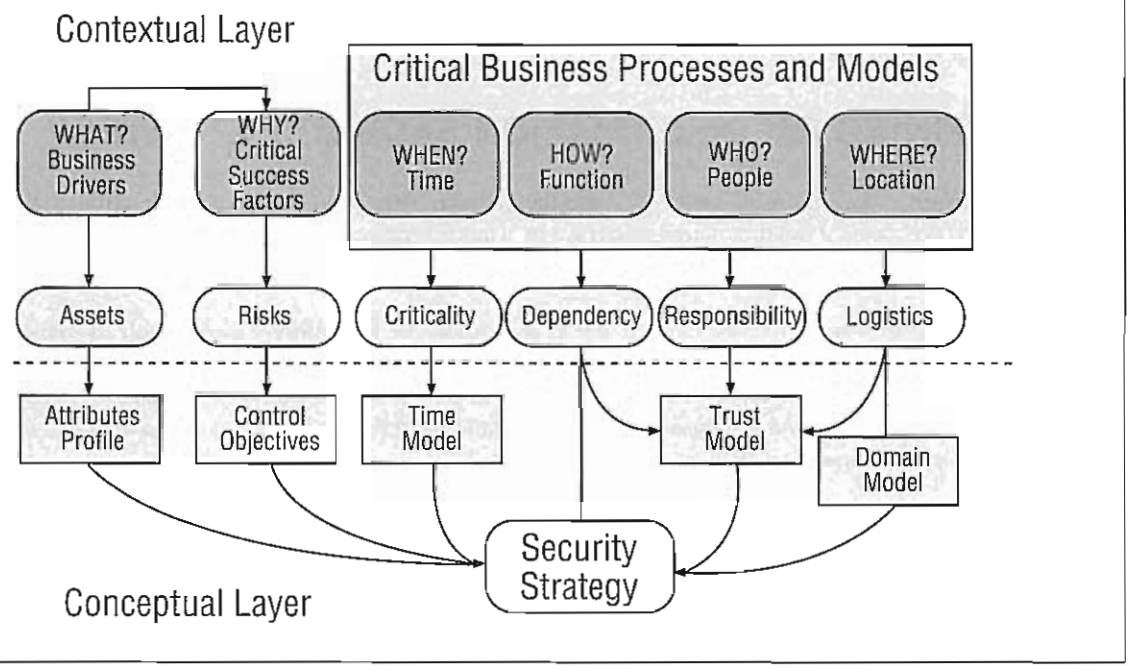
Whichever definition or approach is appropriate to a particular organization, the implementation steps remain essentially the same. The "adaptive" McKinsey model may be more appropriate to organizations experiencing a great deal of change. The more traditional model may achieve the same adaptability by increasing the monitoring of key performance indicators (KPIs) and reviewing strategy suppositions more frequently.

The arguably more important criteria for good outcomes from a successful strategy is strong ongoing senior management leadership and commitment to achieving effective information security governance.

[8] Andrews, Kenneth; *The Concept of Corporate Strategy, 2nd Edition*, Dow-Jones Irwin, 1980
[9] Roxburgh, Charles; "Hidden Flaws in Strategy," *The McKinsey Quarterly*, number 2, 2003

Another perspective on strategy is provided from an architectural viewpoint as shown in **figure 1.3**.

Figure 1.3—Strategy



1.11 CHALLENGES IN DEVELOPING AN INFORMATION SECURITY STRATEGY

1.11.1 Common Pitfalls

It would be an understatement to say history is littered with examples of bad strategies. It is surprising that after nearly four decades of development of business strategy theory that failure of strategy continues unabated. Some reasons are fairly evident including inadequate analysis, greed, unmitigated ambition and other corporate malfeasance.

Other causes of strategy failures are not so well understood but have root causes explained by behavioral economics, a branch of psychology that studies, among other things, decision-making processes and departure from rational choice. Experiments and studies have shown a variety of underlying causes for flawed decision making. Being aware of them may allow compensation to reduce adverse effects. Some of the main reasons include:

- **Overconfidence**—Research shows a tendency for people to have excessive confidence in the ability to make accurate estimates. Most people are reluctant to estimate wide ranges of possible outcomes and prefer being precisely wrong rather than vaguely right. Most also tend to be overconfident of their own abilities. For organizational strategies based on assessments of core capabilities, this can be particularly troublesome.
- **Optimism**—People tend to be optimistic in their forecasts. A combination of overconfidence and overoptimism can have a disastrous impact on strategies based on estimates of what may happen. Typically these estimates will be unrealistically precise and overly optimistic.
- **Anchoring**—Research shows that once a number has been presented to someone, a subsequent estimate of even a totally unrelated subject involving numbers will anchor on the first number. While potentially useful for marketing purposes, anchoring can have serious consequences in developing strategies when future outcomes are anchored in past experiences.
- **The status quo bias**—Most people show a strong tendency toward sticking with familiar and known approaches even when they are demonstrably inadequate or ineffective. Research also indicates that concern with loss is generally stronger than the excitement of possible gain. The "endowment effect" is a similar bias for people to keep what they own and that simply owning something makes it more valuable to the owner.

- **Mental accounting**— This is defined as "the inclination to categorize and treat money differently depending on where it comes from, where it is kept, and how it is spent." Mental accounting is common even in the boardrooms of conservative and otherwise rational corporations. Some examples of this include:
  - Being less concerned with expenses against a restructuring charge than those against the profit and loss (P&L) statement
  - Imposing cost caps on a core business while spending freely on a start-up
  - Creating new categories of spending, such as revenue investment or strategic investment as if the name impacted the amounts or justification
- **The herding instinct**—It is a fundamental human trait to conform and seek validation by the actions of others. It is the comfort and perceived safety of doing the same thing others are doing. It is observed in animals that "herd together" when faced with danger or uncertainty. This can also be observed when particular technologies or approaches are selected because "everyone else is doing it" regardless of applicability to a particular situation. This tendency can have significant adverse implications when developing strategy.
- **False consensus**—There is a well-documented tendency for people to overestimate the extent that others share their views, beliefs and experiences. A number of causes have been uncovered by research including:
  - Confirmation bias—Seeking opinions and facts that support one's own beliefs
  - Selective recall—Remembering only facts and experiences that reinforce current assumptions
  - Biased evaluation—Easy acceptance of evidence that supports one's hypotheses while contradictory evidence is challenged and almost invariably rejected. Critics are often charged with hostile motives or their competence impugned.
  - Groupthink—Pressure for agreement in team-based cultures. When developing strategies, false consensus can lead to ignoring or minimizing important threats or weaknesses in the plans and to persist with doomed strategies.

There have been numerous studies on the topic of departures from rational choice during the past several decades that may be worthy of study to reduce the risks of faulty decision making. Some of these may be found in the reference section for additional reading.[10]

1.12 INFORMATION SECURITY STRATEGY OBJECTIVES

1.12.1 The Goal

The first question that must be answered by an organization seeking to develop an information security strategy is—what is the goal?

While this seems a trivial question, most organizations fail to define the objectives of information security with any specificity. This may be because it seems obvious that the goal of information security is to protect the organization's information resources. However, that answer assumes knowledge of two things: that information resources are known with any degree of precision, which for most organizations is not the case, and that there is an assumed understanding of what it means to protect. Everyone understands the notion in general. It is considerably more difficult to state with precision the nature and degree of protection required for an organization's information resources much less what information needs what kind of protection.

These problems exist because organizations typically have little knowledge of what information is available within the enterprise. There is generally no process to purge useless, outdated or potentially dangerous information or data or, for that matter, unused applications. It is extremely rare to find a comprehensive catalog or index of information or a process to define what is important and what is not, or even who "owns" it. As a result, everything gets saved under the assumption that storage is cheaper than data classification and because it is not known who owns it or might need it. For large organizations, this can amount to terabytes of useless data and literally thousands of outdated and unused applications accumulated over decades.

[10] Porter, M. E.; "What Is Strategy?" *Harvard Business Review*, November-December 1996

This situation makes it difficult to devise a rational data protection plan, since it arguably makes little sense to expend resources protecting data or applications that are no longer used to serve a business need.

Assuming current relevant information is located and identified, then it must be cataloged, or classified, as to its criticality and sensitivity. A great deal of a typical organization's data and information will be neither critical nor sensitive, and it is wasteful to expend substantial resources to protect it. However, just as values are assigned to an organization's physical resources, information must be assigned values to prioritize budget-constrained protection efforts and determine required levels of protection.

Valuations of information are in most cases difficult to do with any precision. In some cases, it can be the cost of creating or replacing it. In other cases, information in the form of knowledge or trade secrets is difficult or impossible to replace and may literally be priceless. It is obviously prudent to provide excellent protection to "priceless" information.

Another approach that may be more useful and substantially easier to perform is a business dependency evaluation as an indication of value. This will provide a measure of the level of criticality of information resources that can be used as a guide to protection efforts. The level of sensitivity should also be defined at the same time to determine to what extent an information classification level requires controlled access. For most organizations, this still is a daunting task.

In summary, it will be difficult to develop a cost-effective security strategy that is aligned with business requirements prior to:
1. Determining the objectives of information security
2. Locating and identifying information resources
3. Valuating information resources
4. Classifying information resources as to criticality and sensitivity

Most organizations have taken years or decades to create terabytes of data and the problem of useless, outdated or dangerous information is unlikely to be resolved quickly. However, delaying resolution will only compound the problem and increases the ultimate cost. It must be considered deferred maintenance and probably should be booked as a liability. Unless dealt with, the problem will clearly continue to grow as Gartner estimates that business will within the next decade need to deal with 30 times as much information as they do now.

One approach to resolve the problem is to have the information security strategy include the goal of clearing out the "information attic" over time. The strategy should in conjunction set the goal of not compounding the problem by allowing these practices, or lack of them, to continue. This includes creating and implementing information ownership policies as well as data retention and destruction policies

From the perspective of making a business case for getting data under control, it may be useful to realize that a number of organizations have suffered significant financial losses in the course of legal actions when the opposing side located incriminating e-mails and other data that should have been subject to a data destruction policy.

1.12.2 Defining Objectives

If an information security strategy is the basis for a plan of action to achieve security objectives, it will obviously be necessary to define those objectives. Defining long-term objectives in terms of a "desired state" of security is necessary for a number of reasons. Without a well-articulated vision of desired outcomes for a security program, it will not be possible to develop a meaningful strategy.

Without a strategy, it also will not be possible to develop a meaningful plan of action and the organization will continue to implement *ad hoc* tactical point solutions. There will be nothing to provide an overall integrating effect. The resulting disintegrated systems will be increasingly difficult to manage and will become increasingly costly and difficult or impossible to secure.

1.12.2.1 Business Linkages

Many objectives will be stated in terms of mitigating risks. Information security strategy objectives should also be stated in terms of specific objectives to better support business activities. Some risk mitigation will apply to the organization generally such as virus and other malware protection. Such protection is generally not considered a specific business enabler, rather it supports the overall health of the organization by reducing adverse impacts that hinder business.

A review of the organization's strategic business plans are likely to uncover opportunities for information security activities to be directly supportive of or enable a particular avenue of business. For example, the implementation of a public key infrastructure (PKI) can enable high-value transactions between trusted trading partners or customers. Deploying virtual private networks (VPNs) may provide the sales force with secure remote connectivity enabling improved performance. In other words, information security can facilitate business activities that would otherwise be too risky.

Other business linkages can start from the perspective of the specific objectives of a particular line of business. A review and analysis of all the elements of a particular product line can illustrate this approach.

Consider an organization that manufactures breakfast cereal. The raw materials come into the plant on a just-in-time basis via train. The grains are dumped into hoppers that feed the various processing machinery. The finished flakes are packaged and moved to a warehouse.

This relatively straightforward process relies on numerous information flows subject to a failure of availability, confidentiality or integrity. Any breakdown or significant disruption in the supply chain side (e.g., ordering, tracking, payments) is likely to cause a disruption in manufacturing. Failure in the accounting processes will disrupt the business. Virtually all the processing of materials in the plant will be tied to information flows. Information security, to be effective, must take into consideration all of the information flows that are critical to ensuring continued operations. To accomplish this, it is necessary to have a good understanding of the business and on what critical information flows it depends.

It is important to take the approach of identifying the threats to information flows. Obviously, anything that can affect the integrity of the information will be a problem as will any effect on availability. The linkage to the business in this case can provide value from security by reducing the ability of threats to impact the processes and subsequently reduce negative impacts. The other possibility is that analysis of the process may yield improvements in productivity as well as security by eliminating unnecessary steps or automating processes.

The analysis in the foregoing example might look at the dozens of discrete information handling processes that occur in this operation. Investigation into the history of the process may reveal past failures that will indicate a weaknesses in the system. Most failures will be human error and it may be possible to reduce that by increased training and awareness, better controls, or more reliable automated processes.

Typical errors include entry mistakes, which might be improved by range checking or other technical processes. It may require procedural changes or an entry validation process.

Effective business linkages will serve to uncover information security issues at the operational level that can be addressed by security. This will visibly improve the perception of the value of information security and make business processes more robust.

Improved business linkage can be one of the beneficial outcomes of establishing an information security steering group if operations managers are included. Linkages may also be established by regular meetings with business owners to discuss security-related issues. This may also provide an opportunity to educate business process owners on potential benefits that security may provide for their operation.

1.12.3 The Desired State

Defining a state of security in quantitative terms is not possible. Consequently, a desired state of security must be defined qualitatively in terms of attributes and characteristics. Several useful approaches are available to do this. The various approaches should be evaluated to determine which provides the best form, fit and function for the organization. Several of the most accepted approaches are briefly described in the following subsections.

1.12.3.1 COBIT

Control Objectives for Information and related Technology (COBIT) focuses on IT controls. From the ISM perspective, control objectives and procedures must be broadened beyond IT activities to include any activity that may impact information security. Despite the technology focus, COBIT is a powerful, well-developed system that can serve information security objectives well.

COBIT defines controls as "the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."[11]

Control objectives are defined as "a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity."[12]

COBIT defines governance as "a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes."[13]

COBIT sets out 34 high-level control objectives for information and the technology that supports it. The controls are divided into four domains:

- *Plan and Organize*—This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organization as well as technological infrastructure must be put in place.
- *Acquire and Implement*—To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems
- *Deliver and Support*—This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. To deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.
- *Monitor and Evaluate*—All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

1.12.3.2 Capability Maturity Model

The desired state of security may also be defined as achieving a specific level in the Capability Maturity Model (CMM) developed by Carnegie Mellon University. It consists of grading each defined area of security on a scale of 0 to 5 based on the maturity of processes. The approach is presented in detail in Appendix B. The maturity levels are described as shown in **figure 1.4**.

[11] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Controls—An Integrated Framework*, USA, 1992
[12] *Ibid.*
[13] IT Governance Institute, COBIT *Security Baseline*, USA, 2004

Figure 1.4—CMM Maturity Levels	
Maturity Level	**Description**
0	Nonexistent—No recognition by organization of need for security
1	*Ad hoc*—Are considered on an *ad hoc* basis—no formal processes
2	Repeatable but intuitive—Emerging understanding of risk and need for security
3	Defined process—Companywide risk management policy/security awareness
4	Managed and measurable—Risk assessment standard procedure, roles and responsibilities assigned, policies and standards in place
5	Optimized—Organizationwide processes implemented, monitored and managed

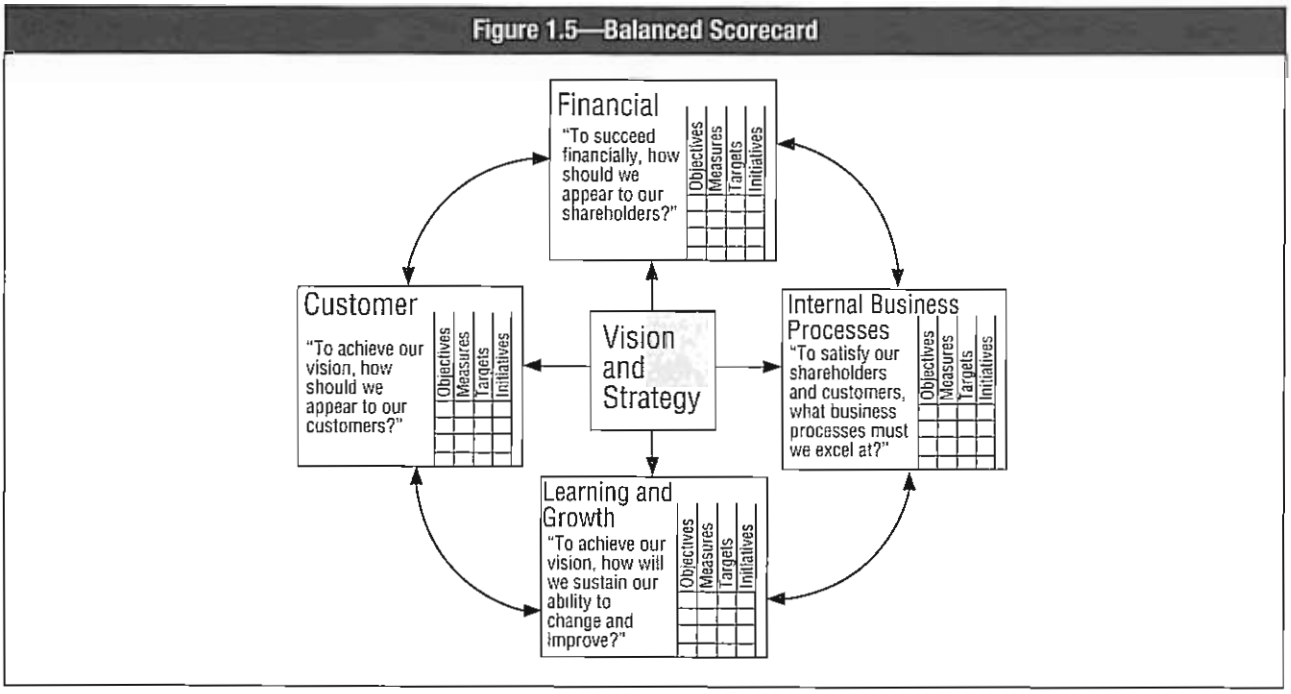
1.12.3.3 Balanced Scorecard

The balanced scorecard is a management system (not only a measurement system) that enables organizations to clarify their vision and strategy and translate them into action. It provides feedback about the internal business processes and external outcomes to continuously improve strategic performance and results. When fully deployed, the balanced scorecard transforms strategic planning from an academic exercise into the nerve center of an enterprise.

The balanced scorecard uses four perspectives, and develops metrics, collects data and analyzes them relative to each of these perspectives:

- Learning and growth
- Business process
- Customer
- Financial

Figure 1.5—Balanced Scorecard



1.12.3.4 Systems and Business Security Architecture

The key to success in the Systems and Business Security Architecture (SABSA®) methodology is to be business-driven and business-focused. The business strategy, objectives, relationships, risks, constraints and enablers all explain what sort of security architecture the organization needs. This analysis and description of the business itself is called the contextual security architecture.

SABSA uses a matrix of business drivers and attributes to describe the objectives of security from an architectural perspective. Architecture should be an expression of strategy and, therefore, the attributes apply to both. This approach also emphasizes traceability from strategy through to execution.

Figure 1.6—Security Architecture

	Data (What)	Function (How)	Location (Where)	People (Who)	Time (When)	Motivation (Why)
Contextual	Business information security	List of business security processes	List of business locations	Organizations significant to the business	List of significant to the business	Goals, success factors and risks
Conceptual	Business entities and relationships	Business security process model	Nodes and linkages	Organizational units and work flow	Master schedule of events	Business objectives and strategy
Logical	Data entities and relationships	Security service	Service elements at nodes and links	Roles and deliverables	Processing cycle	Business rules and policies
Physical	Data tables and messages	Security mechanisms	Security infrastructure	Users and the user interface	Control structure execution	Business practices and actions
Component	Data fields and addresses	Security products and tools	Processes, N/W addresses and protocols	User identities	Step timing and sequencing	Business steps
Operational	Data security	Security functions	Network and platform security	Work done by users	Business operational schedule	Business operations

1.12.3.5 BS ISO/IEC 17799

To ensure that all relevant elements of security are addressed in an organizational security strategy, the 10 areas of ISO 17799 can provide a useful framework to gauge comprehensiveness. In similar fashion, policies and standards must be created that can track directly to each element of the standard.

The 10 major divisions of ISO 17799 are:
- Security policy
- Security organisation
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance with legal requirements

Each of the 10 major divisions are divided into 10 sections that must be appropriately addressed in a comprehensive security strategy and architecture. Not all sections of the standard will be relevant to a particular organization; therefore, it must be adapted as required.

1.12.3.6 Other Approaches

Other approaches and methods exist that may be useful and include some of the other ISO standards on quality (9001-2000), Six Sigma, publications from the US National Institute of Standards and Technology (NIST), standards from the Information Security Forum, the US Federal Information Security Management ACT (FISMA), and many others. Some of these focus more on management processes and quality management than on strategic security objectives. Although certainly a valid argument could be made that if the objective of a security strategy was to fully implement relevant components of ISO 17799, most or all security requirements are likely to have been met. However, that would probably be a needlessly expensive approach, and the standard itself suggests that it be carefully tailored to the specific requirements of the adopting organization. Other methodologies will undoubtedly emerge in the future that may prove to be more effective than those mentioned. The ones outlined are not meant to be exhaustive, merely some of the more widely accepted approaches to arrive at a well-defined information security objective.

It may be useful to employ a combination of methods to reach the desired state to assist in communications with others and as a way to cross-check the objectives to make certain all relevant elements are considered. For example, a combination of COBIT control objectives, CMM, the balance scorecard and SABSA would make a powerful combination. While it may seem overkill, each approach presents a different viewpoint which in combination is likely to make certain no significant aspect is overlooked. Since it is unlikely that an effective security program will devolve from a faulty strategy, this may be a prudent approach to ensure that does not occur.

1.12.3.7 GASSP/GAISP

Another useful guide when developing an information security strategy is the Generally Accepted Security System Principles (GASSP) and/or its successor, the Generally Accepted Information Security Principles (GAISP). Either provides a clear articulation of essential security features, assurances and practices. The pervasive principles enumerated should be considered an essential checklist for strategy and all security plans of action.

The nine pervasive principles are:

- **Accountability principle**—Information security accountability and responsibility must be clearly defined and acknowledged.
- **Awareness principle**—All parties, including, but not limited to, information owners and information security practitioners, with a need to know should have access to applied or available principles, standards, conventions or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information.
- **Ethics principle**—Information should be used, and the administration of information security should be executed, in an ethical manner.
- **Multidisciplinary principle**—Principles, standards, conventions and mechanisms for the security of information and information systems should address the considerations and viewpoints of all interested parties.
- **Proportionality principle**—Information security controls should be proportionate to the risks of modification, denial of use or disclosure of the information.
- **Integration principle**—Principles, standards, conventions and mechanisms for the security of information should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system.
- **Timeliness principle**—All accountable parties should act in a timely, coordinated manner to prevent or respond to breaches of and threats to the security of information and information systems.
- **Assessment principle**—The risks to information and information systems should be assessed periodically or when significant changes to systems, environment or technology occur.
- **Equity principle**—Information security must reflect an unbiased regard for the needs, rights and obligations of all parties affected by or accountable for the information.

1.12.4 Risk Objectives

One of the major inputs into defining the desired state will be the organization's approach to risk and its risk appetite, that is, what does management consider acceptable risk. It is vital although usually difficult to define without thorough consideration. This is, however, a critical step since defined acceptable risk will devolve into the control objectives or other mitigation measures employed. Control objectives will in turn be instrumental in determining the type, nature and extent of controls the organization will employ.

Developing the right strategy objectives usually needs to be an iterative approach based upon analysis of costs to achieve the desired state and achieve acceptable risk levels. It is likely that lowering the level of acceptable risk will be more costly. However, the approach to achieving the desired state will have a significant bearing on costs as well.

Once objectives have been crisply defined, there will be a number of ways to architect solutions that will vary significantly in costs and complexity. Whichever process is used, the objective is to define in meaningful, concrete terms the desired overall state of security at some future point

1.13 DETERMINING CURRENT STATE OF SECURITY

A current-state evaluation of information security must also be determined using the same methodologies or combination of methodologies employed to determine strategy objectives, or the desired state. In other words, whatever combination of COBIT, CMM, balanced scorecard, is used to define desired state must also be used to determine the current state. This will provide comparison between the two providing the basis for a gap analysis, which will delineate what is needed to achieve the objectives.

Using these same methodologies periodically will also provide the metrics on progress toward meeting the objectives as well as a security baseline. As has often been stated, "you must measure it to manage it."

1.13.1 Current Risk

The current state of risk must also be assessed through a comprehensive risk assessment. Just as risk objectives must be determined as a part of the desired state, so must the current state of risk be determined to provide the basis for a gap analysis of what risks and to what extent they must be addressed by the strategy. A full risk assessment will include threat and vulnerability analysis which individually may provide useful information in building a strategy as well. Since risks can be addressed in different ways such as altering risky behavior, developing countermeasures to threats, reducing vulnerabilities or developing controls, this information will provide the basis for determining the most cost-effective strategy to addressing risks. Additional periodic assessments will likewise provide the needed metrics to determine progress.

1.13.1.1 Business Impact Analysis

The current state evaluation should also include a thorough BIA to help round out the current state picture. Since the ultimate objective of security is to provide business process assurance and minimize the impacts of adverse events, an impact analysis provides some of the information needed to develop an effective strategy. The difference between acceptable levels of impact and current level of potential impacts must be addressed by the strategy.

1.14 DEVELOPING AN INFORMATION SECURITY STRATEGY

It is now possible to develop a meaningful strategy to move from the "current state" to the "desired state." Knowing where the organization is and where it is going will allow it to get there. The strategy provides the basis for creating a road map.

A set of information security objectives coupled with available processes, methods, tools and techniques create the means to construct a security strategy. A good security strategy should address and mitigate risks while complying with the legal, contractual and statutory requirements of the business, provide demonstrable support for the business objectives of the organization, and maximize value to the stakeholders. The security strategy also needs to address how the organization will embed good security practices into every business process and area of the business.

Often, those charged with developing a security strategy will think in terms of controls as the means to implement security. Controls, while important, are not the only element available to the strategist. In some cases, for example, reengineering a process can reduce or eliminate a risk without the need for controls. Potential impacts may also be mitigated by architectural modifications rather than controls. It should be considered that in some cases mitigating risks can reduce opportunities to the extent of being counterproductive.

Ultimately, the goal of security is business process assurance, regardless of the business. While the business of a government agency may not result directly in profits, it is still in the business of providing cost-effective services to its constituency and must still protect the assets for which it has custodial care. Whatever the business, its primary operational goal is to maximize the success of business processes and minimize impediments to those processes.

Some might argue that the primary goal of security is to protect information assets. However, information is only an asset insofar as it supports the primary purpose of the business, generating revenues (or cost- effective services) through value-add processes. All other information is a liability. As some organizations have discovered, information that should have been subject to a retention and destruction policy turned out to be a major liability when incriminating e-mails were discovered by the opposition in a lawsuit. Even if not incriminating, useless information is a cost to the organization, it consumes resources and is a liability.

1.14.1 Elements of a Strategy

What should go into a security strategy? The starting point and the destination have been defined. The next consideration must be what resources are available and what constraints must be considered when developing the road map? The resources are the mechanisms that will be used to achieve various parts of the strategy bound by the constraints.

1.14.1.1 Road Map

The typical road map to achieve a defined, secure desired state will include people, processes, technologies and other resources. The interaction and relationship between these elements are likely to be complex. As a consequence, it is prudent to consider the initial stages of developing a security architecture. An architecture such as SABSA, mentioned previously, can provide a structured approach to defining business drivers, resource relationships and process flows. It can help ensure that contextual and conceptual elements, such as business drivers and consequences, are considered in the strategy development stage. It is likely to be a misnomer to state that there is a strategy. There will likely be a variety of connected strategies required to achieve various objectives that cumulatively result in achieving the desired state over time.

Achieving the desired state will be a long-term project or series of projects. Like most large, complex projects, it will be necessary to break it down into a series of shorter term projects that can be accomplished in a reasonable time period given the inevitable resource constraints. The entire road map can and should be charted while understanding that there is no steady state for information security and some objectives will need to be modified over time. Some objectives, such as attaining a particular maturity level, reengineering high-risk processes or achieving specific control objectives, may not require modification.

Shorter-term projects aligned with the long-range objectives will serve to provide checkpoints and opportunities for midcourse corrections. They will also provide metrics to validate the overall strategy. For example, one long-term objective defined in the strategy may be data classification according to sensitivity and criticality. Because of the sheer magnitude of the effort required in a large organization, it is likely to require a number of years to accomplish. The strategy may include the requirement to determine that 25 percent of data will be targeted for classification each fiscal year utilizing a variety of tactical approaches. A second component of the strategy might be to create policies and standards that preclude the practices that gave rise to the problem, so it does not get worse while the remediation process is underway. An example of a short-term action plan to accomplish this objective is detailed below.

The development of a strategy to achieve long-term objectives and the road map to get there coupled with shorter-term, intermediate goals will provide the basis for sound policy and standards development in support of the effort.

1.14.2 Strategy Resources and Constraints

1.14.2.1 Resources

The resources available to the organization will need to be enumerated and considered when developing a security strategy. To the extent the resources exist within the organization, a more cost-effective approach can be developed minimizing the need to acquire additional resources.

Information security resources can be considered the mechanisms that are available in some optimal mix to achieve the desired state of security over time. They will typically include:

- Policies
- Standards
- Procedures

- Guidelines
- Architecture(s)
- Controls—physical, technical and procedural
- Countermeasures
- Layered defenses
- Technologies
- Personnel security
- Roles and responsibilities
- Skills
- Training
- Awareness and education
- Audits
- Compliance enforcement
- Threat analysis
- Vulnerability analysis
- Risk assessment
- Business impact assessment
- Resource dependency analysis
- Outsourced security providers
- Other organizational support and assurance providers
- Facilities
- Environmental security

1.14.2.2 Constraints

There will also be a number of constraints that must be considered when developing a security strategy and subsequent action plan. Constraints will typically include:

- **Law**—Legal and regulatory requirements
- **Physical**—Capacity, space and environmental constraints
- **Ethics**—Appropriate, reasonable and customary
- **Culture**—Both inside and outside the organization
- **Costs**—Time and money
- **Personnel**—Resistance to change and resentment against new constraints
- **Resources**—Capital, technology and people
- **Capabilities**—Knowledge, training, skills and expertise
- **Time**—Window of opportunity and mandated compliance
- **Risk tolerance**—Threats, vulnerabilities and impacts

Some of the constraints such as ethics and culture may have been dealt with in developing the desired state, especially if the pervasive principles of GASSP were considered. Others will arise as a consequence of developing the road map and action plan.

1.15 STRATEGY RESOURCES

1.15.1 Policies and Standards

There are a broad range of interpretations for policy, standards, procedures and guidelines. The definitions used in this document are in agreement with the major standards bodies and should be adopted to preclude miscommunication. Policies and standards are considered tools of governance and management respectively, procedures and guidelines the purview of operations. For clarity, the four are defined in the following subsections.

1.15.1.1 Policies
Policies are the high-level statements of management intent, expectations and direction.

An example of a policy statement on access control could be: information resources shall be controlled in a manner that effectively restricts unauthorized access.

Policy can be considered the "constitution" of security governance.

1.15.1.2 Standards
Standards are the rules or specificatins that when taken together define the requirements that implement a policy. As such, standards also form the metrics that can be used to determine if practices meet policy.

A standard for passwords used for access control could be: passwords for medium and low security domains shall be comprised of no less that eight characters consisting of a mixture of upper and lower case letters, at least one number and one punctuation mark.

The standard for access control for employees on the premises can include password composition requirements, minimum and maximum password length, frequency of password changes, rules for re-use and so forth. Generally, a standard must provide sufficient parameters or boundaries that a procedure or practice can be unambiguously determined to meet the requirements of the relevant policy. Standards must change as requirements and technologies change. Policies, in a mature organization, can for the most part remain fairly static. Multiple standards will usually exist for each policy depending on the security domain, e.g., the password standard would be more restrictive when accessing high-security domains.

1.15.1.3 Procedures
Procedures are the responsibility of operations but are included here for clarity. Procedures must be unambiguous and include all necessary steps needed to accomplish specific tasks. They must define expected outcomes and displays and required conditions precedent to execution. Procedures must also contain the steps required when unexpected results occur.

Procedures must be clear and unambiguous, and terms must be exact. For example, the words "must" "shall" "will" have to be used for any task that is mandatory. The words "should" can be used to mean a preferred action that is not mandatory. The term "may" or "can" must only be used to denote a purely discretionary action.

Procedures for passwords would include the detailed steps required for setting up password accounts, steps for changing or resetting passwords, etc.

1.15.1.4 Guidelines
Guidelines for executing procedures are also the responsibility of operations. Guidelines should contain information that will be helpful in executing the procedures. This can include dependencies, suggestions and examples, narrative clarifying the procedures, background information that may be useful, tools that can be used, etc. Guidelines can be useful in many other circumstances as well but are considered here in the context of information security governance.

1.15.2 Architecture

It is evident that there is not a general consensus on what security architecture is or why an organization might want one. Architecure can be a powerful tool as an element of strategy. There is a general lack of understanding as to what constitutes a security architecture and how it can be important in developing and implementing a security strategy.

The following analogy from the Meta Group provides a useful explanation.

> *In many respects, the information security architecture is analogous to the architecture associated with buildings. It begins as a concept, a set of design objectives that must be met (e.g., the function it will serve; whether it will be a hospital, a school, etc.). It then progresses to a model, a rough approximation of the vision forged from raw materials (read: services). This is followed by the preparation of detailed blueprints, or tools that will be used to transform the vision/model into a real and finished product. Finally there is the building itself, the realization, or output, of the prior stages.*[14]

Given the increasing size of security staffing in most organizations, the growing cyberrisks and losses coupled with increasing regulatory pressures and more problematic security administration, it is suprising that security architecture generally has had little impact on enterprise security efforts. This may be largely attributable to the fact that few organizations have what can be called a security architecture or for that matter, even a security strategy on which to base it.

> *Indeed, without one,(security architecture), evidence suggests that enterprises will default to a haphazard, reactive, tactical approach to constructing a secure environment, regrettably wasting resources and introducing more vulnerabilities as they proceed to fix others.*[15]

The failure of organizations to embrace the notion of security architecture appears to have several identifiable causes. One is that such projects are expensive and time-consuming, and there is little or no understanding or appreciation at most organizational levels for the necessity or the potential benefits.

It may also be that there is not an abundance of competent architects that have sufficiently broad and deep experience to address the wide range of issues necessary to ensure a reasonable degree of success.

The effect of this lack of architecture over time has been to have functionally less security integration and increasing vulnerability across the enterprise at the same time that technical security has seen significant improvement. This lack of integration contributes to the increasing difficulty in managing enterprise security efforts effectively.

1.15.3 Controls

Controls are defined as the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. They are the primary components to consider when developing an information security strategy. Controls can be physical, technical, or procedural. The choice of controls must be based on a number of considerations including ensuring their effectiveness, that they are not unduly expensive or restrictive to business activities, and what the optimal form of control will be.

1.15.3.1 IT Controls

The COBIT focus is on IT controls which may constitute the majority of those required in many organizations. Arguably, COBIT is one of the most developed and comprehensive approaches to determining control objectives for IT and subsequent implementation and management.

Control objectives are defined as "a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity."[16]

1.15.3.2 Non-IT Controls

The ISM must be aware that information security controls must be developed for non-IT-related information processes as well. This will include secure marking, handling and storage requirements for physical information. It must include considerations for handling and preventing social engineering. Environmental controls must also be taken into account, so that otherwise secure systems are not subject to being stolen, as has occurred in some well-publicized cases.

[14] Howard, Steven; *Strategy, Architecture and Communications Best Practices*, Gartner, 10 July 2002, *http://dataquest.com/DisplayDocument?doc_cd=108169*
[15] James, Greta A.; "Seven Architecture Management Best Practices," Gartner Group, 31 December 2002, *www.gartner.com*
[16] IT Governance Institute, COBIT 4.0, USA, 2005, *www.isaca.org/cobit*

1.15.3.3 Layered Defenses

Layering defenses, or defense in depth, is an important and effective concept in risk management and developing controls and countermeasures to limit adverse impacts of compromises. Excessive reliance on a single control is likely to create a false sense of confidence. For example, a company that depends solely on a firewall can still be subject to numerous attack methodologies. It should also be considered that education and awareness can create a human firewall that constitutes one critical layer of defense.

One approach to layering security is to review the functional elements that must be considered. This approach defines what each layer is designed to accomplish. See **figure 1.7**.

Figure 1.7—Defenses and Security Standards

Defenses Against System Compromise	Policies, Standards, Procedures,Technology
Prevention	Authentication Authorization Encryption Firewalls Data labeling/handling/retention Management Physical security Intrusion prevention Viruse scanning Personnel security Awareness and training
Containment	Authorization Data privacy Firewalls/security domains Network segmentation Physical security
Detection/notification	Monitoring Measurements/metrics Auditing/logging Honeypots Intrusion detection Virus dectection
Reaction	Incident response Policy/procedure change Additional security mechanisms New/better controls
Evidence collection/event tracking	Auditing/logging Management/monitoring Nonrepudiation Forensics
Recovery/restoration	Backups/restoration Failover/remote sites Business continuity/disaster recovery planning

1.15.4 Countermeasures

There are many definitions of countermeasures, but they generally agree with: "Countermeasures are the protection measures that reduce the level of vulnerability to threats."[17]

Countermeasures to threats should be considered from a strategic perspective. They can be passive or active but in many cases may be more effective and less constricting than controls might be. A countermeasure might consist of making the most sensitive information only accessible from a separate subnet not externally available. It might consist of changing to an inherently more secure operating system or preventing unsecured systems from connecting to the network.

1.15.5 Technologies

The past few decades have seen the development of numerous security technologies to address the ever-growing threats to information resources. Technology will be one of the cornerstones of an effective security strategy. The ISM must be familiar with how these technologies can serve as controls in achieving the desired state of security. Technology will, however, not compensate for management, cultural or operational deficiencies and the ISM is cautioned to not place excessive reliance on these mechanisms.

There are a number of security technologies and mechanisms that can play a critical role in the success of an organization's security strategy. These technologies are discussed in greater detail in chapter 3, Information Security Program(me) Management.

Some of the typical available security technologies include but are not limited to:
- Firewall technology
- User account administration
- Intrusion detection and intrusion prevention technology
- Antivirus technology
- Certificate authority technology (PKI)
- Biometric technology
- Encryption technology
- Privacy compliance technology
- Remote access technology
- Digital signature technology
- EDI and EFT technology
- VPN technology
- SET technology
- Forensics technology
- Monitoring technologies
- Log reading and correlation technologies
- Data labeling technologies
- Document and email content scanning technologies

A number of technical solutions exist that may be relevant to a particular strategy. Given the ongoing and rapid development of technology in this area, the prudent ISM will utilize available resources to stay current on the latest developments.

1.15.6 Personnel

Personnel security is an important area that the ISM must consider as a preventive means of securing an organization. Since the most costly and damaging compromises are usually the result of insider activities, the first line of defense is to try to ensure the trustworthiness and integrity of new and existing personnel. The limited traditional background checks can provide indicators of negative characteristics, but the extent of these checks may be constrained by privacy and other laws particularly in the European Union nations.

[17] "Physical Security Risk Analysis," July 2004, *http://security.lifesafety.ca/2004articles/2004sec0047.htm*

In addition, the extent and nature of background investigations should be relevant and proportional to the sensitivity and criticality of the requirements of the position held. An extensive background investigation of a receptionist might be considered an unwarranted privacy intrusion. Privacy regulations must be considered within the context of the relevant jurisdiction as regulations vary greatly in different countries. Nevertheless, consideration must be given to controls aimed at both preventing personnel likely to harm the organization from being employed and providing ongoing intelligence indicative of emerging or potential problems with existing staff.

Methods of tracking incidences of pilfering and theft should be developed and these events should be investigated when feasible and tracked. The appearance of what may be considered minor events may be indications of a more serious situation. It may also be an indicator of personnel that may be involved in illegal or improper activities.

If the organization's policy is that e-mail is not private and may be inspected by the company and employees have been properly made aware of this policy, it may be appropriate to consider monitoring e-mail of personnel that have been identified as potential problems. Legal protections vary on this type of monitoring and it is the responsibility of the security officer to understand the legal requirements of the jurisdiction involved.

It may also be prudent to develop an investigation and background check policy and standards that should be reviewed by the organization's legal and HR departments. These policies should also be reviewed by senior management for consistency with the organizations culture and governance approach.

1.15.7 Roles and Responsibilities

With the many tasks today's employees must complete, it is important that the strategy includes a mechanism that defines all security roles and responsibilities and incorporates them in employee job descriptions. Ultimately, if employees are compensated based on their adherence to meeting their job responsibilities, there is a better chance that security governance objectives will be achieved. Employee annual job performance and objectives can include security-related measurements.

The ISM should work with the personnel director to define security roles and responsibilities. The related competencies required for each job position should also be defined and documented.

1.15.8 Skills

The skills required to implement a security strategy are an important consideration. Choosing a strategy that utilizes skills already available, other elements being equal, is likely to be a more cost-effective option. A skills inventory will be important to determine the resources available in developing a security strategy. Proficiency testing may be useful to determine if the requisite skills are available or can be achieved through training.

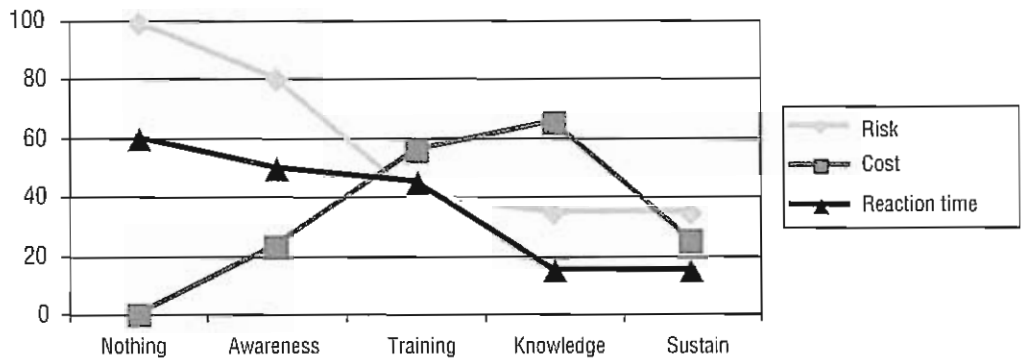
1.15.9 Awareness and Education

Training, education and awareness are vital in the overall strategy, as security is often weakest at the end-user level. It is here, as well, that one will consider the need for the development of methods and processes that enable the policies, standards and procedures to be more easily followed, implemented and monitored. A recurring security awareness program aimed at end users will reinforce the importance of information security and is now required for a number of sectors by law in some jurisdictions.

In most organizations, evidence indicates that the majority of personnel are not aware of security policies and standards even where they do exist. Awareness and training programs can provide for widespread acknowledgement that security is important to the organization. Since security relies heavily on individual compliance, it is important that a robust security awareness program be in place and is an element that must be considered in strategy development.

Studies have indicated that improving security awareness and training has in many cases resulted in the most cost-effective improvement in overall security. A large study performed by the US military in Europe is indicative and shown below in **figure 1.8**.

Figure 1.8—Impact of Security Training



Based upon direct experience with the US Military Regional Computer Emergency Response Team (RCERT) in Europe from 1994-2002, humans were the weakest link in the security chain. Security technology was purchased and implemented, but evidence indicated that the risk to information remained a human problem. Reduction of risk was achieved only after the RCERT initiated an awareness and training program that covered all 90,000 users and the 2000 IT staff personnel.

The graph depicts the relationship between risk and awareness program. As awareness and training of the personnel took place, the risk was reduced as they were taught the value of assets, the risks, and took actions to protect it. The personnel became aware, then trained on security issues and procedures, which allowed the RCERT to lower the reaction time when vulnerabilities occurred in the organizations. The cost of the program increased until the program was stabilized.[18]

Broadening and deepening the appropriate skills of security personnel through training can do a great deal to improve an organization's overall security effectiveness. The challenge is to determine what are the appropriate skills that need improvement to effectively protect against the seemingly endless array of security risks.

Finding employees with the necessary combination of security skills to be effective in today's ever-changing, diverse environments and complex regulatory climate can be difficult and expensive. One way some organizations attempt to insure all needed skills are available is to hire over-qualified people. The concern with this approach is that these individuals are costly to acquire and maintain and, failing to be challenged, are often dissatisfied with the position. This can lead to excessive employee turnover, unproductive attitudes or substandard performance.

Training for new or existing security personnel to equip them with the skills needed to meet specific existing and emerging security requirements can be more cost-effective. This is a strong argument for an ongoing program of training targeted to the needs of the organization and, at the same time, providing a career path for employees based on continuous improvement.

For training to be an effective option, however, it must be targeted to specific systems, processes and policies—the organization's unique and specific way of doing busines and the organization's unique security context. Anything less is likely to be inadequate, anything more wastes resources. Properly executed, this approach can seamlessly integrate into existing programs and initiatives, shore up areas of deficiency and align security processes with business processes.

[18] Sparks, Phillips M.; Litton/PRC, 2003, *www.prc.com*

1.15.10 Audits

Audits, both internal and external, are one of the main processes that are used to determine information security deficiencies from a control and compliance standpoint.

External audits are most often performed by the finance department and often do not find their way to information security. Since these audits can provide powerful monitoring tool for the ISM, it is important to ensure the security department has access to this information.

Under compliance provisions of various recent regulations, such as the US Sarbanes-Oxley Act, controls are required to be tested. It is important that the results of these tests are available to the ISM and should be required as part of strategy considerations.

1.15.11 Compliance Enforcement

Security violations are an ongoing concern for ISMs and it is important that procedures for handling them are developed. It is critical that there is senior management buy-in and backing for these procedures, especially in the area of enforcement. Security managers often find that the greatest compliance problems arise with management. If there is a lack of commitment and compliance in management ranks, it will be difficult if not impossible to enforce compliance across an organization.

The most effective approach to compliance in an organization where openness and trust are valued and promoted by management is likely to be a system of self-reporting and voluntary compliance, based on the understanding that security is clearly in everyone's best interest. This usually also requires these processes to be carefully thought out, clearly communicated and cooperatively implemented. How to accomplish this will be an element of strategy.

1.15.12 Threat Analysis

Threat analysis will be a component of risk analysis and the result will be a critical element of the strategy. The strategy must consider the types, nature and extent of threats in developing countermeasures and controls as well as the attributes of a security architecture.

1.15.13 Vulnerability Analysis

In most organizations, technical vulnerability assessments using scans are common. These can have a limited value for security strategy development. A comprehensive vulnerability assessment will, however, be important. This should include vulnerabilities in processes, technologies and facilities. Processes and facilities are frequently the most vulnerable components, yet because of the greater difficulty in performing assessments on them, also the least frequently assessed.

For the purposes of developing a strategy based on accurate information, it is critical that these assessments be performed. There is little security benefit for the organization to have a well-secured technical infrastructure, if it is being used to process fraudulent orders.

It is also of little value to the organization if technically secure servers are physically stolen because of inadequate environmental security.

1.15.14 Risk Assessment

While threat and vulnerability assessments are useful in their own right in considering the elements of security strategy, assessing the risk to the organization will also be required. While threats and vulnerabilities that pose no risk to the organization are not immediately significant, the ever-changing landscape ensures that this may not continue to be the case. In any event, to the extent that strategy development can address threats and vulnerabilities, it should do so as a matter of good practice.

For example, while it was recognized that the World Trade Center in New York, USA, was vulnerable to an aircraft being crashed into it and that there was a threat, the risk was considered low. If, as a practical matter, either the threat or the vulnerability had been addressed as a matter of course, the results would likely have been less-catastrophic.

The lesson learned is that every opportunity to reduce either threat or vulnerability should, as a matter of course, be taken. While vulnerabilities for which no threat exists poses no risk, it is all too likely that, at some point, a viable threat will emerge.

From a strategy point of view, there should be consideration of the several ways to address risk. For any given risk, this would include:
- Accept the risk
- Mitigate the risk
- Transfer the risk
- Cease the activity giving rise to the risk

Examples of risk transfer include insurance and indemnity agreements. It should be noted that, while risk can be transferred, generally responsibility can not.

1.15.15 Business Impact Assessment

Business impact is the bottom line of risk. Risks that cannot result in appreciable impact are obviously not important. Impact assessments are an important component of developing a strategy that addresses potential adverse impacts to the organization. This may be important, because it may turn out that it may be easier to reduce a potential impact than to mitigate a risk or reduce a vulnerability.

Business impact analysis must also be considered a requirement to determine the criticality and sensitivity of information. As such, it provides the basis for developing an approach to information classification and business continuity requirements.

1.15.16 Resource Dependency Analysis

Resource dependency is another perspective on the criticality of information resources. It can, to some extent, be used instead of an impact analysis to ensure the strategy takes due consideration of resources critical to business operations.

1.15.17 Outsourced Security Providers

Outsourcing is increasingly common both onshore and offshore as companies focus on core competencies and ways to cut costs. From an information security point of view, these arrangement can present a set of risks that may be difficult to quantify and potentially difficult to mitigate. Typically, both the resources and skills of the outsourced functions are lost to the organization, which may present a set of risks. Providers may operate on different standards and can be difficult to control. The security strategy should consider outsourced security services carefully to ensure that they either are not a critical single point of failure or that there is a viable backup plan in the event of service provider failure.

1.15.18 Other Organizational Support and Assurance Providers

When developing a security strategy, there are usually a number of support and assurance service providers within an organization that should be considered a part of information security resources. These can include a variety of departments including legal, compliance, audit, insurance, disaster recovery, physical security, training, project office, human resources and, in some cases, change management and quality assurance (QA) into a general assurance structure.

Typically, these assurance functions are not well integrated, if at all. Strategic considerations should include approaches to ensure that these functions operate seamlessly together to prevent gaps that may lead to security compromises.

1.16 STRATEGY CONTRAINTS

1.16.1 Legal and Regulatory Requirements

There are a number of legal and regulatory issues affecting information security that must be considered in developing a strategy. Information security is inevitably intertwined with questions of privacy, intellectual property and contractual law. Any effort to design and implement an effective information security strategy must be built on a solid understanding of the pertinent legal requirements and restrictions. Different regions in a global organization may be governed by conflicting legislation. An example of this is in the area of privacy legislation, which is strong in the EU and virtually nonexistent in Asia.

In some countries, thorough background checks may be performed on a new employee, but such background checks are illegal under laws in other countries. To address these situations, the global organization may need to establish different security strategies for each regional division, or it can employ a least-common denominator policy to be consistent.

There are also a number of legal and regulatory issues associated with Internet business, global transmissions and transborder data flows (e.g., privacy, tax laws and tariffs, data import/export restrictions, restrictions on cryptography, warranties, patents, copyrights, trade secrets, national security). These will vary depending upon the organization's location and result in constraints and boundaries on security strategies. Research into these areas must be undertaken in conjunction with legal and regulatory departments as well as any areas of the business that may be affected. Personnel safety is also the subject of regulations in many jurisdictions that the strategy must take into consideration.

1.16.1.1 Requirements for Content and Retention of Business Records

There are two main aspects that an information security strategy must take into consideration regarding the content and retention of business records and compliance:

- The business requirements for business records
- The legal and regulatory requirements for records

Business requirements may exceed the legal and regulatory requirements imposed by applicable legislating bodies due to the nature of the organization's business. Some organizations have business needs requiring access to data that are 10 or 20 years old or more. This can include customer records, patient records, engineering information and many others. As a rule, the retention strategy and subsequent policy should meet the minimum legal requirements in the applicable jurisdiction and industry.

Depending upon an organization's location and industry, regulatory bodies have requirements with which an organization must comply. Organizations may also need to consider common practices or guidelines developed by trade associations in developing records retention policies.

Regulations such as Sarbanes-Oxley have imposed various mandatory retention requirements for various types and categories of information regardless of storage medium. The strategy will require that the ISM stay current with these requirements and ensure compliance. Another legal requirement that should be considered is the lawful preservation order requirement to provide retention of specific data upon being served by law enforcement and other authorities.

1.16.2 Physical and Environmental Factors

There will inevitably be a variety of physical and environmental factors that will influence or constrain an information security strategy. The obvious ones will include such matters as capacity, space, environmental hazards, availability of infrastructure and so forth.

Others constraints that have on occasion been ignored include environmental hazards. The security strategy should make certain that provisions are made for the consideration of environmental hazards and adequate infrastructure capacity.

The strategy must also include a requirement of consideration for personnel and resource safety.

1.16.3 Ethics

The perception of ethical behavior by an organization's customers and the public at large can have a major impact on an organization and affect its share value. These perceptions are often influenced by location and culture, and an effective strategy will include ethical considerations in the areas of its operations.

1.16.4 Culture/Regional Variances

The internal culture of the organization must be taken into account in developing a security strategy. The culture in which the organization operates must also be considered. A strategy that is at odds with cultural norms will encounter resistance and make successful implementation difficult.

1.16.5 Costs

The development and implementation of a strategy will consume resources including time and money. Obviously, the strategy will need to consider the most cost-effective way it can be implemented.

Organizations often justify spending based on a project's value. With security, projects however, the avoidance of specific risks or compliance with regulations are generally the primary drivers.

Generally, a cost-benefit analysis is the most accepted approach and should be considered when developing a strategy.

An approach considered by many to be flawed is to consider the value of avoiding specific risks by estimating the potential losses incurred by a specific event multiplied by the probability of it occurring in a given year. This results in an annual loss expectation (ALE). The cost of a security program to preclude such an event can then be compared on a as a return on investment (ROI).

Many practitioners believe that ROI is not a good approach to justifying security programs. This is especially true for programs implemented for the purposes of regulatory compliance. For example, under Sarbanes-Oxley, enhanced penalties are prescribed for some violations consisting of long terms in the federal penitentiary for senior executives. The ROI on programs to prevent such penalties can be difficult to quantify.

Recently, the advances in single sign-on and user access provisioning technologies and procedures have resulted in savings in time and cost over traditional manual administration techniques, which may provide a reasonable basis for ROI calculations. There are a number of examples that compare the costs of traditional processes against the newer procedures, and these can be used in developing a business case.

1.16.6 Personnel

A security strategy must consider what resistance will be encountered during implementation. It can generally be expected that there will be resistance to significant changes as well as possible resentment against new constraints possibly viewed as making tasks more difficult or time consuming.

1.16.7 Resources

An effective strategy must consider not only available budgets but also the costs of new or additional technologies to be used. It must also consider the manpower requirements in design, implementation, operation and eventual decommisioning. Typically, the TCO must be developed for the full life cycle of technologies, processes and people.

1.16.8 Capabilities

The resources available to implement a strategy will include the known capabilities of the organization including expertise and skills. Obviously, a strategy that relies on demonstrated capabilities is more likely to succeed than one that does not.

1.16.9 Time

Time will be a major constraint in developing a strategy. There may be compliance deadlines that must be met or support for certain strategic operations such as a merger that must be accommodated. There may be windows of opportunity for particular business activities that will mandate certain timelines for implementation of certain strategies.

1.16.10 Risk Tolerance

The risk tolerance of the organization will play a major role in developing an information security strategy. While difficult to apply a yardstick to, there are a variety of methods to arrive at useful approximations. One method is to develop RTOs for critical systems. The shorter the times decided by appropriate managers, the greater the cost and the lower the risk tolerance. RTOs are based on a business impact or dependency analysis to determine allowable down times for various resources. Generally, the optimal point is reached when the cost of reducing RTOs is equal to the value derived from the operation of the resources.

1.17 IMPLEMENTING INFORMATION SECURITY GOVERNANCE

1.17.1 Gap Analysis—Basis for an Action Plan

Implementing a strategy will require one or more action plans. An analysis of the gap between the current state and the desired state for each defined metric identifies the requirements and priorities for a plan of action. A gap analysis will be required for various components of the strategy previously discussed, such as maturity levels, each control objective, each risk and impact objective, and so forth. This exercise may need to be repeated annually or more frequently to provide performance and goal metrics and to provide information on possible midcourse corrections needed in response to changing environments or other factors. A typical approach to gap analysis is to work backward from the endpoint to the current state and determine the intermediate steps needed to accomplish the objectives.

1.17.2 Policy Development

One of the most important aspects of the action plan to execute the strategy is to create or modify, as needed, policies and standards. Policies are the constitution of governance, standards are the law. Policies must capture the intent, expectations and direction of management. As a strategy evolves, it is vital that supporting policies are developed to articulate the strategy. For example, if the objective is to become ISO 17799 compliant over a three year period, then the strategy must consider which elements are addressed first, what resources are allocated, how the elements of the standard can be accomplished and so forth. The roadmap will show the steps and the sequence, dependencies, milestones, etc. The action plan is essentially a project plan to implement the strategy following the roadmap.

If the objective is ISO 17799 compliance, each of the relevant 10 domains and major subsections must be the subject of a policy. In practice, this can be effectively accomplished with about two dozen specific policies for even large institutions. Each of the policies is likely to have a number of supporting standards typically divided by security domains. In other words, a set of standards for a high security domain will be more stringent than the standards for a low security domain. Other standards may need to be developed for different business units depending on their activities and regulatory requirements.

The completed strategy provides the basis for creation or modification of existing policies. The policies should be directly traceable to strategy elements. If they are not, either the strategy is incomplete or the policy is incorrect. It should be apparent that a policy that contradicts the strategy will be counterproductive. The strategy is the statement of intent, expectations and direction of management. The policies must in turn be consistent with and support the intent and direction of the strategy.

Most organizations today have some information security policies. Typically, they have evolved over time usually created in response to a security problem or regulations and are often inconsistent and sometimes contradictory. These policies generally have no relationship to a security strategy (if one exists) and only a coincidental relation to business activities.

Policies are one of the primary elements of governance. They must be properly created, accepted and validated by the board and executive management, and broadly communicated throughout the organization. There may be occasions where subpolicies must be created to address unique situations separate from the bulk of the organization. An example would be where a separate part of the organization is performing highly classified military work. Policies that reflect the specific security requirements for classified defense work may exist as a separate set.

There are several attributes of good policies that should be considered:
- Security policies should be an articulation of a well-defined information security strategy and capture the intent, expectations and direction of management.
- Each policy should state only one general security mandate.
- Policies must be clear and easily understood by all affected parties.
- Policies should rarely be more than a few sentences long.
- There should rarely be a reason to have more than two dozen policies.

Most organizations have created security policies prior to developing a security strategy. Indeed, most organizations still have not developed a security strategy. In many cases, policy development has not followed the approach defined above and has been *ad hoc* in a variety of formats. Often, these policies have been written to include standards and procedures in lengthy, detailed documents compiled in large dusty volumes relegated to the stock room.

In many cases, however, especially in smaller organizations, effective practices have been developed that may not be reflected in written policies. Existing practices that adequately address security requirements may usefully serve as the basis for policy and standards development. This approach will minimize organizational disruptions, communications of new policies, and resistance to new or unfamiliar constraints.

1.17.3 Standards Development

Standards are a powerful security management tool. They set the permissible bounds for procedures and practices, of technology and systems, and for people and events. Properly implemented, they are the law to the constitution of policy. They provide the measuring stick for policy compliance and a sound basis for audits. They govern the creation of procedures and guidelines.

Standards are the predominant tool for implementing effective security governance and must be "owned" by the ISM. They must be carefully crafted to provide only necessary and meaningful boundaries without unnecessarily restricting procedural options. Standards serve to interpret policies and it is important that they reflect the intent of policy. Standards must be unambiguous, consistent and precise as to scope and audience. Standards must exist for the creation of standards and policies including format, content and required approvals.

Standards must be disseminated to those governed by them as well as those impacted. Review and modification processes must be developed as well. Exception processes must be developed for standards not readily attainable for technological or other reasons. A process for implementing compensatory controls must be developed for out-of-compliance situations.

1.17.4 Training and Awareness

An effective action plan to implement strategy must consider an ongoing program of security awareness and training. In most organizations, evidence indicates that the majority of personnel are not aware of security policies and standards even where they do exist. Even today, many organizations do not have formal security policies much less a security strategy. However, the increasingly restrictive regulatory requirements for most organizations is likely to improve the situation over the next few years. The most significant of these regulations include the US Sarbanes-Oxley Act for public companies, Financial Services Authority (FSA) in the UK for financial institutions, BASEL II for global financial organizations and the local articulation of the EU Privacy Directives for most of Europe and others. There are a number of other regulations dependant on sector and geography that must be considered when applicable.

1.17.5 Action Plan Metrics

1.17.5.1 KPIs, CSFs, KGIs

The plan of action to implement the strategy will require methods to monitor and measure progress and the achievement of milestones. As with any project plan, progress and costs should be monitored on an ongoing basis to determine conformance with the plan and to allow midcourse corrections on a timely basis. There are likely to be a variety of near-term goals each requiring resources and a plan of action to achieve it.

Each plan of action will require developing appropriate monitoring and metrics such as developing a set of KPIs, defining critical success factors (CSFs) and setting KGIs. For example, the plan of action to achieve regulatory compliance may require among other things:

- A detailed analysis by competent legal personnel to determine regulatory requirements for affected business units
- Knowledge of current state of compliance
- Definition of required state of compliance

Possible monitoring and metrics for each might include the following.

Key performance indicators may include:

- Detailed compliance action plans
- Achieving compliance milestones

Critical success factors may include:
- Understanding resources that will be affected
- Modifying or developing suitable controls
- Determining and committing resources to accomplish required changes

Key goal indicators may include:
- Achieving compliance mandates
- Independent compliance assurance

1.18 INTERMEDIATE IMPLEMENTATION GOALS

For most organizations, a variety of specific near-term goals that align with the overall information security strategy can be defined readily. If the objectives of the security strategy ultimately require compliance with defined portions of ISO 17799, then an example of a near-term 12-month action (or tactical) plan may state:
- Each business unit must identify current applications in use
- Twenty-five percent of all stored information must be reviewed to determine ownership, criticality and sensitivity
- Each business unit will complete a BIA for information resources to identify critical resources
- Business units must achieve regulatory compliance
- All security roles and responsibilities must be defined
- A process will be developed to ensure business process linkages
- A comprehensive risk assessment must be performed for each business unit
- All users must be educated on an acceptable use policy
- All policies must be reviewed and revised as necessary
- Standards must exist for all policies

Near-term goals and milestones will be required as part of the action plans; however, the entire 'desired state' objectives should be defined for the long term to maximize potential synergies and ensure that no short- or intermediate-term action plans are not aligned with the end goals. For example, a tactical solution that will need to be replaced because it will not integrate into the overall plan is likely to be more costly than one that will.

It is important that the strategy and long-range plan serve to integrate near-term tactical activities. This will counter the tendency to implement point solutions that are typical of the crisis mode of operation in which many security departments find themselves. As many security managers have discovered, numerous unintegrated solutions implemented in response to a series of crisis over a period of years become increasingly costly and difficult to manage.

1.19 INFORMATION SECURITY PROGRAM OBJECTIVES

Implementing the strategy with an action plan will result in an information security program. The program is essentially the project plan to implement some part or parts of the strategy.

Once implemented, the objective of the information security program is: "Protecting the interests of those relying on information, and the processes, systems and communications that handle, store and deliver the information, from harm resulting from failures of availability, confidentiality and integrity."[19]

While emerging definitions are adding concepts such as information usefulness and possession (the latter to cope with theft, deception and fraud), the networked economy certainly has added the need for trust and accountability in electronic transactions.

[19] IT Governance Institute, *IT Controls for Sarbanes-Oxley*, USA, 2003, *www.isaca.org/cobit*

For most organizations, the security objective is met when:
- Information is available and usable when required and the systems that provide it can appropriately resist attacks (availability)
- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is protected against unauthorized modification (integrity)
- Business transactions as well as information exchanges between enterprise locations or with partners can be trusted (authenticity and nonrepudiation)

The relative priority and significance of availability, confidentiality, integrity, authenticity and nonrepudiation vary according to the data within the information system and the business context in which they are used. For example, integrity is especially important relative to management information due to the impact that information has on critical strategy-related decisions. Confidentiality may be the most important based on regulatory or legal requirements regarding personal financial or medical information or to protect trade secrets.

It is important to understand that these concepts apply equally to electronic systems as well as physical systems. Confidentiality, for example, is as much at risk from social engineering or dumpster diving, as it is from a successful external attack. Integrity of information can be compromised a least as easily from forged physical inputs to the system as from electronic compromise.

It must also be considered that the majority of significant losses occur from insiders and not from external attacks. The result is that controls used to detect anomalies and ensure integrity of systems must be equally concerned with nontechnical attacks by insiders.

1.20 CHAPTER 1 GLOSSARY

Acceptable use policy
A policy that establishes an agreement between users and the organization and defines for all parties ranges of use that are approved before gaining access to a network or the Internet

Access control
The set of rules and procedures implemented within hardware and software to provide for the identification of users, the granting and denying of access, the recording of access attempts, and the administrative tools necessary to manage and monitor access activities

Access rights
Permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy

Accountability
The ability to map a given activity or event to the responsible party to make the individual accountable for his/her actions

Administrative controls
The actions or controls dealing with operational effectiveness, efficiency and adherence to regulations and management policies

Application controls
Manual or programmed activities intended to ensure the completeness and accuracy of records and the validity of entries made. The objective of application controls, either manual or programmed, is to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from manual and programmed processing.

Audit trail
A series of records either in hard copy or in electronic format that provide a chronological record of user activity and other events that show the details of user and system activity. Audit trails can be used to document when users log in, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred.

Authentication
The verification of the authenticity of a person or system requesting access to a resource to establish their legitimacy before access to the requested resource is granted. During the authentication process, the user enters a name or account number (identification) and password (authentication).

Availability
Ensuring that information systems and data are ready for use when they are needed; often expressed as the percentage of time that a system can be used for productive work

COBIT
Control Objectives for Information and related Technology, the international set of IT control objectives published by the IT Governance Institute

Confidentiality
The protection of sensitive or private information from unauthorized disclosure

Corporate governance
A set of responsibilities and practices, exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are met, ascertaining that risks are managed appropriately and verifying that the enterprises resources are used responsibly

COSO
A report titled *Internal Controls—An Integrated Framework* sponsored by the Committee of Sponsoring Organizations of the Treadway Commission in 1992. It provides guidance and a comprehensive framework of internal controls for all organizations.

Data classification
The assignment of a level of sensitivity to data that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the organization.

Decentralization
The process of distrubiting computer processing to different locations in an organization

Discretionary access control (DAC)
A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Dual control
A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource

Guidelines
A suggested action or recommendation related to an area of information security policy that is intended to supplement a procedure. The implementation of guidelines is encouraged but not enforced.

Information security governance
The leadership organizational structures and processes that safeguard information

Information security program
The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis

Integrity
The accuracy, completeness and validity of information in accordance with business values and expectations

ISO/IEC 17799
Originally released as part of the British Standard for Information Security in 1999 as the Code of Practice for Information Security Management, in October 2000 it was elevated by the International Organization for Standardization (ISO) to an international code of practice for information security management. This standard defines information confidentiality, integrity and availability controls in a comprehensive information security management system.

Mandatory access control (MAC)
A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf

Monitoring policy
Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted

Nonrepudiation
Assurance that a party cannot later deny originating data. It is the provision of proof of the integrity and origin of the data and can be verified by a third party. A digital signature can provide nonrepudiation.

Privacy
Freedom from unauthorized intrusion or disclosure of information about individuals

Procedures
A detailed description of the steps necessary to perform specific operations in conformance with applicable standards; a portion of a security policy that states the general process that will be performed to accomplish a security goal

Security metrics
A standard of measure used to monitor information-security-related activity and evaluate the performance of security-related programs

Standards
Definition of the metrics used to determine the correctness of a thing or process; a set of rules or specifications that, when taken together, define a software or hardware device. A standard is also an acknowledged basis for comparing or measuring something.

Steering committee
A management committee assembled to sponsor and manage various projects such as an information security program

1.21 CHAPTER 1 SAMPLE QUESTIONS

CISM exam questions are developed with the intent of measuring and testing practical knowledge in information security management. All questions are multiple choice and are designed for one best answer. Every CISM question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement.

In some instances, a scenario or a description problem may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided.

Many times a CISM examination question will require the candidate to choose the **MOST** likely or **BEST** answer. In every case the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked and how to study to gain knowledge of what will be tested will go a long way toward answering them correctly.

The sample questions contained below are designed to depict the type of question format on the CISM examination.

1. A security strategy is important for an organization **PRIMARILY** because it provides:

   A. a basis for determining the best logical security architecture for the organization.
   B. management intent and direction for security activities.
   C. provides users guidance on how to operate securely in everyday tasks.
   D. helps IT auditors ensure compliance.

2. The **MOST** important reason to make sure there is good communication about security throughout the organization is:

   A. to make security more palatable to resistant employees.
   B. because people are the biggest security risk.
   C. to inform business units about security strategy.
   D. to conform to regulations.

3. The regulatory environment for most organizations mandates a variety of security-related activities. It is **MOST** important that the ISM:

   A. rely on corporate counsel to advise which regulations are relevant.
   B. stay current with all relevant regulations and request legal interpretation.
   C. involve all impacted departments and treat regulations as just another risk.
   D. ignore many of the regulations that have no teeth.

4. The **MOST** important consideration in developing security policies is that:

   A. they are based on a threat profile.
   B. they are complete and no detail is left out.
   C. management signs off on them.
   D. all employees read and understand them.

5. The **PRIMARY** security objective in creating good procedures is:

A. to make sure they work as intended.
B. that they are unambiguous and meet the standards.
C. that they be written in plain language.
D. that compliance can be monitored.

6. On which of the following would an information security strategy place the **MOST** emphasis?

A. Business goals and objectives
B. Technology plans and deliverables
C. Industry best practices
D. Security metrics

7. Which of the following **BEST** describes an information security department's strategic planning process?

A. The department will have either short-range or long-range plans depending on the organization's broader plans and objectives.
B. The department's strategic plan must be time and project-oriented, but not so detailed as to address and help determine priorities to meet business needs.
C. Long-range planning for the department should recognize organizational goals, technological advances and regulatory requirements.
D. Short-range planning for the department does not need to be integrated into the long-range plans of the organization since technological advances will drive the department plans much quicker than organizational plans.

1.22 CHAPTER 1 ANSWERS TO SAMPLE QUESTIONS

1. **B** A security strategy will define management intent and direction for a security program. It should also be a statement of how security aligns with and supports business objectives and provides the basis for good security governance.

2. **B** Communications are important to ensure continued awareness of security policies and procedures. Security failures are in the great majority of instances directly attributable to lack of awareness or failure of employees to follow procedures.

3. **C** While it can be useful to stay abreast of all current and emerging regulations, it can become a full time job by itself. Departments such as human resources, finance and legal are most often subject to new regulations and must therefore be involved in determining how best to meet the existing and emerging requirements. Treating regulations as another risk puts them in the proper perspective and the mechanisms to deal with them should already exist.

4. **A** Relevant security policies must be based on viable threats to the organization prioritized as to potential impact on the business. Where there is no threat, there is no risk and the strictest policies should be developed for the areas of greatest risk. This ensures that proportionality is maintained and great effort is not expended on unlikely threats or threats with trivial impacts.

5. **B** All of the answers are obviously important, but the first criteria must be to ensure that there is no ambiguity in the procedures and that, from a security perspective, they meet the applicable standards and comply with policy.

6. **A** A security strategy must support business goals and objectives and be aligned with the overall business strategy. Security exists to provide assurance that business processes operate as intended and to manage risks to those processes to acceptable levels.

7. **C** Long-range planning for the information security department should recognize organizational goals, technological advances and regulatory requirements. Typically, the department will have both long-range and short-range plans that are consistent and integrated with the organization's plans. These plans must be time- and project-oriented, as well as address the organization's broader plans for attaining its goals.

1.23 CHAPTER 1 REFERENCES

Ahuja, Jay; "Identity Management: A Business Strategy for Collaborative Commerce," *Information Systems Control Journal*, vol. 6, 2003, p. 49-53

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, *Privacy Framework Principles and Criteria*, USA and Canada, 2004

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants, *SysTrust Principles and Criteria for Systems Reliability V2.0*, USA and Canada, 2001

Asian School of Cyber Laws, *www.asianlaws.org/infosec/archives/08_02_oecd.htm* (Contains references to cyberlaws that are in force in Asia)

Australian Computer Emergency Response Team, *www.auscert.org.au* (Contains security guidelines from this Australian Emergency Organization)

British Standards Institute, BS 7799 Security Standard, "Audit & Compliance," *www.riskserver.co.uk/bs7799*

Business Roundtable, "Building Security in the Digital Resource: An Executive Resource," November 2002, *www.businessroundtable.org*

Business Roundtable, "Information Security Addendum to Principles of Corporate Governance," April 2003, *www.businessroundtable.org*

Carnegie Mellon University, *Governing for Enterprise Security*, USA, June 2005

European Union (EU), *EU Privacy Directive*, 1995

Federal Financial Institution's Examination Council, *IT Examination Handbook: Management,* Federal Financial Institution, June 2004, *www.ffiec.gov/ffiecinfobase/html_pages/it_01.html*

Fiedler, Andreas E.; "On the Necessity of Management of Information Security: The Standard ISO17799 as International Basis," Northwest Controlling Corporation Ltd., 2002, *www.noweco.com/wp_iso17799e.htm* (Contains an overall description of ISO 17799.)

The GASSP Committee at MIT, *http://web.mit.edu/security/www/GASSP/gassp021.html*

General Accounting Office, *Federal Information System Controls Audit Manual*, USA, January 1999

General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, USA, 1996

Gerdes, Michael; "An Exploration of Global Perceptions of Security and Privacy," *Information Systems Control Journal*, vol. 6, 2002, p. 27-30

Hallawell, Arabella; *Gartner Global Security and Privacy Best Practices,* Gartner Analyst Reports, 16 March 2004, *www.csoonline.com/analyst/report2332.html*

Information Systems Security Association (ISSA), *The Generally Accepted Information Security Principles* (GAISP)

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

Information Security Forum, *The Standard of Good Practice for Information Security, Version 4*, UK, March 2003

Information Technology Committee, *International Information Technology Guidelines—Managing Security of Information*, International Federation of Accountants (IFAC), January 1998

Institute of Internal Auditors (IIA), *Information Security Governance: What Directors Need to Know*, 2001

Institute of Internal Auditors (IIA), *Information Security Management and Assurance: A Call to Action for Corporate Governance*, 2000

Institute of Internal Auditors (IIA), *Presenting the Information Security Case to the Board of Directors*, 2001

International Federation of Accountants, *Managing Security of Information*, USA, 1998

International Organisation for Standardisation (ISO), "Code of Practice for Information Security Management," ISO 17799, Switzerland, 2005

IT Governance Institute, CobiT 4.0, USA, 2005, *www.isaca.org/cobit* (Source of widely accepted control objectives)

IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2001, *www.itgi.org*

KPMG, *Creating Stakeholder Value in the Information Age: The Case for Information Systems Governance*, 2004, *www.kpmg.co.uk/services/ras/irm/isg.cfm*.

National Cyber Security Partnership, *www.cyberpartnership.org/init-governance.html*

National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), USA, *www.csrc.nist.gov*

National Institute of Standards and Technology (NIST), "Recommended Security Controls for Federal Information Systems," NIST 800-53, USA, 2005, *http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf*

Organisation for Economic Co-Operation and Development, *www.oecd.org* (An international organization providing guidance and standards based on economic impact)

Organization for Economic Co-operation and Development (OECD), *Guidelines for the Security of Information Systems,* France, 2002

Organization for Economic Co-operation and Development (OECD), *Guidelines for the Security of Information Systems and Networks—Towards a Culture of Security*, 2003

Pironti, John P; "Key Elements of an Information Security Program," *Information Systems Control Journal*, vol. 1, 2005, p. 23-28

Ross, Steven J.; "Why Passwords Persist," *Information Systems Control Journal*, vol. 1, 2001, p. 13-14

Scammell, Tim; "Security Architecture: One Practitioner's View," *Information Systems Control Journal*, vol. 1, 2003, p. 24-28

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

Schreider, Tari; "Privacy Is in the Eye of the Beholder," ***Information Systems Control Journal*****, vol. 6, 2003, p. 46-48**

Thorp, Carl; "Implementing ISO 17799: Pleasure or Pain?," ***Information Systems Control Journal*****, vol. 4, 2004, p. 25-26**

Tongia, Rahul; Kanika Jain; "Investing in Security—Do Not Rely on FUD," ***Information Systems Control Journal*****, vol. 6, 2003, p. 27-28**

US Computer Emergency Readiness Team, *www.us-cert.gov/resources.html*

Wang, George; "Strategies and Influence for Information Security," ***Information Systems Control Journal*****, vol. 1, 2005,** ***www.isaca.org/jonline***

Chapter 2:

RISK MANAGEMENT

2.1 DEFINITION

The systematic application of management policies, procedures and practices to the tasks of identifying, analyzing, evaluating, treating and monitoring risk

2.2 OBJECTIVE

The objective of risk management is to identify, quantify and manage information security risks to achieve business objectives through a number of tasks utilizing the ISM's knowledge of key risk management techniques.

This job practice area represents 21 percent of the CISM examination (approximately 42 questions).

2.3 TASKS

There are five (5) tasks within this job practice area:
1) Develop a systematic, analytical and continuous risk management process.
2) Ensure that risk identification, analysis and mitigation activities are integrated into life cycle processes.
3) Apply risk identification and analysis methods.
4) Define strategies and prioritize options to mitigate risk to levels acceptable to the enterprise.
5) Report significant changes in risk to appropriate levels of management on a periodic and event-driven basis.

2.3.1 Knowledge Statements

1) Knowledge of information resources used in support of business processes
2) Knowledge of information resource valuation methodologies
3) Knowledge of information classification
4) Knowledge of the principles of development of baselines and their relationship to risk-based assessments of control requirements
5) Knowledge of life-cycle-based risk management principles and practices
6) Knowledge of threats, vulnerabilities and exposures associated with confidentiality, integrity and availability of information resources
7) Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events
8) Knowledge of use of gap analysis to assess generally accepted standards of good practice for information security management against current state
9) Knowledge of RTOs for information resources and how to determine RTOs
10) Knowledge of RTOs and how they relate to business continuity and contingency planning objectives and processes
11) Knowledge of risk mitigation strategies used in defining security requirements for information resources supporting business applications
12) Knowledge of cost-benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels
13) Knowledge of managing and reporting status of identified risks

2.3.2 Relationship of Tasks to Knowledge Statements

The task statements are what the CISM candidate is expected to know how to do. The knowledge statements delineate what the CISM candidate is expected to know in order to perform the tasks.

The task and knowledge statements are approximately mapped in **figure 2.1** insofar as it is possible to do so. Note that although there is often overlap; each task statement will generally map to several knowledge statements.

Figure 2.1—Knowledge and Task Statements Mapping

Task Statements	Knowledge Statements
1. Develop a systematic, analytical and continuous risk management process.	1. Knowledge of information resources used in support of business processes 2. Knowledge of information resource valuation methodologies 3. Knowledge of information classification 4. Knowledge of life-cycle-based risk management principles and practices 7. Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events 8. Knowledge of the use of gap analysis to assess generally accepted standards of good practice for information security management against current state 9. Knowledge of RTOs for information security resources and how to determine RTOs 12. Knowledge of cost-benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels
2. Ensure that risk identification, analysis and mitigation activities are integrated into life cycle processes.	4. Knowledge of the principles of development of baselines and their relationship to risk-based assessments of control requirements 5. Knowledge of life-cycle-based risk management principles and practices
3. Apply risk identification and analysis methods.	4. Knowledge of the principles of development of baselines and their relationship to risk-based assessments of control requirements 6. Knowledge of threats, vulnerabilities and exposures associated with confidentiality, integrity and availability of information resources 7. Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events 8. Knowledge of the use of gap analysis to assess generally accepted standards of good practice for information security management against current state 9 Knowledge of RTOs for information security resources and how to determine RTOs 10. Knowledge of RTOs and how they relate to business continuity and contingency planning objectives and processes 12. Knowledge of cost-benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels

Figure 2.11—Knowledge and Task Statements Mapping (*cont.*)	
Task Statements	**Knowledge Statements**
4. Define strategies and prioritize options to mitigate risk to levels acceptable to the enterprise.	2. Knowledge of information resource valuation methodologies 3. Knowledge of information classification 6. Knowledge of threats, vulnerabilities and exposures associated with confidentiality, integrity and availability of information resources 7. Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events. 9 Knowledge of RTOs for information security resources and how to determine RTOs 12. Knowledge of cost-benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable level
5. Report significant changes in risk to appropriate levels of management on both a periodic and event-driven basis.	4. Knowledge of the principles of development of baselines and their relationship to risk-based assessments of control requirements 6. Knowledge of threats, vulnerabilities and exposures associated with confidentiality, integrity and availability of information resources 7. Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events 8. Knowledge of the use of gap analysis to assess generally accepted standards of good practice for information security management against current state 12. Knowledge of cost-benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels 13. Knowledge of managing and reporting status of identified risks

2.4 RISK MANAGEMENT OVERVIEW

Risk management is the process of ensuring that the impact of threats exploiting vulnerabilities is within acceptable limits at an acceptable cost. In practical business terms, it means that risks are managed to a level that does not materially impact the business process, that it provides an acceptable level of assurance and predictability to the desired outcomes of any important organizational activity. It is a fundamental organizational function, since risk is inherent in all activities. The relevance and criticality of information today gives rise to the necessity for managing information risks in addition to the multitude of other risks with which an organization is faced.

The foundation for effective risk management is a comprehensive risk assessment combined with a BIA. Failing to understand the nature and extent of risks to information resources and the potential impacts on the organization's activities, it will not be possible to devise a relevant risk management program. In turn, a BIA will not be possible without information asset classification or, in the less-desirable alternative, a business dependency evaluation to determine criticality and sensitivity.

If the organization has established information security governance as detailed in chapter 1, Information Security Governance, both risk and business impact assessments and analyses are fundamental prerequisites to developing a meaningful security strategy. However, in the majority of organizations, information security governance is just beginning to develop and risk management is a necessity that must be addressed regardless of the state of governance. At a high level, risk management is accomplished by balancing risk exposure against mitigation costs and implementing appropriate countermeasures and controls.

Controls are defined as the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. They are one of the primary components considered when developing the implementation plan for an information security strategy. Controls can be physical, technical, contractual or procedural.

Countermeasures can be any process that serves to reduce threats or vulnerabilities. Countermeasures can range from rearchitecting or reengineering processes to reduce or eliminate inherent vulnerabilities to offering financial rewards for information leading to the arrest of perpetrators of attacks as a means to reduce threats. In the same manner, they can be physical, technical, contractual or procedural.

Risk management forms the basis of the security decisions and projects that are undertaken. Since these decisions typically have major financial implications, and can require changes across the entire organization, it is imperative that executive management has bought into the process and fully understands and agrees with the results of the program. In some organizations, the information security risk management program is integrated into its existing risk management framework.

An effective risk management program is complex and encompasses the entire organization. Experience shows that it can become a very time-consuming task with significant cost implications. In designing and implementing a risk management program, it is critical to involve executive management from the onset and ensure that they are an integral part of the entire process. It must also be remembered that the program is a means to support business activities and provide assurance of desired outcomes and not an end in itself.

It may be useful for the security manager to be aware that risk management means different things to different people in the organization. For example, the auditors view may be that it means the prevention of loss, whereas an insurance manager might define it as cost-effective risk financing.

The ISM should also understand that risk management must operate at multiple levels includingthe operational level, the project level and the strategic level.

Risk is the probability of an event causing financial loss or damage to the company, its staff, assets or general reputation. A summary of this concept is shown in the following equations:
Total risk = Sum (Threats x Vulnerabilities x Asset Values)

This conventional manner of expressing risk is the subject of considerable controversy for several reasons. One is that not all threats can ever be known and can rarely be quantified. The probability of threats manifesting can generally not be determined. Many practitioners also contend that risk cannot be reduced as would be indicated by this formula. The contention is that reducing one risk merely increases another by the same amount or the risk is a constant that is only subject to management. Whatever the case, it is useful to understand the basic notion that more threats meeting more vulnerabilities will increase the likelihood that there will be adverse consequences or impacts and the greater the value of the assets, the greater the financial impact.

2.4.1 The Importance of Risk Management

Risk management is a fundamental function of information security. It provides the rationale and justification for virtually all information security activities. Information security exists to manage the risks to confidentiality, integrity and availability. While information security can be cast in the light of being a business enabler, functionally it enables business activities by mitigating or managing risks to reasonably predictable levels acceptable to the activity being undertaken. Without determining the risks, it is not possible to determine the potential cost/benefit of a particular activity.

2.4.2 Outcomes of Risk Management

Effective risk management serves to reduce the incidence of significant adverse impacts on an organization's operations. It provides a level of predictability that supports the organization's ability to operate profitably.

As stated in chapter 1, Information Security Governance, one of the outcomes of good governance is risk management, i.e., executing appropriate measures to mitigate risks and reduce potential impacts on information resources to an acceptable level and providing a:
- Collective understanding of the organization's threat, vulnerability and risk profile
- Understanding of risk exposure and potential consequences of compromise
- Awareness of risk management priorities based on potential consequences
- Risk mitigation sufficient to achieve acceptable consequences from residual risk
- Risk acceptance/deference based on an understanding of the potential consequences of residual risk

2.5 EFFECTIVE INFORMATION SECURITY RISK MANAGEMENT

As in all aspects of effective information security risk management activities must be supported on an ongoing basis by senior management. The tone at the top must be conducive to good security to lend credibility and impetus to risk management efforts. Even the best designed and implemented controls will not function as intended to protect an organization's information assets if operations are conducted by careless, indifferent or untrained personnel. A culture of quality coupled with senior management commitment to effective risk management is required to achieve the objectives of the program.

In addition, personnel must understand their responsibilities and be trained in applicable control procedures. Compliance must be tested and enforced on a consistent basis. Efforts must be made to integrate all risk management functions to ensure the continuity and comprehensiveness of risk management activities across the enterprise and provide an adequate level of assurance to business processes.

The basic steps in developing a risk management program are:
- Establish the context and purpose.
- Identify assets, asset owners and asset value.
- Classify assets.
- Identify threats and vulnerabilities.
- Determine risks.
- Assess impacts.
- Treat risks.
- Educate users.
- Monitor and review.
- Communicate and consult.

The first step is to determine the organization's purpose for creating a risk management program. The program's purpose may be to reduce the impacts of Internet-based attacks and accidents or it could be to ensure compliance with regulatory requirements.

By determining its intention before initiating risk management planning, the organization can evaluate the results to determine the effectiveness of the program. Each organization has a different tolerance or appetite for the amount of risk that it considers to be acceptable. This is a business decision based more on judgment rather than any specific quantitative measures. Typically, executive management, with the board of directors, sets the tone for the risk management program. This tone-at-the-top is an important component of management's responsibility for corporate governance. Also, a top-down approach is generally more effective than a bottom-up approach, where lower-level managers attempt to influence the organization. Employees often look to senior management in determining which issues deserve the highest priority.

The second step is to designate an individual or team responsible for developing and implementing the organization's risk management program. While the team primarily is responsible for the risk management plan, a successful program requires the integration of risk management within all levels of the organization. Operations staff and board members (through an oversight or steering committee) should assist the risk management committee in identifying risks and developing suitable loss-control and intervention strategies. Of overriding importance is that the risk management program be properly aligned with the strategy and direction of the business. For this reason, it is vital that participation include representatives from all key business units. The process should be business-driven and not technology-driven.

2.5.1 Roles and Responsibilities

Information security risk management is an integral part of security governance and it is the responsibility of the board of directors or the equivalent to ensure that these efforts are visible. Periodic reports on the efforts and effectiveness of risk management activities should be required.

Executive management must ensure adequate resources and support for risk management activities and should receive status reports on a periodic and event-driven basis. Management must be involved in and sign off on acceptable risk levels as well as risk management objectives.

A steering committee comprised of major stakeholders as defined in chapter 1, Information Security Governance, must set risk management priorities and define risk management objectives in terms of supporting business strategy. The committee should also be charged with developing levels of acceptable risk for various business processes to be presented to senior management for agreement and sign off. Defining levels of acceptable risk and obtaining senior management support is an essential condition for effective risk management

The ISM is responsible for developing, implementing and managing the information security risk management program to meet the defined objectives. The ISM must also take responsibility for maintaining liaisons with other risk management providers and assurance activities in the organization to promote integration of activities to provide an effective level of business process assurance.

2.6 INFORMATION SECURITY RISK MANAGEMENT CONCEPTS

2.6.1 Concepts

Overall risk management in most organizations is provided by one or more separate departments. Knowledge of the subject matter is, however, required to be effective and as a consequence risk management of information security falls to the ISM. Many other aspects of risk management that may not fall under the purview of the ISM may nevertheless impact information security and it is important that roles and responsibilities are clearly defined.

Threat management concepts important for information security management include:
- Threats
- Vulnerabilities
- Exposures
- Risks
- Impacts

- Controls
- Countermeasures
- Resource valuation
- Information asset classification
- Criticality
- Sensitivity
- Redundancy
- Robustness and resilience
- Hot, warm and cold sites
- RTOs
- RPOs
- Incident response
- Business case development
- Project management
- Baselines
- Security technologies
- Governance
- Strategies
- Policies, standards and procedures

2.6.2 Technologies

Security risk management technologies important for information security management include:
- Application security measures
- Physical security measures
- Logical access controls
- Network access controls
- Firewalls
- Intrusion detection/prevention
- Wireless security
- Platform security
- Encryption technologies
- Antivirus/malware neutralization
- Security architectures
- PKIs

2.7 IMPLEMENTING RISK MANAGEMENT

As a part of planning a risk management program, the ISM should determine all other risk management activities in the organization to integrate functions and leverage existing activities. Most larger organizations have a risk management function that deals with activities typically related to physical risks. In the case of financial institutions, there is also typically a manager dealing with credit risk. Other departments or roles, such as human resources and privacy officers, and compliance functions, such as audit, typically manage risks either formally or informally. To be effective, it is critical that mechanisms be put in place to ensure good communication with other risk management and assurance functions. This is to ensure that otherwise effective information security risk management is not bypassed or subverted by the lack of effective processes in other domains. It also prevents duplication of efforts and minimizes gaps in assurance functions.

2.7.1 Risk Management Process

Developing a systematic, analytical and continuous risk management process is critical to any successful security program that, to be effective, must be implemented as a formal process. Determining the correct or appropriate level of security is dependent on the potential risks that an organization faces. These risks can be unique to each organization and one should be careful not to over generalize by applying risk factors across industries or regions. Furthermore, the challenge of having an adequate information security program is made more challenging by organizational, technological and business/operational change. Risk management should be a continuous and dynamic process to ensure that changing threats and vulnerabilities are addressed in a timely manner.

In addition, processes must be developed to monitor the status of security controls and countermeasures to determine their ongoing effectiveness.

Organizations generally use the following techniques in this process:
- Identifying and gaining authorization for an organization's risk profile
- Understanding and documenting the nature and extent of risk exposures
- Identifying risk management priorities commonly achieved through:
  - Identifying the likelihood of threats
  - Identifying the quantitative (monetary) and qualitative (effect) value of the critical information/asset that the security program is in place to protect
  - Determining the impact to the business if a vulnerability is successfully exploited

The ISM should set up a regular process whereby a formal risk assessment is performed. Ensuring that there are measurements (metrics) in place to assess the risk and the effectiveness of security measures is part of the ISM's ongoing responsibility. The ISM should also employ various continuous manual and automated techniques to monitor the organization's risks.

This risk assessment process is very important, since it is necessary to focus the organization's security activities on addressing issues that have the greatest impact and significance.

To develop an organization's systematic risk management program, a reference model should be used and adapted to the circumstances of the organization. Several excellent publications are available to provide guidance on appropriate risk management approaches. Two examples are the NIST's *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, and the Australian/New Zealand Standard on *Risk Management* (AS/NZS 4360:1999). The latter standard prescribes the following risk management requirements:
- **Policy**—The need for an organization's executive to define and document its policy for risk management, including objectives for, and its commitment to, risk management. The policy must be relevant to the organization's strategic context, goals, objectives and the nature of its business. Management should ensure that this policy is understood, implemented and maintained at all levels in the organization.
- **Planning and resourcing**—The organization should ensure that the program is established and maintained; performance should be reported to management and used as a basis for improvement. Responsibility, authority and interrelationships of personnel who perform and verify work affecting risk management should be defined and documented. The organization should identify resource requirements and facilitate the implementation of risk management programs, through the assignment of trained personnel for ongoing management of work activities and the verification activities for internal review
- **Implementation program**—The organization should define the steps required to implement an effective risk management system.
- **Management review**—Executive management should ensure a review of the risk management system at specific intervals, sufficient to ensure its continuing stability and effectiveness in satisfying requirements of the program. Records of such reviews should be maintained.
- **Risk management (application areas)**—Risk management can be applied at many levels in the organization both strategic and operational. It may also be applied to specific projects, decisions or processes.
- **Risk management documentation**—For each stage of the process, adequate records should be kept that are sufficient to satisfy an independent audit.

Figure 2.2—Operational Risk Categories		
Operational Risk Areas	**Description**	**Information or IT Mapping**
Facilities and operating environment risk	Loss or damage to operational capabilities caused by problems with premises, facilities, services or equipment	Business continuity management for IT facilities
Health and safety risk	Threats to the personal health and safety of staff, customers and members of the public	Confidentiality of home addresses, travel schedules, etc.
Information security risk	Unauthorized disclosure or modification to information, loss of availability of information, or inappropriate use of information	All aspects of information and IT security
Control frameworks risk	Inadequate design or performance of the existing risk management infrastructure	Business process analysis to identify critical information flows and control points
Legal and regulatory compliance risk	Failure comply with the laws of the countries in which business operations are carried out; failure to comply with any regulatory, reporting and taxation standards; failure to comply with contracts; or failure of contracts to protect business interests	Compliance with data protection legislation, cryptographic control regulations, etc.; accuracy, timeliness and quality of information reported to regulators; and content management of all information sent to other parties
Corporate governance risk	Failure of directors to fulfill their personal statutory obligations in managing and controlling the company	Information security policy making, performance measurement and reporting
Reputation risk	The negative effects of public opinion, customer opinion, market reputation and the damage caused to the brand by failure to manage public relations	Controlling the disclosure of confidential information; presenting a public image of a well-managed enterprise
Strategic risk	Failure to meet the long-term strategic goals of the business, including dependence on any estimated or planned outcomes that may be in the control of third parties	Managing the quality and granularity of information on which strategic business decisions are based (such as mergers, acquisitions, disposals)
Processing and behavioral risk	Problems with service or product delivery caused by failure of internal controls, information systems, employee integrity; errors and mistakes; or through weaknesses in operating procedures	All aspects of information systems security and the security-related behavior of employees in carrying out their tasks
Technology risk	Failure to plan, manage and monitor the performance of technology-related projects, products, services, processes, staff and delivery channels	Failure of information and communications technology systems and the need for business continuity management
Project management risk	Failure to plan and manage the resources required for achieving tactical project goals, leading to budget overruns, time overruns or both, or leading to failure to complete the project; the technical failure of a project or the failure to manage the integration aspects with existing parts of the business and the impact that changes can have on business operations	Management of all information security-related projects
Criminal and illicit acts risk	Loss or damage caused by fraud, theft, willful neglect, gross negligence, vandalism, sabotage, extortion, etc.	Provision of security services and mechanisms to prevent all types of cybercrime
Human resources risk	Failure to recruit, develop or retain employees with the appropriate skills and knowledge or to manage employee relations	Need for policies protecting employees from sexual harassment, racial abuse, etc., through corporate e-mail systems, etc.

Figure 2.2—Operational Risk Categories (cont.)		
Operational Risk Areas	**Description**	**Information or IT Mapping**
Supplier risk	Failure to evaluate adequately the capabilities of suppliers leading to breakdowns in the supply process or substandard delivery of supplied goods and services; failure to understand and manage the supply chain issues	Outsourced service delivery of IT or other business information processing activities
Management information risk	Inadequate, inaccurate, incomplete or untimely provision of information to support the management decision-making process	Managing the accuracy, integrity, currency, timeliness and quality of information used for management decision support
Ethics risk	Damage caused by unethical business practices, including those of associated business partners. Issues include racial and religious discrimination, exploitation of child labor, pollution, environmental issues, behavior to disadvantaged groups, etc.	Ethical collection, storage and use of information; management of information content on web sites, intranets, and in corporate e-mails and instant messaging systems
Geopolitical risk	Loss or damage in some countries, caused by political instability, poor quality of infrastructure in developing regions, or cultural differences and misunderstandings	Managing all aspects of information security and IT systems' security in regions where the enterprise has business operations but where there are special geopolitical risks.
Cultural risk	Failure to deal with cultural issues affecting employees, customers or other stakeholders. These include language, religion, morality, dress codes and other community customs and practices.	Management of information content on web sites, intranets, and in corporate e-mails and instant messaging systems
Climate and weather risk	Loss or damage caused by unusual climate conditions, including drought, heat, flood, cold, storm, winds, etc.	Business continuity management for IT facilities
Source: SABSA Security Architecture 2005		

2.7.2 Threats

Threats to information resources and the likelihood of their occurrence must be assessed. In this context, threats are any circumstances or events with the potential to cause harm to an information resource by exploiting vulnerabilities in the system. Common classes of threats are:

- Errors
- Accidents
- Malicious damage/attack
- Naturally occurring events (e.g., flood, earthquake, etc.)
- Fraud
- Theft
- Equipment/software failure
- Loss of services (e.g., utilities, transportation, etc.)

2.7.3 Vulnerabilities

Vulnerabilities must be identified and evaluated. Many IT system weaknesses can be uncovered using automated scanning equipment. Process and performance vulnerabilities are more difficult to ascertain and may require careful analysis to uncover. Audits are usually very helpful in identifying vulnerabilities.

Some examples of vulnerabilities are:

- Defective software
- Improperly configured equipment
- Inadequate compliance enforcement

- Poor network design
- Uncontrolled or defective processes
- Inadequate management
- Insufficient staff
- Lack of user knowledge
- Lack of security functionality
- Lack of proper maintenance
- Poor choice of passwords
- Untested technology
- Transmission of unprotected communications
- Lack of redundancy
- Poor management communications

2.7.4 Risks

The ISM must understand the business risk profile of the organization. No model provides a complete picture, but logically categorizing the risk areas of an organization (as illustrated in **figure 2.2**) facilitates focusing on key risk management strategies and decisions. It also enables the organization to develop and implement risk mitigation measures that are relevant and cost-effective.

Risk is a feature of business life and, since it is impractical and uneconomic to eliminate all risks, every organization has a level of risk it will accept. To determine the reasonable level of acceptable risk, the risk manager must determine an optimal point where the cost of losses intersects with the cost of mitigating the risk.

2.7.4.1 Risk Management Options

Faced with risk, organizations have four strategic choices:
- Terminate the activity giving rise to risk.
- Transfer risk to another party.
- Treat risk by the use of appropriate control measures or mechanisms.
- Accept the risk.

Another alternative is that an organization may choose to reject risk by ignoring it, which can be dangerous. Ignoring a risk over time may lead to a serious underestimation of the magnitude of the risk. Accordingly, this is generally an inadvisable course of action. The only time it may be prudent to ignore a risk is when the likelihood, exposure or impact is so small that the risk is not considered material to the organization.

2.7.4.1.1 Terminate the Activity

There are often ways activities might be modified or processes re-engineered that can serve to mitigate or manage risks to acceptable levels. Analysis of the activity could also lead to the conclusion that it is not worth the risk.

2.7.4.1.2 Transfer the Risk

An example of risk transference is the decision by an organization to purchase insurance to address areas of risk. When a company buys insurance, the risk is transferred to the insurance company in exchange for premium payments that reflect the insurance company's assessment of the degree of risk that it is assuming.

Another example of risk transference is through the use of indemnity agreements with providers of outsourced services. While the possible financial impacts of associated with the risk can be transferred, the legal responsibility for the consequences of compromise can not.

It is typical to transfer risks to insurance companies when the probability is low, but the impact is high. An example would be earthquake or flood. For the ISM, this means that a well-managed risk program must interface with other organizational assurance providers such as the typical insurance department.

2.7.4.1.3 Treat the Risk

Risk can be treated in a variety of ways. Risk can be mitigated by implementing or improving security controls or by countermeasures. These controls may directly address the risk or they may be compensating controls that mitigate the effects of an occurrence. The potential impact may be reduced through procedural or technical processes or threats and vulnerabilities may be addressed directly reducing the likelihood of exploitation.

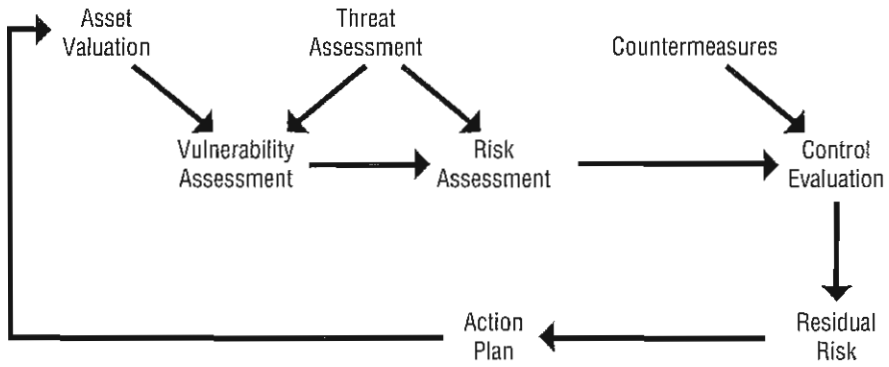
2.7.4.1.4 Accept the Risk

There are a variety of circumstances where a defined risk may be accepted. One condition is if the cost of mitigating it is too high in proportion to the value of the asset. In other cases, it may simply not be feasible to effectively mitigate a risk or the potential impact may be low. Generally, there is an optimal point where the cost of mitigating a risk is equal to the financial impact of compromise. It must be considered that not all impacts can be readily reduced to strictly financial terms and, in many cases, will not be the only consideration. Elements such as customer trust and confidence, legal liability, or breach of regulatory requirements may need to be considered as well.

2.7.4.2 Risk Assessment

In the COBIT framework for risk analysis, illustrated in **figure 2.3**, the first step in performing a risk assessment is to determine asset valuation. Obviously, if the value is low, any risk to it may not be significant and no controls or countermeasures are warranted. Assuming an asset is of significant value, then the next element is to determine what vulnerabilities to loss or damage exist. Next, an assessment of viable threats must be performed. If the asset has value as well as vulnerabilities susceptible to viable threats, then there is a risk. To clarify, it is obvious that vulnerabilities for which no threats exist pose no risk. Another way to look at it is that the greater the value, the greater the number and degree of vulnerabilities, and the greater the number of viable threats, the greater the risk.

Figure 2.3—Risk Analysis Framework



Source: IT Governance Institute

Technical methods including the use of software can be used to identify and track risk as well as provide reporting tools to record the analysis of risks. As with any process, the best tool to use is the one that is best suited to meet the unique needs of the organization. In applying risk analysis and identification methods, the ISM should prepare a detailed action plan, define resource requirements, and establish a budget and timetable for these important tasks. Budgeting and project planning are covered in chapter 3, Information Security Program(me) Management.

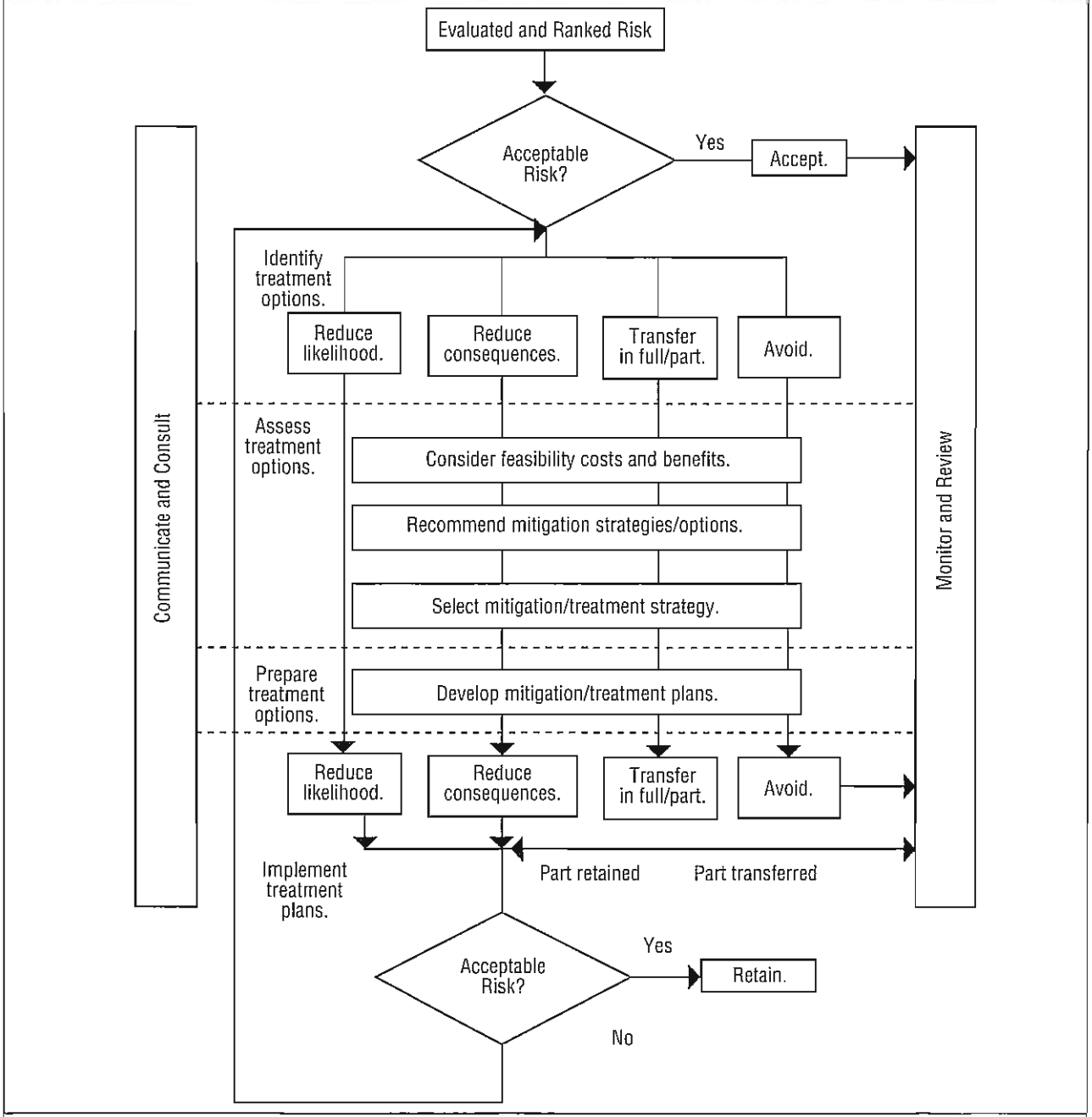
Defining strategies and prioritizing options to mitigate risk to levels acceptable to the enterprise are key responsibilities facing the ISM. The environment provides a wealth of security strategies and options. Once the risks facing an organization have been identified and prioritized and the assets valued and classified, the ISM can customize the security strategies and prioritize the options to mitigate those risks. The controls can include:

- Deterrent controls to reduce probability of or susceptibility to threats by a variety of means to mitigate overall risk
- Preventative controls to reduce vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls to reduce impact
- Detective controls to discover attacks or probes leading up to an attack and trigger preventative or corrective controls

The ISM should be aware of the various tools and processes for mitigating risk within the organization's structure. The ISM must balance the available options against what is acceptable to the enterprise. The ISM must consider the costs and impact of security measures on its organizational culture and its ability to complete its business objectives. The ISM should be aware that an improper set of security strategies and options could inhibit necessary work. One example might be limiting Internet access by employees. While this will reduce some risks, the organization may need the Internet for research and, therefore, restricting access could result in reduced employee effectiveness. As stated previously, the cost of a control should never exceed the benefit to be derived. The cost calculations must include any additional work or time required by personnel as a result of the control deployment.

The key to risk management is the risk mitigation or treatment process (how the evaluated risk is treated in the organization). The risk treatment process is shown below in **figure 2.4**.

Figure 2.4—The Risk Treatment Process



Adapted from the AS/NZS: 4360:1999

2.7.5 Impact

Impact is the bottom line for risk management. Ultimately, all risk management activities are designed to reduce impacts to acceptable levels. The result of any vulnerability being exploited by a threat that causes a loss is an impact. Threats and vulnerabilities that cannot cause an impact are irrelevant.

In commercial organizations, the impact is usually quantified as a direct financial loss in the short term or an ultimate (indirect) financial loss in the long term. Examples of such losses include the following:
- Direct loss of money (cash or credit)
- Criminal or civil liability
- Loss of reputation/goodwill
- Reduction of share value
- Endangering staff or customers
- Breach of confidence
- Loss of business opportunity
- Reduction in operational efficiency/performance
- Interruption of business activity

Impacts are determined by performing a business impact assessment and subsequent analysis. This analysis will determine the criticality and sensitivity of information assets. It will provide the basis for setting access control authorizations as well as the basis for business continuity planning including RTOs. It serves to prioritize risk management and, coupled with asset valuations, it provides the basis for the levels and types of protection required as well as the basis for business case development.

2.7.6 Controls and Countermeasures

The key to risk management is the risk mitigation or treatment process (how the evaluated risk is treated in the organization). The risk treatment process is depicted in **figure 2.4**. Once risks have been identified, existing controls and countermeasures can be evaluated or new ones designed to mitigate risks to acceptable levels.

Controls have previously been defined as the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected

Countermeasures directly reduce a threat or vulnerability. Ceasing an activity that creates risk is an example of a countermeasure. Segmenting a network is also a countermeasure in that it reduces the vulnerability of the network in case of a breach, since it may be contained within the segment. Multiple Internet service providers (ISPs) would also be a countermeasure that reduces the probability of a total outage.

The strength of a control can be measured in terms of its inherent or design strength and the likelihood of its effectiveness. An example of an inherently strong control is provided by balancing the books to account for all cash. An example of an inherently strong control by design is requiring dual control to access sensitive areas or materials.

Elements of controls that should be considered when evaluating control strength include whether the controls are preventative or detective, manual or programmed, and formal (documented in procedure manuals and evidence of their operation is maintained) or *ad hoc*.

Preventative controls would include a policy for separation of duties or firewalls that prevent certain types of access. Detective controls include log reviews, audits or intrusion detection systems (IDSs).

2.7.6.1 Residual Risk

The risks that remain once countermeasures and controls have been applied is called residual risk. Using the example of requiring dual control to access sensitive information, one residual risk is that two individuals collude to provide unauthorized access.

Residual risk identified by a subsequent risk assessment can be used by management to identify those areas in which more control is required to further mitigate risk. Acceptable levels of risk are established as a part of developing an information security strategy as described in chapter 1, Information Security Governance. If a strategy has not been developed, management must determine the acceptable risk levels, usually in terms of allowable impacts. Risks in excess of this level should be further mitigated by the implementation of more stringent countermeasures or controls. Risks below this level should be evaluated to determine if an excessive level of countermeasures or control is being applied and if cost savings can be made by removing or modifying them. Final acceptance of residual risks takes into account:
- Organizational policy
- Sensitivity and criticality of relevant assets
- Acceptable levels of potential impacts
- Uncertainty incorporated in the risk assessment approach itself
- Cost and effectiveness of implementation

In judging the appropriateness of controls or countermeasures, the cost of implementing and operating specific measures or mechanisms must be balanced against the risk being addressed.

This judgment involves assessment of two components:
- The likelihood of loss or damage occurring to specific assets
- The magnitude and effect of the financial or other impact of such occurrence

Determining the likelihood of occurrence involves business judgment, for example:
- The integrity and operating style of an organization's management and its team will influence control consciousness of all staff. If the security environment is weak, despite the best controls design, weak compliance or circumvention may result in increasing the likelihood of a loss or damage occurrence.
- The nature of business processes (e.g., global, remote/unsupervised operations, lack of segregation of duties) can also determine the likelihood of loss or damage.
- The attractiveness of the asset leads to higher risk exposure and loss occurrence.

2.7.6.2 Cost and Benefits

When controls or countermeasures are planned, an organization should consider the costs and benefits. If the cost of controls or countermeasures (control overhead) exceed the benefits, an organization may choose to accept the risk rather than incurring additional costs in securing its systems. This follows the general principle that the cost of a control should never exceed the expected benefit. This is the principle of proportionality described in GASSP (or its successor, GAISP).

When considering costs, the TCO must be considered for the full life cycle of the control or countermeasure. This can include such elements as:
- Acquisition costs if any
- Deployment and implementation costs
- Maintenance costs
- Testing and assessment costs
- Compliance monitoring and enforcement
- Inconvenience to users
- Reduced throughput of controlled processes
- Training in new procedures or technologies as applicable

2.7.7 Information Resource Valuation

The process of valuation, which consists of relating all values in a common financial form, of some assets may be straightforward. Hardware can be easily valued based on replacement costs. The value of information in some cases will be the cost of recreating or restoring it. In other cases, the value will be related to the consequential costs and possible regulatory breaches of the disclosure of private information. The impact or consequences can result from regulatory sanctions and may include individuals suffering identity theft losses filing lawsuits for damages, to possible delayed

class-action lawsuits on behalf of thousands of victims, or reputational damage resulting in loss of share value. Clearly, in this case, the valuation cannot be based on the intrinsic value of the information, which may be low or zero. Rather, valuation must be based on a reduction in potential losses. In other words, value of information may need to be considered from the perspective of potential harm or significant consequences resulting from intrusion or unintended disclosure.

Marketing materials are another type of information with no intrinsic value that can nevertheless create unintended liabilities and, therefore, risks that must be considered. Inaccurate representations of products or services have resulted in significant losses as a consequence of various legal actions. Therefore, a prudent organization must consider ensuring systematic review and control of information to manage the risk of potential liability created by publicly released information.

Examples of typical information assets include:
- Information and data
- Hardware
- Software
- Services
- Documents
- Personnel

2.7.7.1 Information Resource Valuation Methodologies

Once the business resources that need to be protected have been identified, their value must be derived and assigned. Value needs to be considered in terms of the cost of loss either quantitatively, qualitatively or through some combination of the two. The valuation of some assets may be relatively straightforward to determine quantitatively, for example, the loss of a server as a result of damage. Other assets may be virtually impossible to value quantitatively and, as a result, judgment may be required. Valuation of information assets can range from replacement or reconstruction costs of destroyed data to potential regulatory sanctions as a result of compromised information. For example, the result of someone stealing customer personal credit data could be management having to notify a large number of people of the incident under laws such as the US State of California's SB 1386 and the potential costs of legal defense if a suit is filed by those impacted. Under these circumstances, the risk of reputational damage also exists and may adversely impact share value. These risks are difficult to quantify with any precision but must nevertheless be considered when attempting information resource valuations. Absent these valuations, there will be little basis for determining the appropriate levels of security required for adequate protection.

The information resource valuation may consider many different variables. These variables may include the level of technical complexity and the level of potential direct and consequential financial loss. Quantitative valuations will generally be the most precise but can still be quite complex once actual and downstream effects have been analyzed. Another form of valuation that is sometimes used is judgmental or qualitative in nature, where an independent decision is made based upon business knowledge, executive management directives, historical perspectives, business goals and environmental factors. There are situations in which quantitative data are not available and this alternative method is desirable. Many ISMs use a combination of techniques.

In addition, the ISM needs to be aware of ongoing changes in the organization and should alter the use of valuation methodologies to best meet the needs of these changes. If quantitative data are outdated and cannot be updated in a reasonable time frame, it may be desirable to use qualitative data either in place of or to augment the quantitative data.

2.7.8 Information Asset Classification

Information asset classification is required to determine the relative sensitivity and criticality of information assets which provides the basis for protection efforts, and business continuity planning and access control. For larger organizations, this can be a daunting task as there is likely to be terabytes of electronic data, warehouses of documents, and thousands of individuals and devices. Yet, without determining the value, sensitivity and criticality (and increasingly, legal and regulatory requirements) of information resources, it will not be possible to develop an effective risk management program that provides appropriate protection proportional to sensitivity, value or criticality.

In cases where classification is not possible due to resource constraints or other reasons, a less-effective option is a business dependency assessment that can be used to provide a basis for allocating protective activities. This approach is based on the information resources critical business functions utilize.

The first step in the classification process is locating and identifying information resources. In many organizations, this may prove difficult as there often is no comprehensive inventory of information-related assets. This may be especially true in larger organizations with multiple independent business units lacking a strong centralized security function. The identification process will include determining the owners, users, custodians and external service providers. These service providers can include media vaulting and archival firms, mailing list processors, firms that process mail containing company information, firms that act as couriers or transporters of information, and third-party service providers. Service providers may include data centers providing hosting functions, payroll services or health insurance administration.

The ISM should assign classes or levels of sensitivity and criticality to information resources and ensure that management establishes guidelines for the level of access controls that should be assigned. The number of levels should be kept to a minimum. Classifications should be simple, such as designations by differing degrees for sensitivity and criticality. End-user managers in coordination with the security administrator can then use these classifications in their risk assessment process to assist with determining access levels.

One major benefit of data classification is the reduced risk of underprotecting and the cost of overprotecting information resources by tying security to business objectives. Although it is not a small undertaking to implement data classification, the long-term benefits to the organization can be substantial.

There are a number of questions that should be asked in any data classification model, including but not limited to:
- How many classification levels are suitable for the organization?
- How will information be located?
- What process is used to determine classification?
- How will classified information be identified?
- How will it be marked?
- How will it be handled?
- How will it be transported?
- How will confidential information be stored and archived?
- How will it be retained according to policy or law?
- How will it be safely destroyed at the end of the retention period?
- Who has ownership of information?
- Who has access rights?
- Who has authority for determining access to the data?
- What approvals are needed for access?

2.7.8.1 Methods to Determine Criticality of Resources and Impact of Adverse Events

A number of methods exist to determine the sensitivity and criticality of information resources and the impact of adverse events. A BIA is often performed to identify the impact of adverse events. Methods outlined within COBIT, NIST and Software Engineering Institute's OCTAVE framework are representative of the resources the ISM may utilize in this effort.

It is a generally accepted practice to focus on the impact that a loss of information resources would have on the organization rather then on a specific adverse event. Since there are numerous adverse events that could occur, it would be a daunting task to completely list all of them. Such an effort obviously would not be practical or cost-effective. In addition, the effect of a loss of information resources is the objective of this exercise, and the end result is not dependent on the cause. The bottom line is an interruption in processing that causes systems to become unavailable. Therefore, the loss of information resources should be simply categorized as a loss of availability, and the impact should be evaluated based on this simplified categorization. That categorization may include the total loss, partial loss, integrity corruption or availability loss of information resources.

2.7.9 Recovery Time Objectives

The ISM should have knowledge of the RTOs for their organization's information resources as part of the overall evaluation of risk. The organization's business needs will dictate the RTO, which is defined by the business as the amount of down time the resource can endure without severe impact. The information resource's functional criticality, recovery priorities and their interdependencies are variables that should be determined to define the RTO.

Determining RTO can depend upon a number of factors including the cyclical need (time of day, week, month or year) of the information and organization, interdependencies among the information, and the organization's requirements. The organization's requirements can be based upon customer needs, expectations, service level agreements and regulatory requirements.

Through the risk assessment process, the ISM has determined the criticality of various information resources. Now an RTO should be included for each piece of information. Generally, these RTOs are determined by performing a BIA in coordination with developing a business continuity plan. The BIA is generally conducted by interviewing system owners to obtain their perspective on the cost associated with an extended interruption in service for a business system. Often there are two perspectives for RTO. One is the perspective of the individuals whose job it is to utilize the information, and the other is the view of senior management. An information resource that a divisional supervisor may believe is critical may not be critical in the eyes of the vice president of operations, who is able to include the overall organizational risk in the evaluation of the RTO.

The ISM should understand that both perspectives are important and work toward an RTO that considers them. The result will factor into the business continuity plan and priority order for the recovery of systems. In the end, the final decision is that of senior management. Senior management is in the best position to arbitrate the needs and requirements of the different components of the business, such as the regulatory requirements to which the organization is subject, and determine which processes are the most critical to the continued survival of the business as well as determine acceptable costs.

2.7.9.1 RTO and How It Relates to Business Continuity and Contingency Planning Objectives and Processes

Knowledge of the RTO for information resources is needed for an organization to develop and implement an effective business continuity program. Once the RTOs are known, the organization can identify and develop contingency strategies that will meet the RTOs of the information resources. The RTOs will drive the order of priority for restoration of systems and in certain cases, the selection of specific recovery technologies in situations where the RTO is very short.

One critical factor when developing contingency processes is cost. System owners will invariably prefer shorter RTOs, but the trade-offs in cost may not be warranted. Near instantaneous recovery can be achieved where needed using technologies such as mirroring of information resources and duplication of the information, so that, in the event of a disruption, the resources are always available quickly. Therefore, the cost of recovery generally is less expensive, if the RTO for a given resource is longer.

There is a breakeven point, where the impact of the disruption will begin to be greater than the cost of recovery. The length of this time period depends on the nature of the business being disrupted. Qualitative as well as quantitative issues must be taken into consideration, since loss of customer confidence, even if it cannot be estimated, can have a long-term negative impact on the organization. Most organizations can reduce their RTOs, but there is a cost associated with achieving this.

2.7.10 Third-party Service Providers

A typical business organization uses many information resources in support of its business processes. These information resources can originate within the organization or be provided by entities external to the organization. A combination of the two will be employed by a majority of organizations. The ISM needs to be aware of all information resources, since they must all be protected against compromise.

Outsourced information resources may present a security manager with a challenge, since external organizations may be reluctant to share technical details on the nature and extent of their information protection mechanisms. It is important to try to ensure that adequate specified levels of protection are included in service level agreements and other outsourcing contracts. One common approach is to specify requirements for specific audits such as SAS 70 level 2 or BS 7799 certification. It is also important to analyze SAS 70 reports upon receipt for third-party auditor comments and, if present, comments about customer control considerations. Another often-neglected area concerns third-party vendor financial viability. Information can be gleaned from credit reports, SEC filings of publicly traded firms, annual reports, etc. Absent such certifications, information must be obtained from providers sufficient to determine how external entities are securing information assets.

It should be considered that some portion of risk associated with outsourced information services can be transferred by incorporating indemnity clauses in service level agreements.

For internal and external resources, the ISM should understand the business processes and the information resources that are critical to each line of business. This information can be obtained from discussions with the individual owners of the business processes, technical documentation maintained by the systems areas and discussions with senior management. It will not be possible to define and deploy a comprehensive security program until complete information on internal and external information resources is compiled.

2.7.11 Integration Into Life Cycle Processes

Ensuring that risk identification, analysis and mitigation activities are integrated into life cycle processes is an important task of information security management. Most organizations have change management procedures that can provide the ISM with an approach to implementing risk management processes on an ongoing basis. Since changes to any information resource are likely to introduce new vulnerabilities and change the overall risk equation, it is important that the ISM is made aware of proposed modifications. This approach will allow for risk identification, analysis and mitigation activities to be integrated into the life cycle processes of the organization.

Change management has always been a tenet of well-managed IT organizations. But, as distributed computing became the norm and changes were made more easily in a dispersed environment by people with limited knowledge, organizations often experienced a lack of standardization in their hardware and software environments. Realizing this, IT managers have instituted more robust change management procedures and, as a consequence, have begun to achieve enhanced control over the enterprise IT resources. This is of course a moving target, and organizations with remote operations are in some cases still finding effective change management an elusive goal.

Organizations have also instituted change management for other areas of the business and have instituted change management procedures for a variety of business activities. The benefit of these activities is that many organizations now have change management procedures that span the entire organization. The ISM must be aware of these change management activities and ensure that security is well entrenched, so changes are not made without considering the implications to the overall security of the organization's information resources. One method of helping to ensure this is for information security management to participate as a member of the change management committee and ensure that all significant changes are subject to review and approval by security.

While the normal focus in change management addresses hardware and software changes (testing, sign-offs, etc.) and possibly security impact, the change management process should extend beyond the system owners and IT population. The change management process should include facilities management where data center infrastructure (configuration management and capacity planning) must address system changes and facilities maintenance windows with facilities personnel (often outsourced) and business continuity management. Quite often changes are not documented on a timely basis within these areas. Facilities may not have current single line drawings and blue prints. Correspondingly, computer infrastructure/configuration management may not have the changes properly documented or updated on a timely basis. Business continuity may also fall behind on relevant updates when those updates occur in cycles. Emergency response and business continuity may also suffer communications lapses when current and changing processes are not reviewed within facility infrastructure areas.

Facilities personnel often have access to environmental monitoring and control systems (building management system or BMS/scada systems) for heating, ventilating and air conditioning (HVAC), water and electricity. These are often programmed for remote computer access, an area that often escapes information security overview. Facilities service contracts often have emergency response clauses. However, those contracts should be reviewed because they may lack service level agreements or lack sufficient details and accountability for a weak response. A high availability application may suffer unforeseen business impacts as a result of facilities failures.

By integrating risk identification, analysis and mitigation activities into change management (life cycle processes), the ISM can ensure that critical information resources are adequately protected. This is a proactive approach, enabling the ISM to better plan and implement security policies and procedures in alignment with the business goals and objectives of the organization. It also permits information security controls to be interjected into an activity that holds the greatest potential for degrading existing controls.

2.7.11.1 Life-cycle-based Risk Management Principles and Practices

Since risk management is a continuous process, the ISM should view risk management as having a life cycle. Employing a life-cycle-based risk management approach improves costs in that a full risk assessment does not have to be performed periodically. Instead, updates may be made to the risk assessment and risk management processes on a more regular basis.

Generally, project risk management is performed by project managers but usually not in as systematic a manner, and these efforts are generally not as visible to senior management. The life cycle approach should also be considered for use in project management to identify, analyze, assess and track risks, and can also be tied into periodic reporting to system owners.

The ISM should seek to employ a consistent process with supporting tools, training and assistance to better understand and reduce the impact of risks that are inherent in the life cycle of a project. The approach should be a top-down systematic approach because senior management's vision of risk can be employed to guide the process. It will also lend additional weight and credibility to the process.

The ISM should also consider employing software tools designed to track the risk management life cycle. This is advantageous since it allows the leveraging of finite staffing resources to provide adequate monitoring and to generate periodic reports for management.

2.7.12 Baselines

Setting security baselines for an organization's information security has a number of benefits. It standardizes the minimum amount of security measures that must be employed which has positive benefits for risk management. Secondly, it provides a convenient point of reference to measure changes to security and identify corresponding effects on risk.

For a number of information technologies, technology vendors and security organizations have identified the minimum security controls that should be in place to ensure due care in protecting information assets. This information continues to grow and is a resource for ISMs; however, the ISM has to keep in mind that every organization has its own needs and its own requirements. While vendor information can provide a starting point, specific analysis should always be performed. It is also important to keep in mind that in addition to technology in the definition of a risk analysis program, people and processes must be considered as well.

There is a general consensus among many vendors, security organizations, information security professionals and systems auditors about security configuration specifications that represent a prudent level of due care. These cooperative efforts continue to define consensus-based, good-practice security configurations for various systems and platforms. The ISM should examine these specifications and, where appropriate, they should be tailored as appropriate and incorporated into organizational security baselines.

While industry standard baselines are important for the ISM to be aware of, the ISM must assess the level of security that should be employed in their individual organization. The commingling of different technologies can often introduce new risks and change a secure system or platform into one that has vulnerabilities. A tailored risk assessment that recognizes these interactions and dependencies will enable the ISM to determine whether security processes and procedures above the generally accepted baselines are necessary to provide adequate security commensurate with the organizations defined levels of acceptable risk. Some organizations and industries may require higher baselines. Regulatory requirement for certain industries and regions may set a higher standard. Another issue may be that some of the organization's information is classified as highly sensitive, and it must have control mechanisms providing higher level of security.

2.7.13 Monitoring and Communication

2.7.13.1 Reporting Significant Changes in Risk

Reporting significant changes in risk to appropriate levels of management on a periodic and event-driven basis is a primary role of the ISM. As changes occur within the organization, the risk assessment must be updated to ensure it remains an accurate representation. The ISM should have periodic update meetings with upper management to present a status on the organization's overall security program. That update should include any significant changes to the organization's risk profile.

In addition, the security program should include a process whereby a significant security breach or security event will trigger a report to upper management. The ISM should have defined processes whereby security events are evaluated based on impact to the organization. This evaluation may warrant a special report to upper management to inform them of the event, the impact and the steps being taken to mitigate the risk.

An important component of the risk management life cycle is continuously monitoring, evaluating and assessing risks. The results and status of this ongoing analysis needs to be documented and reported to senior management on a regular basis. To facilitate such reporting, visual aids such as color-coding and summarized overviews can be useful. Senior management may not wish to be burdened with technical details and is likely to want an overview of the current status and indicators of any immediate or impending threat. Accordingly, the use of red-amber-green reports, often referred to as security dashboards, which show an overall assessment of the security posture, is often used. The ISM is responsible for the management of this reporting process to ensure that it takes place and that the results are analyzed adequately and acted upon appropriately in a timely manner.

2.7.13.2 Training and Awareness

People typically constitute the greatest risk to any organization generally through accident, mistake, a lack of knowledge or information, and occasionally, through malicious intent. Appropriate training and awareness campaigns can have significant positive impact on managing risks. Many controls are procedural and require some operational knowledge and compliance. Technical controls must be configured and operated correctly to provide the expected level of assurance. Ensuring users are educated in procedures and understand risk management processes is the responsibility of the ISM and appropriate training and awareness activities should be included in any risk management program.

2.7.14 Documentation

To manage risk properly, appropriate documentation is required. Decisions concerning the extent of documentation will involve costs and related benefits. The risk management policy and program should define the documentation needed. Specifically, at each stage of the process, documentation should include:

- Objectives
- Audience
- Information resources
- Assumptions
- Decisions

The risk management policy document may include information such as:
- Objectives of the policy and rationale for managing risk
- Links between the risk management policy and the organization's strategic and corporate business plans
- Extent and range of issues to which the policy applies
- Guidance on what may be regarded as acceptable risk
- Who is responsible for managing risks
- Support expertise available to assist those responsible for managing risks
- Level of documentation required
- A plan for reviewing compliance to the risk management policy

In some circumstances, a compliance and due diligence statement may be required so managers formally acknowledge their responsibility to comply with risk management policies and procedures.

Typical documentation for risk management should include, at a minimum, the following:
- A risk register—For each risk identified, record the:
  - Source of risk
  - Nature of risk
  - Existing controls
- Consequences and likelihood including:
  - Income loss
  - Unexpected expense
  - Legal risk (compliance and contractual)
  - Interdependent processes
  - Loss of public reputation or public confidence
    - Initial risk rating
    - Vulnerability to external/internal factors
- A risk mitigation and action plan, providing:
  - Who has responsibility for implementing the plan
  - Resources to be utilized
  - Budget allocation
  - Timetable for implementation
  - Details of mechanism/control measures
  - Frequency of compliance
- Monitoring and audit documents, which include:
  - Outcomes of audits/reviews and other monitoring procedures
  - Follow-up of review recommendations and implementation status

2.8 CHAPTER 2 GLOSSARY

Availability
Ensuring that information systems and data are ready for use when they are needed; often expressed as the percentage of time that a system can be used for productive work

Business impact analysis (BIA)
An exercise that determines the impact of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting system

Business dependency assessment
A process of identifying resources critical to the operation of a business process

COBIT
Control Objectives for Information and related Technology, the international set of IT control objectives published by the IT Governance Institute

Confidentiality
The protection of sensitive or private information from unauthorized disclosure

Countermeasures
The process used to protect against attacks

Criticality analysis
An analysis to evaluate resources or business functions to identify their importance to the organization and the impact if a function cannot be completed or a resource is not available

Data classification
The assignment of a level of sensitivity to data that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the organization.

Exposure
The extent to which a vulnerability can result in adverse consequences; the potential loss to an area due to the occurrence of an adverse event

Information security program
The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis

ISO/IEC 17799
Originally released as part of the British Standard for Information Security in 1999 as the Code of Practice for Information Security Management, in October 2000 it was elevated by the International Organization for Standardization (ISO) to an international code of practice for information security management. This standard defines information's confidentiality, integrity and availability controls in a comprehensive information security management system.

Policies
High-level statements of management intent and direction

Procedures
A detailed description of the steps necessary to perform specific operations in conformance with applicable standards; a portion of a security policy that states the general process that will be performed to accomplish a security goal

Recovery point objective (RPO)
A measurement of the point prior to an outage to which data are to be restored

Recovery time objective (RTO)
The amount of time allowed for the recovery of a business function or resource after a disaster occurs

Residual risk
The amount of risk that remains after countermeasures and controls are in place

Risk assessment
A process used to identify and evaluate risks and their potential impact on an organization in quantitative or qualitative terms

Risk avoidance
The process for systematically avoiding risk

Risk mitigation
The reduction of risk through the use of countermeasures and controls

Risk transfer
The process of assigning risk to another organization, usually through the purchase of an insurance policy

Sensitivity
A measure of the impact that the disclosure of information may have on an organization

Standards
Definition of the metrics used to determine the correctness of a thing or process; a set of rules or specifications that, when taken together, define a software or hardware device. A standard is also an acknowledged basis for comparing or measuring something.

Steering committee
A management committee assembled to sponsor and manage various projects such as an information security program

Threat analysis
An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against information assets and information technology. The threat analysis usually also defines the level of threat and the likelihood of that threat to materialize.

Vulnerabilities
A weakness in system security procedures, system design, implementation or internal controls that could be exploited to violate system security

2.9 CHAPTER 2 SAMPLE QUESTIONS

CISM exam questions are developed with the intent of measuring and testing practical knowledge in information security management. All questions are multiple choice and are designed for one best answer. Every CISM question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement.

In some instances, a scenario or a description problem may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided.

Many times a CISM examination question will require the candidate to choose the **MOST** likely or **BEST** answer. In every case the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked and how to study to gain knowledge of what will be tested will go a long way toward answering them correctly.

The sample questions contained below are designed to depict the type of question format on the CISM examination.

1. The overall objective of risk management is to:

   A. eliminate all vulnerabilities if possible.
   B. determine the best way to transfer risk.
   C. reduce risks to an acceptable level.
   D. implement effective countermeasures.

2. Residual risks can be determined by:

   A. determining remaining vulnerabilities after countermeasures.
   B. performing a comprehensive threat analysis.
   C. conducting a standard risk assessment.
   D. transferring all risks to third parties.

3. To address changes in risk, an effective risk management program should:

   A. ensure that continuous monitoring processes are in place.
   B. establish proper security baselines for all information resources.
   C. implement a complete data classification process.
   D. change security policies on a timely basis to address changing risks.

4. Information classification is important to properly manage risk **PRIMARILY** because:

   A. it ensures accountability for information resources as required by roles and responsibilities.
   B. it is a legal requirement under various regulations.
   C. there is no other way to meet the requirements for availability, integrity and auditability.
   D. it is used to identify the sensitivity and criticality of information to the organization.

5. Vulnerabilities discovered during an assessment should be:

   A. handled as a risk even though there is no threat.
   B. prioritized for remediation solely based on impact.
   C. a basis for analyzing the effectiveness of controls.
   D. evaluated for threat and impact in addition to cost of mitigation.

6. Indemnity agreements can be used to:

A. ensure an agreed upon level of service.
B. to reduce impacts on critical resources.
C. to transfer responsibility to a third party.
D. provide an effective countermeasure to threats.

2.10 CHAPTER 2 ANSWERS TO SAMPLE QUESTIONS

1. **C** Risk management is the process of reducing risks to an acceptable level. It is usually not possible to eliminate all vulnerabilities, and risk transfer and countermeasures are just some of the methods available to address risks.

2. **C** Residual risk is what is left after countermeasures and controls have been implemented to reduce risks. A risk assessment includes a determination of the effectiveness of risk reduction efforts and will, therefore, determine the remaining (or residual) risk.

3. **A** Risks will change as threats, vulnerabilities or potential impacts change over time. The risk management program must have processes in place to monitor those changes and modify countermeasures as appropriate to maintain acceptable levels of residual risk.

4. **D** Information classification is an essential step to determining how confidential and critical information is to the business. The classification is then used to determine what information must be protected and how well during creation, handling, marking, transporting, storing and destruction. Protection that could include strong encryption and robust access controls, controls on marking, distribution and retention, etc.

5. **D** Vulnerabilities uncovered should be evaluated and prioritized based on whether there is a credible threat, the impact if the vulnerability is exploited and the cost of mitigation. If there is a potential threat but little or no impact if the vulnerability is exploited, there is little risk and it may not be cost-effective to address it.

6. **B** Indemnity agreements serve to reduce financial impacts by providing compensation for adverse events in the scope of the agreement.

2.11 CHAPTER 2 REFERENCES

Andrews, Jonathan D.; "Erosion of Trust—E-commerce and the Loss of Privacy," ***Information Systems Control Journal*****, vol. 3, 2001, p. 46-49**

Ataya, Georges; "Risk-aware Decision Making for New IT Investments," ***Information Systems Control Journal*****, vol. 2, 2003, p. 12-14**

Bakalov, Rudy; "Risk Management Strategies for Offshore Application and Systems Development," ***Information Systems Control Journal*****, vol. 5, 2004, p. 36-38**

Benvenuto, Nicholas A.; David Brand; "Outsourcing—A Risk Management Perspective," ***Information Systems Control Journal*****, vol. 5, 2005, p. 35-40**

Bhatia, Mohan; "New Basel Accord: Operational Risk Management—Emerging Frontiers for the Profession," ***Information Systems Control Journal*****, vol. 1, 2002, p. 37-42**

Braswell, Daniel E.; W. Ken Harmon; "Assessing and Preventing Risks from E-mail System Use," ***Information Systems Control Journal*****, vol. 5, 2003, p. 33-35**

Brooke, Paul; "Risk-Assessment Strategies," Network Computing, 30 October 2000, *www.networkcomputing.com/1121/1121f32.html?ls=NCJS_1121bt*

The Center for Internet Security, *www.cisecurity.org* (Includes applicable publications on standards, risks and baselines)

Cerullo, Michael J.; Virginia Cerullo; "Threat Assessment and Security Measures Justification for Advanced IT Networks," ***Information Systems Control Journal*****, vol. 1, 2005, p. 35-43**

CPM Group, *www.contingencyplanning.com* (Contains business continuity, disaster recovery, RTO and crisis management guidance and information)

Cohen, Gidi; "The Role of Attack Simulation in Automating Security Risk Management," ***Information Systems Control Journal*****, vol. 1, 2005, p. 51-54**

Disaster Recovery Journal, *www.drj.com* (Contains business continuity, disaster recovery, RTO and crisis management guidance and information)

Gaulke, Markus; "Risk Management in IT Projects," ***Information Systems Control Journal*****, vol. 5, 2002, p. 37-39**

Gerdes, Michael; "An Exploration of Global Perceptions of Security and Privacy," ***Information Systems Control Journal*****, vol. 6, 2002, p. 27-30**

Hawaii Health Information Corporation, "Data Classification Policy," *www.hhic.org/hipaa/pdf/dataclass.pdf* (An example of a data classification policy)

IT Governance Institute, COBIT 4.0, USA, 2005, ***www.isaca.org/cobit***

Judge, Joe; "The State of Enterprise Security Management," ***Information Systems Control Journal*****, vol. 6, 2001, p. 38-40**

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

King, Christopher M.; Curtis E. Dalton; Ertem Osmanoglu; *Security Architecture*, McGraw Hill, USA, 2001, p. 444-446

McNamee, David; *Business Risk Assessment*, The Institute of Internal Auditors, USA, 1998

McNamee, David; Joseph R. Pleier; Dr. John D. Tongren; *Risk Management: Best Practice* (CD-ROM only), 1999

National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), USA *http://csrc.nist.gov* (Contains various publications discussing resource and information values)

Parmar, Kamal; "Justifying Investment in Security," *Information Systems Control Journal*, vol. 4, 2003, p. 53-55

Peltier, Thomas R.; *Information Security Risk Analysis*, Auerbach, USA, 2001

Ramakrishnan, Ganesh; "Risk Management for Internet Banking," *Information Systems Control Journal*, vol. 6, 2001, p. 48-50

Schreider, Tari; "Risk Assessment Tools: A Primer," *Information Systems Control Journal*, vol. 2, 2003, p. 23-25

The Security Risk Analysis Directory, *www.security-risk-analysis.com* (Includes general information on security risk analysis and a description of a risk analysis model)

Sherwood, J.; A. Clark; D. Lynas; *Enterprise Security Architecture: A Business Driven Approach*, CMP Books, 2004, *www.sabsa.org*

Software Engineering Institute, Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) framework, *www.cert.org/archive/pdf/99tr017.pdf*

Stanley, Richard A.; "Security, Audit and Control Issues for Managing Risk in the Wireless LAN Environment," *Information Systems Control Journal*, vol. 3, 2004, p. 23-25

Survive, *www.survive.com* (Contains business continuity, disaster recovery, RTO and crisis management guidance and information)

Wright, Catherine; "Top Three Potential Risks With Outsourcing Information Systems," *Information Systems Control Journal*, vol. 5, 2004, p. 40-42

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

Chapter 3:

INFORMATION SECURITY PROGRAM(ME) MANAGEMENT

3.1 DEFINITION

Information security programming management means designing, developing and managing an information security program to implement the information security governance framework.

3.2 OBJECTIVE

The objective of this job practice area is to manage information security risks to achieve business objectives through a number of tasks utilizing the security manager's knowledge of key risk management techniques.

This job practice area represents 21 percent of the CISM examination (approximately 42 questions).

3.3 TASKS

There are nine tasks within this job practice area:
1) Create and maintain plans to implement the information security governance framework.
2) Develop information security baselines.
3) Develop procedures and guidelines to ensure that business processes address information security risk.
4) Develop procedures and guidelines for IT infrastructure activities to ensure that compliance with information security policies.
5) Integrate information security program requirements into the organization's life cycle activities.
6) Develop methods of meeting information security policy requirements that take into account the impact on end users.
7) Promote accountability by business process owners and other stakeholders in managing information security risks.
8) Establish metrics to manage the information security governance framework.
9) Ensure that internal and external resources for information security are identified, appropriated and managed.

3.3.1 KNOWLEDGE STATEMENTS

The CISM candidate must have a good understanding of each of the system areas delivered by the knowledge statements. These statements are the basis for the the examination:
1) Knowledge of methods to develop an implementation plan that meets security requirements identified in risk analysis
2) Knowledge of project management methods and techniques
3) Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise
4) Knowledge of security baselines and configuration management in the design and management of business applications and the infrastructure
5) Knowledge of information security architectures (e.g., single sign-on, rules-based as opposed to list-based system access control for systems, limited points of systems administration)

6) Knowledge of information security technologies (e.g., cryptographic techniques and digital signatures, to enable management to select appropriate controls)
7) Knowledge of security procedures and guidelines for business processes and infrastructure activities
8) Knowledge of the systems development life cycle methodologies (e.g., traditional SDLC, prototyping)
9) Knowledge of planning, conducting, reporting and following up on security testing
10) Knowledge of certifying and accrediting the compliance of business applications and infrastructure to the enterprise's information security governance framework
11) Knowledge of types, benefits and costs of physical, administrative and technical controls
12) Knowledge of planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes
13) Knowledge of security metrics, design, development and implementation
14) Knowledge of acquisition management methods and techniques (e.g., evaluation of vendor service level agreements, preparation of contracts)

3.3.2 Relationship of Tasks to Knowledge Statements

The task statements reflect what the CISM candidate is expected to be able to do within his/her position as an information security manager. The knowledge statements delineate what the CISM candidate is expected to know in order to perform the tasks.

The task and knowledge statements are approximately mapped in **figure 3.1**. Note that there is often an overlap. Each task statement will generally map to several knowledge statements as shown.

Figure 3.1—Knowledge and Task Statements Mapping

Task Statements	Knowledge Statements
1. Create and maintain plans to implement the information security governance framework.	1. Knowledge of methods to develop an implementation plan that meets security requirements identified in risk analysis 3. Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise 12. Knowledge of planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes
2. Develop information security baselines.	4. Knowledge of security baselines and configuration management in the design and management of business applications and the infrastructure 5. Knowledge of information security architectures 6. Knowledge of information security technologies
3. Develop procedures and guidelines to ensure that business processes address information security risk.	3. Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise 7. Knowledge of security procedures and guidelines for business processes and infrastructure activities 11. Knowledge of types, benefits and costs of physical, administrative and technical controls 12. Knowledge of planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes

Figure 3.1—Knowledge and Task Statements Mapping (*cont.*)	
Task Statements	**Knowledge Statements**
4. Develop procedures and guidelines for IT infrastructure activities to ensure that compliance with information security policies.	3. Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise 5. Knowledge of information security architectures 6. Knowledge of information security technologies 7. Knowledge of security procedures and guidelines for business processes and infrastructure activities 11. Knowledge of types, benefits and costs of physical, administrative and technical controls
5. Integrate information security program requirements into the organization's life cycle activities.	1. Knowledge of methods to develop an implementation plan that meets security requirements identified in risk analysis 3. Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise 8. Knowledge of the systems development life cycle methodologies 12. Knowledge of planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes
6. Develop methods of meeting information security policy requirements that take into account the impact on end users.	1. Knowledge of methods to develop an implementation plan that meets security requirements identified in risk analysis 3. Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise 7. Knowledge of security procedures and guidelines for business processes and infrastructure activities 11. Knowledge of types, benefits and costs of physical, administrative and technical controls 12. Knowledge of planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes
7. Promote accountability by business process owners and other stakeholders in managing information security risks.	3. Knowledge of the components of an information security governance framework for integrating security principles, practices, management and awareness into all aspects and all levels of the enterprise 7. Knowledge of security procedures and guidelines for business processes and infrastructure activities 9. Knowledge of planning, conducting, reporting and following up on security testing 10. Knowledge of certifying and accrediting the compliance of business applications and infrastructure to the enterprise's information security governance framework 12. Knowledge of planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes 13. Knowledge of security metrics, design, development and implementation

Figure 3.1—Knowledge and Task Statements Mapping (*cont.*)	
Task Statements	**Knowledge Statements**
8. Establish metrics to manage the information security governance framework.	9. Knowledge of planning, conducting, reporting and following up on security testing 10. Knowledge of certifying and accrediting the compliance of business applications and infrastructure to the enterprise's information security governance framework 12. Knowledge of planning, designing, developing, testing and implementing information security requirements into an enterprise's business processes 13. Knowledge of security metrics, design, development and implementation
9. Ensure the internal and external resources for information security are identified, appropriated and managed.	6. Knowledge of information security technologies 7. Knowledge of security procedures and guidelines for business processes and infrastructure activities 10. Knowledge of certifying and accrediting the compliance of business applications and infrastructure to the enterprise's information security governance framework 14. Knowledge of acquisition management methods and techniques

3.4 INFORMATION SECURITY PROGRAM MANAGEMENT OVERVIEW

3.4.1 Importance of Information Security Program Management

Security failures can be costly to business. Losses may result from the failure itself or from recovering from the incident, followed by more costs to secure systems and prevent further failure. In addition, a significant security failure can negatively affect the organization's competitive posture in the market place. Identifying and implementing key elements of information security management can prevent losses, save money and give the organization a competitive advantage.

3.4.2 Outcomes of Information Security Program Management

The information security manager's ultimate objective is not to completely eliminate all risk, but rather to ensure that the organization's information systems and resources are managed within an acceptable level of risk.

The information security manager has three basic options for dealing with risk:

- **Risk avoidance**—In the IT arena risk can never be altogether avoided because complete control in these environments is impossible to achieve because of less than perfect reliability in systems, applications and networks. Even if it were possible to gain complete control over the operation of computers, applications, network devices and so on, the fact that people must interact with them subjects them to insider risk.
- **Risk transfer**—Another option is to transfer risk to another entity, normally an insurance carrier, by getting insurance against financial losses caused by security-related incidents. If an organization were to suffer a massive denial-of-service attack that resulted in a US $2 million loss, for example, it would be reimbursed for this amount if it had the proper insurance policy in place. Note, however, that virtually every insurance company that issues policies that pay in the event of security-related incidents will not insure organizations that flunk a special security audit. An organization cannot get an insurance policy if it completely ignores risk.
- **Risk management**—Risk management involves considering three factors:
  - Asset value
  - Impact of loss
  - Likelihood of an event impacting that asset

Note: More information on risk management can be found at: *http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.*

In practical terms, this involves making difficult choices. The choices include:
- **Security control vs. ease-of-use**—An organization cannot afford for users to spend inordinate amounts of time using security controls. If a security measure is considered too onerous, management will withdraw it or users will work around it, which diminishes security rather than enhances it. In such situations, the more effective measure may have been the one that is a little weaker from a security control standpoint but more user-friendly.
- **Security vs. cost**—The cost of a security measure must be commensurate with both the value of the resource the measure protects and the likelihood that an adverse event will occur. It is not effective to spend US $100 to protect something that is worth only US $10.
- **Security vs. likelihood**—If the likelihood that an event will occur is miniscule (even if the impact were to be devastating), it may not be cost-effective to implement measures to prevent the event.
- **Security vs. impact**—If the impact of an event is miniscule (even if the likelihood is high), it may not be cost-effective to implement a measure to prevent the event.
- **Security vs. maintenance**—If a measure has high maintenance and support requirements, it may not be the best place to invest security resources. For instance, in a small organization with limited funds and insufficient staffing to monitor and respond to alarms issued by an intrusion detection system, it may be more effective to spend these funds on moderately priced protection measures, such as a firewall or strong identification and authentication, rather than on an expensive intrusion detection system.

However, the business case drives the extent to which a company needs to go for securing its assets. Thanks to the extensive dependence of companies on networking technologies, the primary focus of security initiatives is not to keep people away from computing and information resources, but rather to allow controlled, need-based access to the right people at the right time. The information security manager should be able to convince senior management of the need for security and obtain its mandate.

The ideal protection measure would be easy to use and inexpensive, protect highly valued resources from highly likely, high impact events, and require minimal maintenance and support. However, the real-world scenario often requires the information security manager to decide between two difficult options, for example:
- One measure is easy to use, but expensive; it protects against something with a high impact, but a low likelihood of occurrence.
- The other measure is both difficult to use and expensive, and protects against something with a moderate impact and a moderate likelihood of occurrence.

Security objectives to meet an organization's business requirements include the following:
- Ensuring the integrity of the information stored on its computer systems
- Preserving the confidentiality of sensitive data
- Ensuring the continued availability of their information systems
- Preventing nonrepudiation of electronic transactions and other computer-related activity
- Ensuring conformity to applicable laws, regulations and standards

3.4.3 Key Elements

For security to be successfully implemented and maintained, essential elements related to information security management must be established and communicated clearly to all appropriate parties. Key elements are presented in **figure 3.2**.

Figure 3.2—Key Elements of Information Security Management

Senior management commitment and support	This is the cornerstone for successful implementation and maintenance of an information security program. Without it, all other efforts are almost certainly doomed to fail.

Figure 3.2—Key Elements of Information Security Management (*cont.*)	
Policies	Security policy provides the overall framework for an information security program, with a general organization policy providing a concise top management declaration of direction. Topics addressed may include the importance of information assets, the need for security, and the importance of defining sensitive and critical assets to protect in regards to their confidentiality, integrity and availability requirements.
Roles and responsibilities	Once a policy has been approved by the governing body of the organization, the related roles are defined with responsibilities assigned for the different aspects of the information security program.
Standards	Standards are then established that govern development of minimum security baselines and guidelines.
Implementation	Policies and standards essentially define the security goals. Measures, practices, and procedures are then developed to meet those goals (i.e., enforcing policy and meeting standards). These measures, practices and procedures govern how individual systems are subsequently introduced and maintained, so that the security goals are achieved.
Organization	Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly defined. The information security policy should provide general guidance on the allocation of security roles and responsibilities in the organization. This should be supplemented, where necessary, with more detailed guidance for specific sites or services. Local responsibilities for individual physical and information assets and security processes, such as business continuity planning, should be clearly defined.
Communications	All defined and documented responsibilities and accountabilities must be established and communicated to all organizational personnel and management, and include conducting programs to increase security awareness and provide security training.

3.4.4 Summary of Tasks

The information security manager needs to develop and maintain plans for meeting the security requirements identified in the security strategy (as explained in chapter 1, Information Security Governance). The objectives of the plans should be accomplished via projects designed to implement and maintain appropriate security controls to mitigate risk; each project should have defined deliverables, milestones and budgets. Additionally, the information security manager needs to select and implement additional security countermeasures described in security baselines that specify the minimum acceptable security controls needed to protect assets, depending on their level of business criticality. Procedures and guidelines that ensure that business processes appropriately address information security risk need to be created and followed. The information security manager also needs to develop guidelines and procedures for IT infrastructure activities to comply with requirements in information security policies. Four types of controls—process, physical, platform and network controls—can be deployed. Appropriate architectures and security technologies must be used. Furthermore, effective information security programs are those in which security is considered throughout the entire life cycle activity. Through awareness and security policies the information security manager should leverage security awareness as well as policies to ensure that information security is adequately considered and integrated during each business process life cycle. The impact of security controls upon users must also be considered—testing is a particularly important activity in this regard. Avoiding deployment of controls that very negatively impact users and thus disrupt business processes is a paramount consideration. Developing and using

metrics to determine the effectiveness of controls is another component of information security management. Without suitable metrics, determining and communicating how well the information security governance framework is being implemented cannot be done with precision. Promoting accountability is still another critical part of information security management. Executive management needs to assume overall responsibility for information security. Business owners need to ensure appropriate security measures are consistent with organizational policy and maintained. Other entities also need to understand and accept responsibility for their roles in protecting an organization's assets. Finally, the ISM needs to manage both internal and external resources by making sure that both types of these resources are identified, appropriated and managed, and that proper acquisition management methods and techniques are put in place.

3.5 PLANNING

3.5.1 Creating and Maintaining Plans to Implement the Information Security Governance Framework

An information security governance framework is critical to the success of a security program. The ISM needs to develop a plan to:
- Define the framework
- Gain approval for the framework from senior management
- Implement the information security governance framework
- Monitor its progress and make changes as required

This plan should specify responsibilities for tasks and establish target dates for their completion. Depending on the size of the organization, the ISM may be responsible for most of the management tasks involved in this process. In a larger organization, the ISM may delegate some tasks to others in the IT and/or security departments.

The information security governance framework should also include the development and implementation of the security policy, security standards and guidelines.

3.5.2 Methods to Develop an Implementation Plan

The ISM should have an understanding of the methods available to develop and implement a security program. With the understanding of the organization's security requirements, as defined in the security strategy, the ISM should develop a plan for implementation of the security procedures to protect the information resources.

The ISM may either develop the implementation plan or use contractors/consultants to do so. In either case, the implementation plan should cover basic aspects including process, physical, platform and network areas. The implementation plan should also be based on accepted practices that will help the ISM to execute the plan more quickly.

As explained in chapter 2, Risk Management, the information security manager should first conduct a risk analysis that identifies the criticality levels of the information resources and the threats and vulnerabilities relevant to each resource. A matrix should be developed to depict how each information resource will be protected. This will help the ISM address the completeness of the implementation plan and make changes during this planning stage. Changes made during the implementation stage are less costly and more effective than those made after the security program has been implemented.

The ISM should also build performance measures into the implementation plan that can be used to determine if the security program meets its business objectives.

3.5.3 Project Management Methods and Techniques

Developing and implementing a security plan involves a number of variables, participating groups and tasks. Consequently, strong project management skills and effective tools are essential to the success of the overall security program.

The ISM should determine whether the organization in which information security resides has an established project management function. If it does, the information security manager should coordinate with that function to ensure that the security program complies with the organization's project management standards.
If the organization does not have an established project support function, the information security manager should employ generally accepted project management techniques, such as setting goals, measuring progress, tracking deadlines, and assigning responsibilities in a controlled and repeatable manner. This will help ensure that the security program's design and implementation will be successful.

Professional standards and certifications in the project management field can enhance the ISM's effectiveness.

3.5.4 Budgets

The security program implementation plan should be analyzed to estimate the level of effort and the resources required to carry out each task. At a minimum, the estimates for each task should consider the following elements:
- The overall scope of the effort (e.g., number of locations to be covered, types of business services offered, the IT infrastructure mix, extent of outsourcing), as described in the organization's information security policy
- Person hours by type (e.g., system analyst, programmer, clerical)
- Facility requirements (e.g., will the implementation of physical security require additional lighting, steel doors, card readers, guards?)
- Hardware/software requirements (e.g., firewalls, intrusion detection systems, penetration testing, monitoring tools)
- Training requirements (e.g., if an intrusion detection system will be installed, how much training will be needed?)

Having established a best estimate of expected work efforts by task (actual hours, minimum/maximum), budgeting becomes a two-step process to:
- Obtain a phase-by-phase estimate of level of effort and resources by summing the expected effort for the tasks within each phase
- Extend the summation of effort expressed in hours by the appropriate hourly rate to obtain a phase-by-phase estimate of security program implementation expenditure

Figure 3.3 illustrates the type of data required for the budget.

Figure 3.3—Security Program Budget Estimate

Phase	Task	Labor	Hrs	Rate	Cost
I	1. Risk assessment	Risk analyst	200	$100	$20,000
		Clerical support	50	$20	$1,000
		Office supplies/copies, etc.	N/A	N/A	$500
	Task 1—Total				**$21,500**
	2. Penetration testing	Technical personnel	75	$100	$7,500
		Clerical	50	$20	$1,000
	Task 2—Total				**$8,500**
Total Phase I					*$30,000*
II	1. Whatever	Risk analyst	200	$100	$20,000
		Clerical support	50	$20	$1,000
		Office supplies/copies, etc.	N/A	N/A	$600
	Task 1—Total				**$21,600**
	2. Whatever	Test techs	80	$100	$8,000
		Clerical	10	$20	$200
	Task 2—Total				**$8,200**
Total Phase II					*$29,800*
Grand Total					**$59,800**

3.5.5 Scheduling

While budgeting involves totaling the resources required to accomplish each task, scheduling involves establishing the sequential relationships among tasks and the time required to accomplish each task. Tasks need to be arranged according to:

- Earliest start date—Considering the logical sequential relationship among tasks, attempting to perform tasks in parallel whenever possible
- Latest expected finish date—Considering the estimated hours per task and expected availability of personnel or other resources, allowing for known elapsed time considerations (e.g., holidays, recruitment time, full-time/part-time employees)

The schedule can be represented graphically using various techniques, such as Gantt charts or PERT diagrams. At key points/milestones within the project, the budget and schedule should be revisited to assess the extent to which target dates and budget estimates are met to identify variances. Any variances to the budget and schedule should be analyzed to determine the cause and corrective action to take in minimizing or eliminating the total project variance. Variances and the variance analysis should be reported to management on a timely basis.

3.6 SECURITY BASELINES

3.6.1 Developing Information Security Baselines

An information security baseline means the minimum acceptable security controls to be implemented to protect information resources in accordance with their respective criticality levels. Developing information security baselines is one of the most important tasks in establishing the information security governance framework. The ISM should use security baselines to decide what additional measures need to be implemented to achieve and sustain that security baseline. Security measures include personnel, physical, management, technical and operational controls, including tools and procedures. Please note, however, that before determining security baselines, the ISM must establish the security policy, identify the relative criticality levels of the organization's information resources and assess the risk environment in which those resources operate.

Information security baselines should include a policy directive on data classification and data ownership. While data classification may not appear to be system-related, it plays a very important role in determining the extent of logical access that needs to be provided across the various components of an information systems environment.

A primary requirement for developing an information security baseline is to identify the control objectives that are sought to be achieved by the information security policy. COBIT guidelines can help in determining and firming up the control objectives at the outset.

Security baselines, particularly ISO/IEC 17799/BS 7799 (described as a "best practices" document), that have had a huge impact upon the current practice of information security and compromise a large piece of what might be called "the foundations of information security management."

Professional organizations such as the Information Security Forum regularly make survey-based results (also commonly called "baselines") concerning the types of controls available to its members. These results help member organizations adjust their controls posture, such that, for example, if they score considerably below their peers in authentication controls, they are likely to deploy more of them.

Two common sources for overall security baselines are the ISO/IEC 17799 and BS 7799, comprehensive sets of controls comprising best practices for information security management. With the International Organization for Standardization's update—ISO/IEC 17799:2005—in June 2005, a new series of standards known as the ISO/IEC 27000 series is dedicated to information security management systems. The 2005 version has 11 chapters instead of 10 as found in the previous version and has a total of 134 controls, including 17 new ones. By the end of 2005, BS7799-2:2002 will be replaced by ISO/IEC 27001.

Another source of security baselines can be found in the President's Critical Infrastructure Protection Board's *National Strategy to Secure Cyberspace* report. This report outlines more than 70 recommendations for security. In the US, the NIST, in collaboration with industry, has sponsored the development of Protection Profiles based on the Common Criteria. This is an additional example of how baselines can be established for products. Baseliners are also often defined by technology organizations, including hardware and software vendors. Vendors recommend security baselines based on the size and purpose of the hardware or software product. They are good resources for this type information, because they often have extensive knowledge of their security tools and are in the best position to recommend baselines to best utilize the tool in a secure manner. In the end, however, tools are a means to an end, not an end in themselves. The ISM must decide which recommendations are applicable and worth implementing. Finally, NIST has also written a widely used security baseline, NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.*[20] Additionally, legislation relating to information technology can shape security baselines. Many countries have enacted laws on issues such as copyright and software privacy, intellectual property and the confidentiality of personal data. These commercial, competitive and legislative pressures require the implementation of proper security policies and procedures and related system access controls.

3.6.2 Security Baselines and Configuration Management

Best practices suggest that information security can be employed most effectively by addressing security during the design, development and management of business applications and the infrastructure.

As various aspects of the organization's business applications and infrastructure are implemented across the enterprise, postimplementation security efforts become more complex. Therefore, the information security manager should work closely with the teams that design and manage the organization's infrastructure, configuration and business applications to ensure that they are aware of the security policy and the security baselines and that they meet the security requirements when they design, develop and manage business applications and infrastructure.

This approach also decreases the risks that any new or changed applications or infrastructure changes may adversely affect the security of the organization's information resources. This approach lets the ISM focus on enhancing and improving security rather than diverting resources to address vulnerabilities introduced by careless application or infrastructure changes. Time and resource permitting, the ISM must also from time-to-time review the application and infrastructure for gaps and vulnerabilities.

The NIST's Computer Security Resource Center develops guidance to increase secure IT planning, implementation, management and operation. Although this guidance is intended for US government systems, it is based on the international Common Criteria and is applicable in any IT environment. The 800 series of NIST Special Publications (SP) is particularly useful.[21]

3.7 BUSINESS PROCESSES

3.7.1 Ensuring Business Processes Address Information Security Risk

Business processes occur every day on a continuous basis. The most effective program for information security is one in which security is considered within each process. The information security manager should establish security policies and promote security awareness programs to ensure that information security is considered during each business process life cycle.

[20] See *csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf.*
[21] *http://csrc.nist.gov/*

As those responsible for developing and operating the business processes ultimately are responsible for the information they generate or use, they are the most qualified people to develop the priorities and identify what risks and impacts would occur if the organization's information resources were lost or corrupted. The information security manager should coordinate the security efforts with business process efforts. This is to ensure that information security is considered and that the information security function understands the organization's business needs so that appropriate security procedures can be designed and implemented. The overall security program must meet the business needs of the organization.

The ISM can accomplish this by instituting regular meetings with business process owners and documenting this approach in security guidelines that can be accepted and supported by senior management.

3.7.2 Security Procedures and Guidelines

All business processes and infrastructure activities occur in an environment subject to particular risks. It is incumbent upon the ISM to understand the business process, the infrastructure activities and the risk environment and to develop security guidelines and procedures to mitigate environmental risks.

3.8 INFRASTRUCTURE

3.8.1 IT Infrastructure Activities to Ensure Compliance With Information Security Policies

There are various definitions and implementations of IT infrastructure, depending on an organization's business objectives and how it uses technology. However, generally accepted components of IT infrastructure include process, physical, platform and network controls. Because a security system needs to consider users and others, personnel controls are an important consideration in developing an information security solution.

Each component has requirements for information confidentiality, integrity, availability and nonrepudiation. The ISM must consider these requirements for each component, not only individually but also collectively, and use them to determine the controls that are needed to adequately enforce the security policy and protect the organization's information, computing and networking resources.

The following are necessary controls to meet an organization's overall security policy:

- **Process controls**—The security policy and overall governance are key process controls. They are the foundation of the security program and are critical to the IT infrastructure.
- **Physical controls**—Physical controls are intended to restrict access to facilities (areas in which sensitive processes or activities take place) and other tangible information resources (hardware). Methods to keep unauthorized individuals from gaining access to tangible information resources include identification badges and authentication devices, such as smart cards or access controls, based on biometrics, security cameras, security guards, fences, lighting, locks and sensors. Physical controls are also intended to prevent or mitigate damage to facilities and other tangible resources that might be caused by natural or technological events (backup power sources can sustain operations if a hurricane damages the power lines serving the facility or if the power grid fails).
- **Personnel controls**—These controls are people-based. They include measures such as performing background checks on job applicants as well as individuals who hold positions requiring higher levels of trustworthiness and integrity than normal.
- **Platform controls**—These controls are technology-based and include things such as implementing security features in operating systems, implementing application-specific security controls (role-based access) or deploying adjunct security technology (such as virus/worm detection or intrusion detection/intrusion prevention systems).
- **Network controls**—These controls are technology-based and are focused on interfaces among the network components, such as firewalls, routers, switches, remote access (including VPNs) and any devices that monitor and restrict information traveling over the network.

3.8.2 Information Security Architectures

Since organizations rarely address security comprehensively and across the enterprise, it is likely that several information security architectures have been employed. The information security manager, therefore, needs to be aware of the various types of security architectures, their respective strengths and weaknesses, which particular ones are implemented in the organization, and how the various security architectures used within the organization are deployed. Some of the architectures include:

- Identity management (rules-based)
- Single sign-on
- List-based system access
- Points of systems administration
- Managed security
- Open systems
- Closed systems

The ISM must manage an enterprisewide security architecture and determine whether the organization should move toward implementing an enterprisewide security architecture.

3.8.3 Information Security Technologies

ISMs should be knowledgeable of proven security technologies, so they can select appropriate security measures to protect their organization's information resources. Several of these technologies include:

- Firewalls
- Network security features inherent in network elements (e.g., routers, switches)
- IDSs
- IPSs
- Cryptographic techniques (e.g., PKI, DES, etc.)
- Digital signatures
- Smart cards
- One-time passwords
- Wireless security
- Application security
- Remote access (VPNs, etc.)
- Web security techniques

The ISM should also be aware of emerging security technologies and techniques and take advantage of them to protect the organization's information resources. Embracing emerging technologies and techniques may help "raise the bar" for cybercriminals, because most attack tools and techniques target the more mature technologies. However, the ISM must also take into account the potential vulnerabilities that accompany emerging technologies, and take this into consideration in making any decisions regarding implementing such technologies.

3.8.4 Key Concepts for Architecture and Technologies

Today's networks are part of a large, inter-networked architecture of high-speed local and wide area computer networks serving organizations' client-server-based environments. These networks are usually centrally managed to facilitate more optimized network services by improving the efficiency of troubleshooting and performance management functions. Such architectures may include clustering common types of IT functions together in network segments, each of which is uniquely identifiable and specialized to task. For example, network segments or blocks may include web-based front-end application servers (public or private), application and database servers, and mainframe servers using terminal emulation software to allow end users to access these back-end legacy-based systems. In turn, end users can be clustered together within their own network LANs, but with capabilities to rapidly access corporate information resources. Within this environment, information is highly accessible and can be assumed to be available anytime and anywhere.

The types of networks common to most organizations are defined as follows:
- **Local area network (LAN)**—A nonpublic switched network that lies within a limited area providing services to a particular organizational group and using a specific type of network topology. Services provided by a network include web access, file transfers, e-mail, use of printer resources, terminal emulation, communications such as voice over IP, and much more.
- **Wide area network (WAN)**—A network of geographically dispersed subnetworks that provides network connectivity and services for LANs and other types of interconnected network segments.
- **Metropolitan area network (MAN)**—A type of network larger than a LAN, but smaller than a WAN that covers a metropolitan area. The Internet today is essentially comprised of many interconnected MANs, with various ISPs operating the MANs.

Implementing an integrated, efficient, reliable, scalable and secure network architecture of LANs and WANs with connectivity to the public Internet is a major challenge for organizations.

Critical success factors include the following:
- **Interoperability**—To support communication between systems composed of disparate technologies and multiple sites using different types of media and operating at differing speeds
- **Availability**—To provide continuous, reliable and secure service that meets the end users' requirements (in most cases 24/7)
- **Efficiency**—To provide the most effective way for network traffic to get from one part of the network to another
- **Flexibility**—To facilitate network scalability and accommodate network expansion and requirements for new applications and services

To accomplish the objectives of interoperability, availability, efficiency and flexibility, organizations must first define specifications for the types of networks (e.g., LANs/ WANs) that will create an integrated environment that will support their applications. They also must provide centralized support and troubleshooting over heterogeneous, but highly integrated systems. Network architecture standards facilitate this process by providing a reference model for designing an architecture for intercomputer and network communication processes. There are three major international organizations developing standards and specifications for protocols used in communications:
- The International Organization for Standardization (ISO)
- The IEEE, which produces standards used by computer manufacturers
- The International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) [formerly the International Telegraph and Telephone Consultative Committee (CCITT)], which produces standards for interconnecting different types of national and international public networks

The benchmark standard for this process, the Open Systems Interconnection (OSI) reference model, was developed by the ISO in 1984. The OSI is a proof-of-concept model composed of seven layers, each performing specialized tasks or functions. Each layer is self-contained and relatively independent of the other layers in terms of its particular function, enabling solutions offered by one layer to be updated without adversely affecting the other layers.

The objectives of the ISO/OSI model was to provide a set of open system standards for equipment manufacturers and to provide a benchmark to compare different communication systems, taking into account various protocols that can operate over the Internet Protocol (IP) used throughout the world. In effect, the ISO reference model was formulated as a template for the structure of communication systems.

The functions of the ISO/OSI layers are described as follows:
- **Application layer**—The application layer provides a facility for applications to communicate with the network (e.g., save files to the network, print files on a network printer, or receive data from the network). It thus acts as an interface to the network. In addition, it communicates the computer's available resources to the rest of the network. The application layer is distinct from, and should not be confused with, application software.
- **Presentation layer**—This layer performs transformations on data to provide a standardized application interface and to provide common communication services, such as encryption, text compression and reformatting. This layer provides representation of information: formats, codes, transformation and encryption. The function of the presentation layer is to ensure that the format of the data submitted by the application layer conforms to the applicable network standard and, if not, to convert the data to the correct format prior to passing the data to the

session layer. Conversely, when the presentation layer receives data from the network, it assesses the format of the data and, if necessary, converts it to the appropriate format required by the application layer.

- **Session layer**—The session layer controls the dialogs (sessions) between computers. It establishes the session by requesting it and providing the rules for communication. The session layer conducts the transfer of data and terminates the session once data transfer is complete. Because the rules for communication are established, the computers are able to communicate efficiently and are able to detect and deal with any errors.
- **Transport layer**—The transport layer provides reliable and transparent transfer of data between end points, end-to-end error recovery, and flow control (Windowing) for minimizing network congestion problems that may occur when data reaches its destination. Its duties include breaking down a message into packets, addressing the packets, forwarding them across the network, and acknowledging and reassembling them into the original message. This identifies how users get between points, (i.e., traffic within transmission). An important function of the transport layer is segment sequencing. This allows the transport layer to take segments (packets) received out of order and resequence them into the correct order.
- **Network layer**—The network layer addresses and delivers packets between networks. This is done through physical devices such as routers, and on the basis of the logical network address assigned to each network and the service address of the destination device. A network address differentiates one network from all other networks that may be interconnected. Service addresses (well-known service addresses are known as sockets or ports) allow the network to specify the destination program for which the data are sent. This layer also provides network management (routing, switching and traffic monitoring) and initiates an end-to-end pathway. This layer controls the packet routing and switching within the network, as well as to any other network, if applicable. Controls over network connections, logical channels, segmenting and sequencing, and data flow can be placed in this layer.
- **Data link layer**—This layer provides for the reliable transfer of data across a physical link for either LAN or WAN mediums. It sends blocks of data, called frames, using a variety of data link LAN/WAN protocols along with data fields that provide synchronization, bit error detection/correction error control, and flow control. A unique feature of the data link layer includes its ability to handle physical addressing through Media Access Control (MAC) addresses for communication with devices physically linked together in a network. Each device on the network has a unique MAC hardware address, which is normally assigned when manufactured.
- **Physical layer**—This layer concerns the physical aspects of networking. Electronic signals that traverse physical media, such as network cables, as well as signals sent over wireless channels and physical properties of networks and network interfaces are at this layer.

The OSI reference model is a proof-of-concept model only; in itself, it is not an actual method of communication. The actual implementation of the functions defined in each layer is based on protocols developed for each layer. A protocol is an agreed-upon set of rules and procedures to follow when implementing the tasks associated with a given layer of the OSI model.

Each layer in the OSI layers generally communicates with three other OSI layers:

- The layer directly above it
- The layer directly below it
- Its peer layer in other networked computer systems

This supports system-to-system communication (peer-to-peer relationships), where each layer on the sender side provides information to its peer layer on the receiving side.

Organizations use the OSI model in the design and development of their network architectures. This includes LANs, WANs, MANs and use of the public TCP/IP-based global Internet. The following sections will describe each type of network and how OSI concepts apply to them.

3.8.4.1 Local Area Networks

LANs are localized, packet-based switching networks within an organization that enable information resources to be shared within a relatively small, localized area, such as a specific business department in a networked campus environment. These networks were derived from information technology advances in the use of personal computers, which brought with it a heightened interest in the ability to exchange or share computerized data. LANs were developed to facilitate this exchange as well as sharing data, software, storage, printers and telecommunications equipment.

LANs are also characterized as high-speed fault-tolerant data networks, operating principally at the physical and data link layers of the OSI reference model. LANs facilitate the storage and retrieval of programs and data used by a group of people. LAN software and practices also need to provide for the security of these programs and data. Unfortunately, most LAN software provides a low level of security. The emphasis has been on providing capability and functionality rather than security. As a result, risks associated with use of LANs include:

- Loss of data and program integrity through unauthorized changes
- Lack of current data protection through inability to maintain version control
- Exposure to external activity through limited user verification and potential public network access from dial-in connections
- Virus infection
- Improper disclosure of data because of general access rather than need-to-know access provisions
- Violating software licenses by using unlicensed or excessive numbers of software copies
- Illegal access by impersonating or masquerading as a legitimate LAN user
- Internal user's sniffing (obtaining seemingly unimportant information from the network that can be used to launch an attack, such as network address information)
- Internal user's spoofing (reconfiguring a network address to pretend to be a different address)
- Denial of service or slowdowns due to flooding the LAN with packets, system crashes caused by fragmented packets, and failure of one or more network services
- Destruction of the logging and auditing data

LAN security provisions available depend on each software product, product version and implementation. Commonly available network security administration capabilities include:

- Declaring ownership of programs, files and storage
- Limiting access to a read-only basis
- Implementing record and file locking to prevent simultaneous update
- Enforcing user ID/password sign-on procedures, including the rules relating to password length, format and change frequency, or, better yet, requiring third-party authentication measures
- Limiting services to those required for business-related reasons

The use of these security procedures requires administrative time to implement and maintain. Network administration often is inadequate, providing global access because of the limited administrative support available when limited access is appropriate.

To gain a full understanding of the LAN, the information security manager should identify and document the following:

- LAN topology and network design
- LAN administrator/LAN owner
- Functions performed by the LAN administrator/owner
- Distinct groups of LAN users
- Computer applications used on the LAN
- Procedures and standards relating to network design, support, naming conventions and data security

LANs have many security implications, including numerous vulnerabilities. The administrative and control functions available with network software are often limited. Software vendors and network users have recognized the need to provide diagnostic capabilities to identify the cause of problems when the network goes down or functions in an unusual manner. The use of logon IDs and passwords with associated administration facilities is starting to become standard, although threats due to the sophistication of network attacks are starting to make the use of conventional passwords unadvisable.

Read, write and execute permission capabilities for files and programs are options available with some network operating system versions, but detailed automated logs of activity (audit trails) are seldom found on conventional LANs. Fortunately, newer versions of network software have significantly more control and administration capabilities.

LANs can represent a form of decentralized computing. Decentralized local processing provides the potential for a more responsive computing environment; however, organizations do not always take the opportunity to efficiently develop staff to address the technical, operational and control issues that the complex LAN technology represents. As a result, local LAN administrators frequently lack the experience, expertise and time to effectively manage the computing environment.

The various alternatives of media, protocol, hardware, transmission techniques, topology and network software help ensure that each LAN is unique. This mix of vendors and unique environments makes it difficult to implement standard management, operating and control practices. As a result, the costs of resolving problems can be substantial.

Normal LAN users recognize only one attribute of the LAN—it works. In a well-structured LAN, the unsophisticated user is not able to judge whether the technology is appropriate, the software is installed and documented properly, or necessary control and security measures have been taken. Audit trails are considered only after a problem occurs.

3.8.4.2 Wide Area Networks

A WAN is a data communications network that transmits information across LANs geographically dispersed among plant sites, cities and nations. A WAN can apply to the physical, data link and network layers of the OSI reference model. Its data flow can be simplex (one-way flow), half duplex (one way at a time) or full duplex (both ways at one time without turnaround delay). Also, a WAN's communication lines can be either switched or dedicated.

WAN message transmission techniques include:

- **Message switching**—Sending a complete message to the concentration point for storage and routing to the destination point when a communications path is available. Transmission cost is based on message length.
- **Packet switching**—A sophisticated means of maximizing transmission capacity of networks. It is accomplished by breaking a message into transmission units, called packets, and routing them individually through the network depending on the availability of a channel for each packet. Passwords and all types of data can be included within the packet. The transmission cost is by packet, not by message, route or distance. Sophisticated error and flow control procedures are applied to each link by the network.
- **Circuit switching**—A network switch circuit based upon traffic loads. Connections through a circuit-switched network, such as point-to-point (i.e., leased line) or multipoint, a public-switched telephone network (PSTN) or an integrated services digital network (ISDN) result in a dedicated physical communications channel being established between the calling and called subscriber equipment. This connection is then used exclusively by the two subscribers for the duration of the call. The network does not provide any error or flow control on the transmitted data, so this must be performed by the user.
- **Virtual circuits**—A logical circuit between two network devices that provides reliable data communications. Two types available are referred to as switched virtual circuits (SVCs) and permanent virtual circuits (PVCs). SVCs dynamically establish on-demand connectivity and permanently establish an always-on connection in which data transfer between network devices is constant.
- **WAN dial-up services**—Dial-up services using asynchronous and synchronous connectivity and are widely available and well-suited for organizations with a large number of mobile users. Its disadvantages are low bandwidth and performance.

Devices specific to WAN environments typically operate at either the physical or data link layer of the OSI reference model include the following:

- **Switches**—Data link layer devices used for implementing various WAN technologies, such as Asynchronous Transfer Mode (ATM,) point to point, frame relay, and ISDN. These devices are typically associated with carrier networks providing dedicated WAN switching and router services to organizations via T-1 or T-3 connections.
- **Routers**—Devices that operates at the network layer of the OSI reference model and interface outside of an organization's internal environment via carrier networks.
- **Modems (modulator/demodulator)**—Data communications equipment (DCE) devices that provide WAN connections for computers over a telecommunication network (generally the public telephone network). Modems convert computer digital signals into analog data signals that can be transmitted along the telecommunication lines. A modem on the other end of the line or link then converts the analog signal back into a digital signal.
- **Access servers**—Provide centralized access control for managing remote access dial-up services
- **Channel Service Unit/Digital Service Unit (CSU/DSU)**—Interfaces at the physical layer of the OSI reference model, data terminal equipment (DTE) to data circuit terminating equipment (DCE), for switched carrier networks
- **Multiplexors**—Physical layer devices that use several communication channels at the same time. A multiplexor allows a physical circuit to carry more than one signal at a time when the circuit has more capacity (bandwidth) than required by individual signals. It transmits and receives messages and controls the communication lines to allow multiple users access to the system. It can also link several low-speed lines to one high-speed line to enhance transmission capabilities.

Some common types of WAN technologies include:

- **Point-to-Point Protocol (PPP)**—The Internet standard for transmission of IP packets over serial lines. PPP supports asynchronous and synchronous lines. As a widely available remote access solution, PPP provides a single, preestablished WAN communication path from the customer's premises through a carrier network, such as a telephone company, to a remote network. PPP is widely available and is the most commonly used serial encapsulation method for remote access solutions. It is more stable than the older Serial Line Internet Protocol (SLIP). PPP operates over a wide range of media and was designed to simplify the transport of multiple protocols over serial links. PPP features include address notification, authentication, support for multiple protocols and link monitoring. Working in the data link layer, PPP makes use of two primary protocols for operation. The first, Link Control Protocol (LCP) is used when establishing, configuring and testing data link connections. The second, Network Control Protocol (NCP), establishes and configures different network layer protocols (e.g., IPX).
- **Frame Relay**—As a packet switched or virtual circuit implementation, Frame Relay is a data link layer protocol for switch devices that uses a standard encapsulation technique to handle multiple virtual circuits between connected devices. The encapsulation method is high-level data link control (HDLC) for synchronous serial links using frame characters and checksums. Frame Relay is more efficient than X.25, the protocol for which it is generally considered a replacement. Contrary to X.25, Frame Relay relies more on upper-layer protocols for significant error-handling processes in data transmissions. Frame Relay is a low cost, widely available LAN technology used in WAN point-to-point connections.
- **Integrated Services Digital Network**—As a circuit-switched implementation, ISDN corresponds to integrated voice, data and video, and is an architecture for worldwide telecommunications. This service integrates voice, data and video communication through digital switching and transmission over digital public carrier lines. The ISDN technologies now implemented are narrowband (basic-rate) ISDN and broadband ISDN. Separate channels are used for customer information (B channels—voice, data, and video) and to send signals and control information (D channels). ISDN uses a packet-node-layered protocol based on the CCITT's X.25 standard. Unlike Frame Relay, it is moderately available to all and relatively inexpensive.
- **Asynchronous Transfer Mode**—As a packet-switched implementation operating at the data link layer, ATM is based on use of a cell (fixed-size units) switching and multiplexing technology standard that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). Because ATM is asynchronous, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell. ATM is considered relatively expensive as a dedicated leased line option in comparison to other available WAN options.
- **Digital subscriber lines (DSL)**—A network provider service using modem technology over existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video. Characteristics of DSL include:
  - Dedicated, point-to-point, public network access on the local loop. Local loops are generally the "last mile" between a network service provider's (NSP's) central office and the customer site.
  - Delivers high-bandwidth data rates to dispersed customers at a low cost through the existing telecommunications infrastructure
  - Always-on access eliminates call setup, something that is ideal for Internet/intranet and remote LAN access (although it is not ideal from a security viewpoint, because it continually exposes systems to attacks).
- **Virtual private networks**—Extend the corporate network securely via encrypted packets sent out via virtual connections over the public Internet to distant offices, home workers, salespeople and business partners. Rather than using expensive, dedicated leased lines, VPNs take advantage of the public worldwide IP infrastructure, enabling remote users to make a local call (versus dialing-in at long distance rates) or use Internet cable modem or DSL connections for inexpensive public network connectivity. VPNs are platform independent. Any computer system that is configured to run on an IP network can be connected through a VPN with no modifications except for the installation of remote software.
- **Remote-access VPNs**—Used to connect telecommuters and mobile users to the enterprise's WAN in a secure manner. It lowers the barrier to telecommuting by ensuring that information is reasonably protected going through the Internet.
- **Intranet VPNs**—Used to connect branch offices within an enterprise WAN
- **Extranet VPNs**—Used to give business partners limited access to each others corporate network. One example of this would be an automotive manufacturer with its suppliers.

The only difference between a traditional, intracompany VPN (intranet) and an intercompany VPN (extranet) is the way the VPN is managed. With an intranet VPN, all network and VPN resources are managed by a single organization. When an organization's VPN is used for an extranet, management control becomes weak. It is thus good for the sake of security and control that each constituent company sharing the extranet VPN establish its own VPN.

VPNs allow:
- Network managers to cost-efficiently increase the span of the corporate network
- Remote network users to securely and easily access their corporate enterprise
- Corporations to securely communicate with business partners
- Supply chain management to be efficient and effective
- Service providers to grow their businesses by providing substantial incremental bandwidth with value-added services

Determining the network resources that should be linked via a VPN depends on the applications used on the various systems. Requirements often used to determine network connectivity include security policies, business models, intranet server access, application requirements, data sharing and application server access.

The process of encrypting packets to enable VPN technology to be a viable tool for organizations generally occurs through the Internet Engineering Task Force's (IETF's) IP Security (IPSec) standard (proprietary variants exist, but IPSec is the dominant standard). This standard enables the entire packet, including its header, to be encrypted in what is called the IPSec tunnel encryption mode. Another method, the transport mode, results in encryption of only the data portion of the packet. These encryption modes are representative of the encapsulation process whereby a new packet is created.

3.8.4.3 Wireless Networks

Wireless networks are an emerging and fast-growing type of networking that allow users to access information instantly via handheld wireless devices, such as mobile phones, pagers, two-way radios, smart phones and communicators. Wireless technology may also be used in desktops, for example, to provide a network connection without the need to install a communication media (copper, coaxial, etc.).

The protocol for this technology currently in use is referred to as the Wireless Application Protocol (WAP). WAP supports most wireless networks and is supported by all operating systems specifically engineered for handheld devices, including PalmOS, EPOC, Windows CE, FLEXOS, OS/9 and JavaOS. Handhelds that use displays and access the Internet run what are called microbrowsers—browsers with small file sizes that can accommodate the low-memory constraints of handheld devices and the low-bandwidth constraints of a wireless handheld network.

Because WAP is still fairly new, it is not a formal standard yet. It is an initiative that was started by Unwired Planet, Motorola, Nokia and Ericsson.

Wireless access general issues and exposures relate to:
- **The interception of sensitive information**—Information is transmitted through the air, so it increases the potential for unprotected information to be intercepted by unauthorized individuals.
- **The loss or theft of devices**—Wireless devices tend to be relatively small, making them much easier to steal or lose. A hacker can easily get at the information that is password- or PIN-protected.
- **The misuse of devices**—Devices can be used to gather information or intercept information that is being passed over wireless networks for financial or personal benefit.
- **The loss of data contained in the devices**—The size of the devices makes them prone to theft or loss. This can result in the loss of data that has been stored on these devices. Storage capacity ranges from 2 Mb to 128 Mb plus, depending on the device. In the future, these devices will have a storage capacity in the range of 50-80 Gb.
- **Distractions caused by the devices**—The use of wireless devices can result in distractions to the user. If these devices are being used in situations where an individual's full attention is required (e.g., driving a car), they could result in an increase in the number of accidents.
- **Possible health effects of device usage**—There are currently a number of concerns with respect to electromagnetic radiation especially for those devices that must be held beside the head for use. The safety or health hazards have not yet been identified or verified.

- **Spamming**—Wireless networks are often used by unauthorized individuals to send spam.
- **Wireless user authentication**—There is a need for stronger wireless user authentication and authorization tools at the device level. The current technology is just emerging.
- **File security**—Wireless phones and PDAs do not use the type of file access security that other computer platforms can provide.
- **Wired Equivalent Privacy (WEP) security encryption**—WEP security can be overwhelmed and broken without a great deal of effort. The 64-bit encryption keys that are in use in the WEP standard can be broken easily by the currently available computing power. Because all the users of a given access point share the same encryption key, once it is broken all of the information is available for viewing and use. To achieve mobility in a campus environment, all clients must be set to the same transmission key and all clients must use the same encryption key. An attacker possessing the WEP key could sniff packets from the airwaves and decrypt them. Two important standards, IEEE 802.1x and IEEE 802.11, specify much stronger encryption for wireless transmissions than in WEP.
- **Interoperability**—Most vendors offer 128-bit encryption modes. However, they are not standardized, so there is no guarantee that they will interoperate. The use of the 128-bit encryption key has a major impact on performance with 15-20 percent degradation being experienced. Some vendors offer proprietary solutions; however, this only works if all access points and wireless cards are from the same vendor.
- **The use of wireless subnets**—To increase security, it is possible to create special subnets for wireless traffic and require authorization before packets are routed. Subnets can be created via a VLAN. VLANs in the wireless environment have not reached maturity, so are still unproven.

The major vulnerabilities of wireless access are:

- **Translation point**—Location where information being transmitted via the wireless network is converted to the wired network. At this point the information, which has been communicated via the WAP security model using the Wireless Transport Layer Security, is converted to the Secure Socket Layer (SSL), where the information is decrypted and then encrypted again for communication via TCP/IP.
- **Bluetooth Wireless Personal Gateway**—A communications protocol where it is possible to synchronize with not only the device that it is intended to communicate but also any other device in a close proximity. This also is true with regards to some of the infrared communications devices that are currently in use.

There are several major areas of concern regarding emerging wireless technology controls.

- **Authentication and logging**—There is a need to manage and control the information that is accessed by mobile users. For the sake of security all transactions should be adequately encrypted and logged so that management can be sure who accessed information and when.
- **Application persistence for acceptable levels of availability**—Currently normal communication interruptions can disrupt existing transport protocol implementations and cause user applications to either backup or terminate.

The best single solution for wireless security is to upgrade wireless networks to the IEEE 802.11i protocol. This protocol uses the 802.1x/Extensible Authentication Protocol (EAP) for authentication as well as much stronger encryption (64-bit RC4 encryption for authentication, 128-bit RC4 encryption for authentication). It also effectively guards against the threat of breaking the content of WEP wireless transmissions into cleartext.

Wireless technology is still an emerging technology with tremendous growth potential. However, wireless businesses, enabling e-solutions to organizations, will encounter barriers that must be addressed. For example, existing applications may need to be retrofitted to make use of wireless interfaces; network standardization needs to occur so that wireless devices using different operating systems can communicate with one another; and decisions need to be made regarding general connectivity for developing completely wireless mobile applications or applications that rely on synchronization as the conduit for data transfer between mobile computing systems and corporate infrastructure. Other issues include narrow bandwidth, lack of mature standard, conflicting corporate agendas, and unresolved security and privacy issues.

3.8.4.4 Metropolitan Area Networks

A MAN is a support network that exists in a metropolitan area and is regulated by local commissions. Telephone companies, cable television services and other vendors provide MAN services for enterprises that require network construction through cities. In general, these types of networks use the IEEE 802.6 standard. MAN networks commonly use broadband ISDN or ATM technology.

MANs can support several services, such as LAN-to-LAN connections, PBX connections, direct links to work stations and central computer connections. In other words, a MAN is a voice and integrated data network that provides one of the following characteristics:

- Package and circuit commutation services
- Services that are not connection-oriented
- Connection-oriented services over virtual circuits
- Services that relate to asynchronous transmission over a synchronous data link and that guarantee constant sensible data transportation as well as logic connections (e.g., necessary for multimedia streams for synchronizing audio and video data signals)
- Compatabiltiy with the IEEE LAN norms and supports traffic according to the IEEE 802.2 standard of logic link control

3.8.4.5 Public "Global" Internet Infrastructure

The Internet is comprised of networks that connect to one another via pathways that allow the exchange of information, data and files. Being connected to the Internet means having access through these pathways to other computers connected to the Internet. Using these pathways, a computer can send packets of data to other computers and networks.

Today, the Internet is a vast, global network. It is the purest form of electronic anarchy. Networks communicate with each other using certain protocols, such as the Transmission Control Protocol and Internet Protocol TCP/IP). It connects many networks, ranging from university networks to corporate LANs to large online services. Every time a computer connects to the Internet, it becomes an extension of that network.

Users can access the Internet through either a LAN at a place of business or by dialing into a computer connected to the Internet via an online service or a dial-in ISP. Routers and switches, which connect networks, perform most of the work of directing traffic on the Internet. Routers examine the packets of data traveling across the Internet to see where the data are headed. Based on the data's destination, routers and switches direct them to the most efficient route (generally to another router), which in turn sends it to the next routing point and so on. Networks are connected in many different ways. There are dedicated telephone lines that can transmit data at up to 56 kilo bits per second. There are an increasing number of T-1 leased lines that can carry 1.544 Mbps of data. Higher-speed T-3 links, which can carry data at 44.746 Mbps, are used as well. Satellites can also link networks, as can fiber-optic cables or ISDN telephone lines.

The networks in a particular geographic area are connected into a large regional network. Regional networks are connected to one another via high-speed backbones (connections that can send data at extremely high speeds). When data are sent from one regional network to another, they first travel to a network access point (NAP). NAPs then route the data to high-speed backbones, such as the high-speed backbone network service (BNS), which can transmit data at 155 Mbps. The data are then sent along the backbone to another regional network and then to a specific network and computer within that regional network.

3.8.4.6 TCP/IP Internet World Wide Web Services

The most common way users access resources on the Internet is through the TCP/IP Internet World Wide Web (WWW) application service. This Internet application service is the fastest growing and most innovative part of the Internet. When the user browses the web, they view multimedia pages composed of text, graphics, sound and video. The web uses hypertext links that allow users to jump from any place on the web to any other place on the web. The language that allows the user to use hypertext links and to view web pages is called Hypertext Markup Language (HTML). The web works on a client-server model in which client software, known as a web browser, runs on a local computer. The server software runs on a web host, usually an NT or UNIX server. Users utilize a web browser, such as Microsoft Internet Explorer or Netscape Navigator, to access resources on the web.

Another term associated with access and use of the WWW service is the Uniform Resource Locator (URL), which identifies the address on the WWW where a specific resource is located. To access a web site, a user enters the site's location into their browser's URL space, or they can click on a hypertext link that will send them to the location. The web browser sends the request via the Hypertext Transfer Protocol (HTTP). This protocol defines how the web browser and web server communicate with one another.

URLs contain several parts. An example of a URL is *http://www.isaca.org/cert1.htm*. The *http://* details which Internet protocol to use. The *www.isaca.org* identifies the server to be contacted. Usually the first part of the server name ("www" in this case) identifies the kind of Internet resource that is being contacted or addresses several servers in the same "domain" (*isaca.org*), such as: web1, web2, ftp1, ftp2. The cert1.htm identifies a specific directory on the server, a home page, document or other object with the server.

The URL can also be used to access other TCP/IP Internet services (i.e., *ftp://isaca.org*, *telnet://isaca.org*).

The request is sent over the Internet. Routers examine the request to determine where to send the request. The information just to the right of the http:// in the URL reveals the web server on which the requested information can be found. The routers transfer the request to that web server, and the web server receives the request using HTTP. It is told which specific document is being requested. When the server finds the requested home page, document or object, it sends it back to the web browser. The information is then displayed for the user. After the page is sent by the server, the HTTP connection is closed and can be reopened.

3.8.4.7 Applications in a Networked Environment

Use of client-server technology is one of the most popular trends in application development used in networked environments. More and more business applications have embraced the advantages of the client-server architecture, such as distributing the work among servers and performing as much computational work as possible on the client workstation. This allows the users to manipulate and change the data that they need to change without controlling resources on the main processing unit.

In client-server systems, applications no longer are limited to running on one machine. The applications are split so that processing may take place on different machines. The processing of data takes place on the server and the desktop computer (client). The application is divided into pieces or tasks so processing can be done more efficiently.

In a client-server network environment, one computer acts as the server and provides data distribution and security functions to other computers that are independently running various applications. An example of the simplest client-server model is a LAN in which a set of computers is linked to allow individuals to share data, peripheral equipment and software. LANs (like other client-server environments) allow users to maintain individual control over how information is processed.

Client-server network technology involves the allocation of data processing resources in a network, so that computing power is distributed among workstations. This type of computing allows integrated applications to share system and data resources. Client-server processing differs from mainframe or distributed system processing in that each processing component is mutually dependent. The client is a single PC or workstation associated with software that provides a graphical interface to server computing resources. Presentation usually is provided by visually enhanced processing software known as a graphical user interface (GUI). The server is one or more multiuser computer (these may be mainframes, minicomputers or PCs). Server functions include any centrally supported role, such as file sharing, printer sharing, database access and management, communication services, facsimile services and application development. Multiple functions may be supported by a single server.

When addressing client-server architecture, it is important to consider two- and three-tier architectures. A two-tier client-server architecture defines just two parts: a client, which includes a front-end program (developed using popular tools like Visual Basic, Power-Builder, Delphi or a similar program) and a database server or back-end program. The front-end program is in charge of two types of tasks: those related to the GUI and those related to business rules and application logic (data validation, computations, decisions, etc.).

The main limitations with a two-tier architecture are:

- As the application logic is increasingly complex, the program is bigger and requires more memory and CPU power to do the job (the fat-client syndrome).
- As more concurrent users (normally between 50 and 200) are added, different performance problems and bottlenecks will appear (mainly related to managing hundreds of concurrent connections). So this architecture is not highly scaleable.

A three-tier architecture is composed of a thin client, focused on doing GUI tasks (could be an Internet browser), and a group (one or more) of application servers, focused on running the application logic. These servers could run programs generated in JAVA (called servlets) or with other development tools.

The main advantages of this three-tier, client-server architecture are:
- Thin clients
- More scalability (up to several thousands of concurrent users), because the load is being balanced between different servers
- Its ability to be implemented in internal applications or e-business applications (in this case we could have another tier represented by the web server)
- The separation of all the program logic from the rest of the code (via application servers)

Note: Implicit in two- to three-tier architectures is the presence of middleware that supports not just the communications between clients and servers, but the more advanced features, such as load balancing and fail over, dynamic location of components, and establishing synchronous connections or asynchronous queue-based messages.

3.8.4.8 Middleware

Middleware is a client-server-specific term used to describe a unique class of software employed by client-server applications. It serves as glue between two otherwise distinct applications. It provides services such as identification, authentication, authorization, directories and security. This software resides between an application and the network and manages the interaction between the GUI on the front end and data servers on the back end. It facilitates the client-server connections over the network and allows client applications to access and update remote databases and mainframe files.

The major risk associated with middleware in a client-server environment is that system integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in loss of data or program integrity. Management should implement compensating controls to ensure the integrity of the client-server networks. Systems need to be tested properly and approved and any modifications need to be authorized and implemented properly. Management should also ensure that proper version control procedures are followed.

3.8.4.9 Client-server Security

A client-server system typically contains numerous access points. Security procedures for these server environments are usually not as well understood or as protected as a mainframe-based processing environment. Client-server systems utilize distributed techniques, creating increased risk of access to data and processing. To effectively secure the client-server environment, all access points should be identified. In mainframe-based applications, centralized processing techniques require the user to go through one predefined route to access all resources. In a client-server environment, several access routes exist, as application data may exist on the server or on the client. Each of these routes, therefore, must be examined individually and in relation to each other to determine that no exposures are left unchecked. To increase the security in a client-server environment, an information security manager may want to see that the following control techniques are in place:
- Securing access to the data or application on the client-server may be performed by disabling the floppy disk drive, much like a keyless workstation that has access to a mainframe. Diskless workstations prevent access control software from being bypassed and rendering the workstation vulnerable to unauthorized access. By securing the automatic boot or startup batch files, unauthorized users may be prevented from overriding login scripts and access.
- Network monitoring devices may be used to inspect activity from known or unknown users. These devices may identify client addresses, allowing proactive session termination as well as finding evidence of unauthorized access for later investigation. However, the method of securing the client-server environment may be only as good as the administrator who monitors it. Since this is a detective control, if the network administrator does not monitor or maintain these devices, the tool becomes useless against unauthorized intruders.
- Data encryption techniques (symmetric or asymmetric encryption) can help protect sensitive or proprietary data from unauthorized access.

- Authentication systems may provide environmentwide, logical facilities that can differentiate among users. Another method, system smart cards, uses intelligent handheld devices and encryption techniques to decipher random codes provided by client-server systems. A smart card displays a temporary password that is provided by an algorithm on the system and must be reentered by the user during the login session for access into the client-server system.
- The use of application-level access control programs and the organization of end users into functional groups is a management control that restricts access by limiting users to only those functions needed to perform their duties.

The use of client-server technology enables business units to develop and deliver products and services to market much more quickly than traditional legacy methods. The trade-off is that controls over these systems typically are substandard compared to those associated with traditional mainframe systems. There are higher risks that can severely impact a company's business if controls are not in place to prevent or detect them.

The areas of risk and concern in a client-server environment are listed below:
- Access controls may be weak in a client-server environment if network administrators do not set up password change controls or access rules properly.
- Change control and change management procedures, whether they are automated or manual, may be inherently weak. The primary reason for this weakness is the relatively high level of sophistication of client-server change control tools together with inexperienced IS staff, who are reluctant to introduce such tools for fear of introducing limitations on their capability.
- The loss of network availability may have a serious impact on the business or service.
- Obsolescence of the network components, including hardware, software and communications
- Unauthorized and indiscriminate use of synchronous and asynchronous modems to connect the network to other networks
- Connection of the network to public switched telephone networks
- Inaccurate, unauthorized and unapproved changes to systems or data
- Unauthorized access to confidential data, the unauthorized modification of data, business interruption, and incomplete and inaccurate data
- Application code and data may not be located on a single machine enclosed in a secure computer room, as with mainframe computing.

3.8.4.10 Internet Threats and Security

The nature of the Internet makes it vulnerable to attack and poses significant security problems for organizations that want to protect their information assets. For example, hackers and virus or worm writers try to attack the Internet and computers connected to the Internet. Some want to invade others' privacy and attempt to crack into databases containing sensitive information or sniff information as it travels across Internet routes. Consequently, it becomes more important for information security managers to understand the risks to ensure that proper controls are in place when a company connects to the Internet.

One class of network attack involves probing for network information. These passive attacks can lead to active attacks such as intrusions/penetrations into an organization's network. By probing for network information, the intruder obtains network information that can be used to target a particular system or set of systems during an actual attack.

Examples of passive attacks that gather network information include:
- **Network analysis**—The intruder applies a systematic and methodical approach known as "foot printing" to create a complete profile of an organization's network security infrastructure. During this initial reconnaissance phase, the intruder uses a combination of tools and techniques to build a repository of information about a particular company's internal network. This often includes information about system aliases, functions, internal addresses and potential gateways and firewalls. Next, the intruder focuses on systems within the targeted address space that responded to these network queries when the attackers have targeted a system for an actual attack. Once a system has been targeted, intruders scan the system's ports to determine the services and operating system that are running on the targeted system, possibly revealing vulnerable services that could be exploited.
- **Eavesdropping**—Intruders often also gather the information flowing through the network with the intent of acquiring and releasing the message contents for either personal analysis or for third parties who might have commissioned such eavesdropping. This is particularly significant because when sensitive information, including e-mail, passwords and, in some cases, keystrokes, traverses most networks, it can be seen by all other machines in

real time. These activities can help the intruder gain unauthorized access, use information such as credit card accounts fraudulently, and compromise the confidentiality of sensitive information that could jeopardize or harm an individual or an organization's reputation.

- **Traffic analysis**—Intruders also determine the nature of traffic flow between defined hosts and, through an analysis of session length, frequency and message length to guess the type of communication taking place. This type of analysis is typically used when messages are encrypted and eavesdropping would not yield any meaningful results. For example, intruders on law enforcement agency communication networks have often been able to predict major action being contemplated by using traffic analysis methods.

Once enough network information has been gathered, the intruder will launch an active attack against a targeted system to either gain complete or partial control over that system or cause denial or disruption of services. This may include obtaining unauthorized access to modify data or programs, flooding the target system with fragmented packets, escalating privileges, accessing other systems, and obtaining sensitive information for personal gain. These are known as active attacks. They affect integrity, availability and/or confidentiality, and may also result in false repudiation of electronic transactions. Common forms of active attacks may include any of the following:

- **Brute force**—In a brute-force attack, the attacker enters one password after another for a targeted account. Brute-force attacks are often launched by scripts that try many thousands of candidate passwords. The fact that many systems have well-known accounts, such as the system administrator account in Microsoft SQL Server, greatly increases the probability that brute-force attacks will succeed.
- **Password cracking**—An intruder launches an attack, using many of the password cracking tools that are widely available (usually for free). These tools take a large number of potential passwords for each account and encrypt them using the same encryption algorithm that the target system uses to encrypt passwords. If any encrypted candidate matches one in the password file, the password has been cracked. The attacker logs in using the cracked password to gain unauthorized access.
- **Masquerading**—An active attack in which the perpetrator assumes a false identity. In this attack, the purpose is to gain access to sensitive data or computing/network resources to which access is not allowed under the original identity. In one type of masquerading attack the attacker allows a normal session authentication to take place and later enters the information flow masquerading as the authenticated user, something that can allow the attacker to gain control of the session. IP addresses can also be forged. Sending packets with false addresses is referred to as IP spoofing. This form of attack often is used in connection with widespread vulnerability scans launched by attackers. If many of the scans are from spoofed IP addresses, the chances of tracing the origin of the scans diminishes substantially.
- **Packet replay**—This is a combination of passive and active modes of attacks. The intruder passively captures a stream of data packets as it moves along an unprotected or vulnerable network. These packets are then actively inserted into the network as if it were another genuine message stream. This form of attack is effective particularly where the receiving end of the communication channel is automated and will act on receipt and interpretation of information packets without human intervention.
- **Message modification**—Modification involves capturing a message and making unauthorized changes or deletions (of full streams or parts of the message), changing the sequence, or delaying transmission of captured messages. This could have disastrous effects if, for example, the message were an instruction to a bank to pay money.
- **Unauthorized access through the Internet or web-based services**—Many services used in connection with the Internet contain vulnerabilities that render systems subject to attack. Additionally, many of these systems are large and difficult to configure, resulting in a large percentage of unauthorized access incidents. Examples include:
  - E-mail forgery using the Simple Mail Transfer Protocol (SMTP)
  - Telnet passwords transmitted in the clear (via a path between client and server)
  - Altering the binding between IP addresses and domain names to impersonate any type of server. As long as Domain Name Service (DNS) is vulnerable and is used to map URLs to sites, there can be no integrity on the web.
  - Exploiting bugs in Common Gateway Interface (CGI) scripts on web servers. CGI scripts are often not written with security in mind, and web servers often have default CGI scripts with well-known vulnerabilities.
  - Client-side execution of scripts (via JAVA in JAVA Applets), which presents the danger of running code from an arbitrary location on a client machine
- **Denial of service**—Denial-of-service attacks occur when a computer connected to the Internet is flooded with data and/or requests that must be serviced. The machine becomes so busy dealing with these messages that it is rendered useless. Well advertised after a series of successful attacks on well-known web resources, this form of attack is more about frustrating or creating a financial loss for the owner of the network resource rather than any direct financial

gain for the attacker. However, this type of attack can be particularly devastating if critical information systems are down for a prolonged period of time. At the end of a successful attack of this nature, the attacked network resource is paralyzed and unavailable for genuine users. This disruption can be achieved through a variety of means. The most common is to overload the resource with requests that overwhelm the system so that it ceases to function. Common types are:
  - Killing user processes
  - Flooding the machine with connections requests (SYN floods) or fragmented packets
  - Filling up disk or memory
  - Isolating machine through DNS attacks
- **Dial-in penetration attacks (i.e., war dialing)**—An intruder determines the dial-in phone number ranges from external sources such as the Internet. The intruder also may employ social engineering tactics to get information from a company receptionist or obtain the information from a knowledgeable employee inside the company.
- **E-mail bombing and spamming**—E-mail bombing is characterized by abusers repeatedly sending an identical e-mail message to a particular address. E-mail spamming is a variant of bombing; it refers to sending e-mail to hundreds or thousands of users (or to lists that expand to that many users). E-mail spamming can be made worse if recipients reply to the e-mail (such as clicking on what appears to be an "opt-out" function that claims to remove the recipient from the spammer's mailing list), causing all the original addressees to receive the reply. It also may occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of an incorrectly set up responder message, such as a vacation message. E-mail bombing/spamming may be combined with e-mail spoofing, which alters the identity of the account sending the e-mail, making it more difficult to determine from whom the e-mail is coming.
- **E-mail spoofing**—E-mail spoofing may occur in different forms, but all have a similar result: a user receives an e-mail that appears to have originated from one source when it was actually sent from another source. E-mail spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information, such as passwords. Examples of spoofed e-mail that could affect the security of a site include:
  - E-mail claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their accounts if they do not do this
  - E-mail claiming to be from a financial institution requesting users to enter an account or PIN number or other sensitive information—a "phishing" attack

To establish effective Internet security controls, an organization must develop controls within an information systems security framework from which these controls can be implemented and supported. Generally, the process for establishing such a framework entails defining the rules the organization will follow to control Internet usage and establishing corporate policies, guidelines and procedures to implement those rules. For example, one set of rules should address appropriate use of Internet resources with rules that might reserve Internet privileges for those with a business need, define what information resources should be available for outside users, and define trusted and untrusted networks within the organization and external to the organization.

Another set of rules should address the classification of the sensitivity or criticality of corporate information resources. This will help to determine what information will be allowed to be available for use on the Internet and the level of security to be used for corporate resources of a sensitive or critical nature on the Internet.

Building on these rules, an organization then develops guidelines specific to their situations for defining the level of security control related to the confidentiality, integrity and availability of information resources (e.g., business applications) and nonrepudiability of electronic transactions on the Internet. For example, operating system security hardening guidelines can be developed that define how an operating system should be configured, specify which Internet services should be blocked from use or exploitation by external untrusted users, and define how the system will be protected by firewalls. Additionally, supporting processes over these controls should be defined, including:
- Risk assessments performed periodically over the development and redesign of Internet-based web applications
- Security awareness and training for employees, tailored to their levels of responsibilities
- Firewall standards and security to develop and implement firewall architectures
- Intrusion detection and intrusion prevention standards and security to develop and implement IDS and IPS architectures
- Remote access for coordinating and centrally controlling dial-up access on the Internet via corporate resources
- Incident handling and response for detection, response, containment and recovery

- Configuration management for controlling the security baseline when changes do occur
- Encryption techniques applied to protect information assets passing over the Internet in cleartext
- Common desktop environment to control what is displayed on an employee's desktop
- Monitoring Internet activities for unauthorized usage and notification to end users of new vulnerabilities and security incidents via CERT bulletins or alerts

In summary, Internet usage has drastically changed the way business is done and has created opportunities for organizations to compete in what has become a global virtual market. To compete and survive in this new marketplace, organizations have to reconsider the way they regard security to address Internet-related threats.

3.8.5 Firewalls

A firewall is a device installed at the point where network connections enter a site that applies rules to control the type of inbound and outbound networking traffic. Most commercial firewalls are built to handle the most commonly used Internet protocols as well as others. Every time a corporation connects its internal computer network to the Internet, it faces potential danger. Companies should implement firewalls as one means of perimeter security for their networks. Likewise, this same principle holds true for very sensitive or critical systems that need to be protected from untrusted users inside the corporate network (internal attackers).

To be effective, firewalls should allow individuals on the corporate network to access the Internet and, at the same time, stop attackers or others on the Internet from gaining access to the corporate network to cause damage. Generally, most organizations follow a default deny-all philosophy, which means that access to a given resource will be denied unless someone can provide a specific business reason or need for access to the information resource. The converse of this access philosophy, not widely accepted, is the default accept all philosophy in which everyone is allowed access unless someone can provide a reason for denying access.

Firewalls come in many varieties. Some are hardware devices with stripped down functionality—appliance firewalls. Others consist of hardware and software that selectively filters and logs incoming and outgoing network traffic (much like a router) and applies rules. Both of these types of firewalls are primarily perimeter firewalls in that they are generally used to create what is frequently called a "security perimeter" around a network, shielding it from attacks launched by external hosts. Still others, personal firewalls, consist only of software that filters and logs incoming traffic on individual hosts. Perimeter firewalls should control the most vulnerable points between a corporate network and the Internet, and they can be as simple or complex as corporate information security policy demands. There are many different types of firewall functions, including:

- Blocking access to particular IP addresses
- Limiting traffic on an organization's public services segment to certain addresses and ports within that organization's internal network
- Preventing certain users from accessing certain servers or services
- Monitoring traffic between an internal and an external network
- Monitoring and recording all communications between an internal network and the outside world to investigate network attacks
- Encrypting packets that are sent between different physical locations within an organization by creating a VPN over the Internet (i.e., IPSec VPN tunnels)

Firewalls are frequently deployed as bastion hosts in that they handle all incoming requests, such as File Transfer Protocol (FTP) and web requests, from the Internet to internal networks. Bastion hosts are heavily fortified against attack, thereby creating a security perimeter that protects internal hosts. None of the computers or hosts on the corporate network can be contacted directly as the result of requests from the Internet, something that provides an effective layer of security for the entire network. Because only a single bastion host needs to be deployed (although many organizations deploy two firewalls at the external gateway to each of their networks), it is easier to maintain security and track attacks. Finally, firewalls deployed at external gateways allow for the establishment of DMZs, network segments at external gateways that do not have the same levels of controls as internal networks. DMZs serve as good locations for publicly accessible servers that, if placed within an organization's internal network, would generally present an unacceptable level of security risk. Placing a publicly accessible web server deep in an internal

network might, for example, be catastrophic to other hosts within the same network if that server were compromised. Placing the web server within a DMZ will expose it to a higher level of security threat, but it will also help limit the threat to other hosts within the network if that server were to become compromised.

Generally, the types of firewalls available today fall into three categories: packet filtering, stateful inspection, and application firewalling.

3.8.5.1 Packet Filtering Firewalls

The simplest and earliest kind of firewall (i.e., the first generation of firewalls) is the packet filtering firewall. A packet filtering firewall, examines the header of every inbound packet to the corporate network and often also every outbound packet. Packet headers contain information, including the IP address of the sender and receiver, the source and destination port numbers, and type of protocol, that enables a packet filtering firewall to selectively screen each packet. For example, the firewall could block any traffic except for e-mail or could block traffic to and from certain source or destination IP addresses.

The main advantages of this type of firewall are its simplicity and performance. Filtering rules are performed at the network layer; the analysis of network traffic is rudimentary compared to other types of firewalls. Packet filtering firewalls are also usually easiest to implement and maintain.

The simplicity of packet filtering firewalls is also a disadvantage in several ways. The simplicity of analysis allows potentially dangerous traffic that would be blocked by more sophisticated firewalls to get past the firewall and ultimately to hosts that might be successfully attacked.

3.8.5.2 Stateful Inspection Firewalls

A stateful inspection firewall (sometimes simply called a stateful firewall) keeps track of ongoing connections that go through it using a state table. Stateful firewalls do not let incoming TCP packets with the SYN/ACK or ACK flags get through. Instead, they inspect their state table to see if a connection from the indicated source address has already been established. If so, the packets are allowed through; if not, the packets are dropped.

The main advantage of stateful firewalls over packet filtering firewalls is that they analyze packets at the transport layer. Thus, they prevent bogus packets that appear to be part of an ongoing session from getting through. Real-life stateful firewall implementations also analyze packets at the network layer, thus enabling them to drop packets on the same basis as packet filtering firewalls do. Stateful firewalls thus provide two layers of protection, something well-suited to a defense in depth approach. Another advantage of stateful firewalls is that they are less-complex than application firewalls (to be covered next) and thus generally have better performance.

A disadvantage is that stateful inspection firewalls can be relatively complex to administer compared to packet filtering firewalls. Additionally, although they are more sophisticated in their functionality than packet filtering firewalls, stateful firewalls are not as sophisticated as application firewalls.

3.8.5.3 Application Firewalls

Application firewalls provide the greatest degree of control of all types of firewalls. As the name implies, application-level firewalls works at the application layer. This type of firewall is aware of the appropriate types of input for applications running on hosts within an organization's internal network. If input sent to these applications is inappropriate (as in the case of buffer overflow exploitation attempts, in which excessive input is sent in an attempt to overflow part of the input into memory), the firewall drops the connection. A proxied connection, usually simply called a "proxy," is a special type of store-and-forward connection to the firewall that terminates there. The firewall then forms a new connection with the same session characteristics to the destination host, if the original connection is allowed. The result is that information flows between an external and internal system, but (unlike packet filtering and stateful firewalls) there is no direct exchange of packets between the two hosts. Application-level firewalls thus function as proxy servers for connections to applications; they can also log all traffic between the Internet and the network.

Many network security experts prefer application firewalls to other types of firewalls because these firewalls understand the semantics of the applications they protect, making attacking these applications and the hosts on which they reside very difficult. The major disadvantage of application firewalls is that their analysis of input and creation of proxy connections tend to result in lower performance than simpler firewalls such as packet filtering firewalls. Load balancing, in which a redundant fail-over firewall system is deployed, can help counter performance problems, however.

Firewall implementations can take advantage of the functionality available in a variety of ways to provide a robust layered approach in protecting an organization's information assets. Commonly used implementations available today include:

- **External gateway firewall**—An external gateway firewall is deployed at the entrance (external gateway) to a network to create a security perimeter for the entire network. Bastion hosts are often used in this capacity.
- **Screened-subnet firewall**—A screened-subnet firewall is deployed at the entrance to a subnet within a network to selectively limit the types of traffic that can get in or out. Packet screening or stateful firewalls are frequently used in this capacity. Assuming that a bastion host is deployed at the external gateway, a screened-subnet firewall provides a second layer of traffic screening, exemplifying a defense in depth strategy. Access control rules in a screened-subnet firewall are usually substantially different than in a firewall deployed at the external gateway to the entire network in that a screened-subnet firewall's rules will typically allow a great deal of connectivity between internal hosts.
- **Personal firewalls**—Firewalls that reside on individual hosts. Personal firewalls are usually (but not always) packet filtering or stateful firewalls; a few are application firewalls, however. Although each personal firewall protects only one host, the use of personal firewalls often compensates for what amounts to less than adequate security in user workstations. In cases in which workstations are adequately secured, it constitutes an additional layer in a defense in depth security strategy.

Information security managers not only need to be aware of the different types of firewalls and their uses, but they also need to be familiar with their major limitations:

- The false sense of security an organization feels—that no further controls are needed on the internal network—after firewalls are deployed. The unfortunate result is that a network may have a "hard and crunchy exterior, but a soft and chewy interior." Once an attacker bypasses or compromises a firewall, internal hosts may be easy prey.
- Firewalls can be circumvented through the use of modems that connect users directly to corporate or other networks via users' ISPs. Management should assure that the use of modems is adequately controlled, perhaps by providing a separate firewall for all modem connections or by prohibiting such connections altogether.
- Unknown and dangerous services may freely pass through a firewall due to misconfiguration or misunderstanding of the capabilities of a firewall often due to vendor "hype."
- Firewalls generally require a good deal of maintenance. Vulnerabilities in them surface, but if the proper patches or workarounds are not applied, the firewalls cannot only lose their effectiveness, but become conduits for successful externally initiated attacks. Similarly, firewall logs require constant monitoring for the firewall to deliver maximum value.
- Firewalls are so important to network security that a special firewall policy for each firewall, describing the functions the firewall must perform, who owns it, the level of maintenance required, who is authorized to change the firewall's configuration or upgrade it, and so on, should be written. Often such a policy is never written—many firewalls are thus in effect insufficiently controlled and managed.

3.8.6 Intrusion Detection Systems

Although firewall logs are an excellent source of information about attacks that have occurred, combing through them (especially when many firewalls are deployed) is a difficult and time-consuming task. IDSs have thus become an increasingly important part of network security. An IDS is like a smoke detector—it provides information (and in many cases, alarms in the form of messages, pager alerts, and so on) when it detects that there may be a security breach.

IDSs are either network-based or host-based. A network-based IDS captures network traffic and analyzes it to identify attacks. If a network-based IDS is placed at the external gateway, it will detect all externally initiated attack attempts, whether or not the firewall lets the packets associated with each attack through. If the IDS is placed between a firewall and the internal network, it will detect only the traffic that is part of attacks that the firewall allows through. The IDS is not a substitute for a firewall; instead it complements the function of a firewall. In contrast, a host-based IDS is software running on an individual host that uses system log data, resource utilization, modification or deletion of files, abnormal privilege escalation, and other indicators to detect possible attacks.

Some IDSs provide what is frequently called "shunning" capability by sending commands to firewalls to block a certain source IP address that has launched an attack that the IDS has detected. Any subsequent traffic from that address will thus no longer be a problem for hosts within the internal network. Shunning is not, however, always good. Given that a reasonable proportion of packets is spoofed, shunning can result in traffic from a friendly IP address being blocked. Shunning is in fact one type of intrusion prevention measure. IPSs, closely related to IDSs, are designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by them. If a malicious program contains commands that when executed cause a system to delete all the files in a system directory, an IPS needs to prevent this from happening. Although the intrusion prevention approach appears to be promising in limiting damage or disruption to systems that are attacked, it is still in its infancy. Additionally, critics are concerned that IPSs may in themselves constitute a threat; a clever attacker could send commands to a large number of hosts protected by an IPS to cause them to become dysfunctional, a potentially catastrophic outcome in today's typical corporate computing environment in which continuity of service is so critical.

A final caution—intrusion detection and intrusion prevention are both very useful, albeit in somewhat different ways. They are not a panacea, however. Intrusion detection and intrusion prevention should be considered part of a defense in depth, in which multiple layers of controls are deployed in case one or possibly more layer is compromised or bypassed.

The main value of IDSs is that they can lead to early detection of incidents and, thus, also to timely intervention that results in less financial and other types of loss than otherwise might have been. Like firewalls, however, IDSs are no panacea. Many organizations in fact find that intrusion detection returns less than expected value. There are many possible reasons (e.g., intrusion detection staff may not be adequately trained). One deficiency in the use of intrusion detection constantly surfaces, however. As in the case of firewalls, no intrusion detection policy that covers what intrusion detection is supposed to accomplish, how it will be accomplished, the types of safeguards that must be implemented to protect IDSs and their output, who the owner of intrusion detection systems and all the data output is, and so on, ever gets written. Additionally, organizations often fail to create an adequate interface between intrusion detection and incident response.

3.8.7 Encryption

In the most basic sense encryption means converting a plaintext message into a secure-coded form of text, called ciphertext, that cannot be understood without converting back (via decryption) to plaintext. This is done via a mathematical function and a special encryption/decryption object called a "key." Encryption is used to protect data in transit over networks from unauthorized disclosure and manipulation, protect information stored on computers from unauthorized viewing and manipulation, deter and detect accidental or intentional alterations of data, and verify authenticity of a transaction or document.

There are many key elements of an encryption system of which an information security manager should understand:
- **Encryption algorithm**—A mathematically based function or calculation that encrypts/decrypts data
- **Encryption keys**—An object (usually a text string) that is used within an encryption algorithm (calculation) to make the encryption or decryption process unique. A user or program acting on behalf of the user needs to enter the correct key to access or decipher ciphertext that has been encrypted with that key. The wrong key will transform the message into an unreadable form.
- **Key length**—A predetermined length for the key normally measured in bits. For a given encryption algorithm, the longer the key, the more difficult a brute-force attack in which all possible key combinations are tried is.

Encryption is applicable to all layers in the OSI model except the physical layer. It gets in the way of users and applications most at the application layer, but provides users the greatest degree of flexibility at this level because the scope and strength of the protection can be tailored to meet the specific needs of the application. At the network and transport layer, encryption is transparent to users and most applications; it allows systems to converse over existing insecure Internet lines. This level is costly to encrypt and affects all communications among different systems. A general rule is that the lower level of the OSI model at which encryption occurs, the less overhead it causes. The Layer 2 Tunneling Protocol (L2TP) is thus generally more efficient than the IPSec (layer 3) or SSL protocol (layer 4).

Methods designed to break encryption are termed "cryptanalysis." Many cryptanalysis methods are available, one of the most widely known and used of which is the known-text attack, a way of attempting to decrypt a ciphertext message by determining the way a portion of the ciphertext has been transformed from an identified portion of cleartext. Most Internet attackers do not devote the time and effort needed to attempt cryptanalysis attacks, however. Instead they look for weaknesses in the way encryption is used. A careless employee who is required by company policy to encrypt proprietary information to be sent to someone else who works at another location could, for example, make the mistake of sending the encryption key to the other person in cleartext. Anyone who intercepts the network traffic between these two individuals could obtain the key and then use it to decrypt the encrypted message.

3.8.7.1 Secret Key Cryptography

Secret key cryptographic systems are based on a symmetric encryption algorithm, which uses a secret (not publicly distributeed) key to encrypt the plaintext to ciphertext. It is the same key needed to decrypt the ciphertext to the corresponding plaintext—in other words, it is "symmetric."

The most common secret key cryptographic system is the Data Encryption Standard (DES). DES is a standard encryption/decryption technique published in 1977 by the U.S. National Bureau of Standards (NBS), the predecessor of the National Institute of Standards and Technology. DES encrypts blocks of 64 bits. A key of 56 bits is used for the encryption and decryption of plaintext. An additional 8 bits are used for parity checking. Any 56-bit number can be used as a key.

DES is now considered a weak cryptographic solution, since its entire key space can be brute-forced (every possible key tried) by large computer systems within a relatively short period of time. DES is consequently being replaced with the Advanced Encryption Standard (AES), a public algorithm that supports key lengths from 128 to 256 bits. Despite the power of today's computing technology, keys of this size are infeasible to crack, even with an investment of hundreds of millions of US dollars, and will likely be able to protect information assets for many years.

There are two main advantages to secret key cryptosystems. The first is that the user has to use only one key for both encryption and decryption. The second is that secret key cryptosystems generally are less complicated and therefore use less processing power than asymmetric techniques. This makes secret key cryptosystems ideally suited for bulk data encryption. The major disadvantage is in the process of sharing and exchanging keys. In secret key encryption, both the individuals or programs that share a key must keep the key to themselves; if they should disclose the key, the confidentiality of everything they have encrypted with it is at risk. Yet, more than two people may need to decrypt messages that have been encrypted with a secret key. Getting the keys into the hands of multiple people, particularly in e-commerce environments where customers are unknown, untrusted entities, is a cause of many serious concerns.

3.8.7.2 Public Key Cryptography

Public key cryptographic systems developed for key distribution solve the problem of getting symmetric keys into the hands of two people, who do not know each other, but who want to exchange information in a secure manner. Based on an asymmetric encryption process, two keys work together. One key is used to encrypt data, the other to decrypt data. Either key can be used to encrypt or decrypt, but once the key has been used to encrypt data, only its partner can be used to decrypt the data.

The keys are asymmetric in that they are inversely related to each other through a complex relationship based on mathematical integer factorization in which a single product results from multiplying two very large prime numbers. It is impracticable to factor the number and recover the two factors. This integer factorization process forms the basis for public key cryptography, something that involves modular arithmetic, exponentiation and large prime numbers thousands of bits long. Since the keys are large numbers (e.g., up to 3,072 bits), they are best used for encrypting short messages and creating digital signatures. RSA is the best-known public encryption algorithm.

Generally, with public key cryptography, one key—the secret or private key—is known only to one person; the other key—the public key—is known by many people. Asymmetric encryption accomplishes three security goals:

- **Authentication**—A message that has been sent enciphered by the secret key of the sender can be deciphered by anyone with the public key, but could only have come from the sender.

- **Nonrepudiation**—Because the only one with the sender's private key is the sender, this also provides for nonrepudiation (i.e., the sender cannot later claim that he/she did not generate the message).
- **Confidentiality**—A message that has been sent enciphered using the public key of the receiver can be generated by anyone, but can only be read by the receiver. This is the basis of confidentiality.

A message that has been encrypted twice, first by the sender's secret key and secondly by the receiver's public key, achieves both authentication and confidentiality objectives.

3.8.7.3 Hash Functions

Hash functions, sometimes known as one-way or one-time encryption, are not like any other types of encryption, in that once a hashing algorithm is applied to plaintext, it is computationally infeasible to decrypt the ciphertext (more properly called a hash). In hashing algorithms there is also no key *per se* (although the plaintext itself for all practical purposes serves as the key). Although hash functions cannot be used for confidentiality because of their one-way nature, they are extremely useful in checking file and directory integrity (as explained previously) and in protecting passwords from password cracking attempts (because hash representations of passwords are the output of one-way encryption). Hash functions are computationally less intensive than public key algorithms, but computationally more intensive than secret key algorithms.

Message Digest Version 4 (MD4), Messenger Digest Version 5 (MD5) and Secure Hashing Algorithm Version 1 (SHA1) are frequently used hash algorithms. MD4 and MD5 have 128-bit key lengths; SHA1 has a 160-bit key length. Of these algorithms, MD4 is the weakest and SHA1 is the strongest.

3.8.7.4 Digital Signatures

A digital signature is an electronic identification of a person or entity created by using a public key algorithm and intended to verify to a recipient the integrity of the data and the identity of the sender. To verify the integrity of the data, a hashing algorithm is used to hash the entire message, something that generates a small, fixed string message (a message digest) that is usually small (about 128 bytes in length). The message digest, a hash is actually a version of the original message.

The next step verifies the identity of the sender. The message digest is encrypted using the sender's private key, which in affect binds the sender's digital signature to the message to prove its authenticity. To decipher, the receiver uses the sender's public key, proving that the message could have come only from the sender. This process of sender authentication is known as nonrepudiation—the sender cannot later claim that the message was created by anyone else.

Once the message digest is decrypted, the receiver recomputes the hash using the same hashing algorithm and compares the results with what was sent to ensure the integrity of the message. Digital signatures are thus a cryptographic method that ensures:

- **Data integrity**—Any change to the plaintext message would result in the recipient failing to compute the same message hash.
- **Identity**—The recipient can ensure that the message has been sent by the claimed sender; only the claimed sender has the secret key.
- **Nonrepudiation**—The claimed sender cannot later deny generating and sending the message.
- **Replay protection**—If a sequence number and/or time stamp is also built into the message to make it unique, the recipient can check them to ensure that the message was not intercepted and replayed. This could be important if the message were a payment instruction.

However, digital signatures and public key encryption are vulnerable to a variety of attacks, one of the most serious of which is a man-in-the-middle attack in which an attacker captures and then reuses the sender's keys.

3.8.7.5 Public Key Infrastructure

If an individual wants to send messages and digitally sign them using public key cryptography, how does that individual distribute the public key in a secure way? If the public key is distributed electronically, it could be intercepted and changed. To prevent this from occurring, a framework needs to be established to issue, maintain and

revoke public key certificates by a trusted party. This framework is known as a PKI. PKI allows users to interact with other users and applications and obtain and verify identities and keys from trusted sources. Particular implementations of PKI vary according to specific organizations' business requirements.

A digital credential, or certificate, is composed of a public key, together with identifying information about the owner of the public key. The purpose of digital certificates is to associate a public key with the individual's identity. These certificates are electronic documents, digitally signed by some trusted entity using its private key (transparent to users), which contains unique information about the individual.

This process involves proving the sender's authenticity. When a person digitally signs a document, that person attaches a digital certificate issued by a trusted entity. The receiver of the message and accompanying digital certificate relies on the public key of the trusted third-party certificate authority (which is included with the digital certificate or obtained separately) to authenticate the message. The receiver can link the message to a person, not simply to a public key, because of its trust in this third party.

The status and values of a current user's certificate includes (among other things) a distinguishing username, an actual public key, the algorithm used to compute the digital signature inside the certificate and a certificate validity period.

As trusted provider of the public/private key pairs, the certificate/certification authority (CA) attests to the authenticity of the owner (entity or individual) to whom a public/private key pair has been given. The process involves a CA that makes a decision to issue a certificate based on evidence or knowledge obtained in verifying the identity of the requester. Upon verifying the identity of the requestor, the CA signs the certificate with its private key for distribution to the user; upon receipt, the user will decrypt the certificate with the CA's public key). The ideal CA is authoritative (someone that the user trusts) for the name or key space it represents.

The CA is responsible for managing the certificate throughout its life cycle. Key elements or subcomponents of the CA structure include registration authority (RA) and certificate repositories. An optional entity separate from a CA that is often used by a CA customer base is the RA. CAs use RAs to delegate some of the administrative functions associated with recording or verifying some or all of the information needed by a CA to issue certificates or certification revocation lists (CRLs) and to perform other certificate management functions. However, with this arrangement, the CA still retains sole responsibility for signing either digital certificates or CRLs. If an RA is not present in the PKI structure, the CA is assumed to have the same set of capabilities as an RA.

CRL is a capability for checking the continued validity of the certificates for which the CA has responsibility. The CRL flags digital certificates that are no longer valid. The time gap between two updates is very critical and also thus constitutes a risk in the verification of digital certificates.

A certification practice statement (CPS) is a detailed set of rules governing the CA's operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA in terms of the controls that an organization observes, the method it uses to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used. Without a well-written CPS, a PKI is likely to deliver far less than expected.

3.8.7.6 Applications of Encryption

In applications such as e-mail and Internet transactions, the use of encryption generally involves a combination of private/public key pairs, secret keys, hash functions and digital certificates. The purpose of applying these combinations is to achieve confidentiality, message integrity and/or non-repudiation by either sender or recipient. The process generally involves the sender hashing the message into a message digest or a prehash code for message integrity, which is encrypted using the sender's private key for authenticity (i.e., digital signature). The sender then encrypts the message using his/her secret key and the prehash code if authenticity (nonrepudiation) is needed, such as for e-commerce transactions. Afterward, the secret key is encrypted with the recipient's public key, something that provides message confidentiality because only someone with the private key can determine what the secret key is.

The process on the receiving end is the reverse of the process at the sender's end. The recipient uses his/her private key to decrypt the secret key encrypted with the sender's private key, decrypting the message. If the prehash code has been encrypted with the sender's private key, the recipient will verify the authenticity of the public key with a digital

certificate and then decrypt the prehash code, which provides nonrepudiation for the recipient of the sender's message. For integrity purposes, the recipient calculates a posthash code, which should equal the prehash code.

Specific examples of protocols that work in this fashion include:

- **SSL**—A session- or connection-layer protocol widely used on the Internet for communication between browsers and web servers, where any amount of data is transmitted through a secure session. SSL uses a hybrid of hashed, private and public key cryptography to secure transactions over the Internet. This provides the necessary confidentiality, integrity, authenticity and nonrepudiation needed for e-commerce transactions over the Internet. SSL can be characterized as a two-way SSL process such as for business-to-business (B2B) e-commerce activities. It also is commonly used as a one-way consumer process, whereby a retail customer over an Internet retail "virtual store" can verify the authenticity of an e-store's public key through a CA, which can then subsequently be used to negotiate a secure transaction.
- **Secure Hypertext Transfer Protocol (S/HTTP)**—As an application-layer protocol, S/HTTP securely transmits individual messages or pages between a web client and server by establishing an SSL-type connection through the https:// designation in the URL, versus the standard http:// designation. This protocol uses SSL-secure features, but does so as a message-oriented protocol, versus a session-oriented protocol.
- **IPSec**—The network-layer packet protocol used to establish virtual private networks via transport- and tunneling-mode encryption methods. For the transport method, the data portion of each packet [referred to as the encapsulating security payload (ESP)] is encrypted to achieve confidentiality; the specifications or security associations for the receiving end host are specified in an ESP header. In tunneling mode, the ESP payload and its header are encrypted, but also create a revised IP header with a security association field defining parameters used for encryption. To achieve nonrepudiation (i.e., to prevent IP spoofing), an additional authentication header (AH) is also available for use in both modes.
- **Secure Shell (SSH)**—A client-server program used for remote logons that opens a secure, encrypted command line shell session between two hosts. Similar to a VPN, it uses strong cryptography to protect data, including passwords, binary files and administrative command, transmitted between systems on a network. It is typically implemented between two parties by validating each other's credentials via digital certificates. Useful in securing Telnet and FTP services, it is implemented at the application layer.
- **Secure Multipurpose Internet Mail Extensions (S/MIME)**—A standard secure e-mail protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of a message's contents, including attachments.
- **Secure Electronic Transactions (SET)**—A protocol developed jointly by VISA and MasterCard to secure payment card transactions between all parties involved in credit card transactions on behalf of cardholders and merchants. As an open system specification, SET is an application-oriented protocol that uses trusted third-party encryption and digital signatures via a PKI of trusted third-party institutions to address confidentiality of information, integrity of data, cardholder authentication, merchant authentication and interoperability.

3.8.7.7 Encryption Risks

The security of encryption methods relies almost entirely on the secrecy of keys. In general, the more a key is used, the more vulnerable it is to compromise. For example, password-cracking tools for today's computers can brute force every possible key combination for a cryptographic hashing algorithm that uses a 40-bit key in a matter of a few hours.

The randomness of key generation is also a significant factor in the ability to compromise a key. When passwords are tied to key generation, the strength of the encryption algorithm is diminished, particularly when common words are used (as is extremely likely unless proper password control mechanisms are put in place, as explained shortly). This significantly diminishes the key space combinations (e.g., eight character password comparable to a 32-bit key). A 128-bit encryption algorithm's capabilities are less when encryption keys are based on passwords and the passwords lack randomness. For this reason, it is important that effective password rules are applied—easily guessed and short passwords need to be prohibited through software-enforced and/or policy controls.

Encryption is a well-proven security control, but it is limited in that it cannot prevent the loss of data. Additionally, encryption keys can become corrupted or can be lost altogether. Sometimes the consequences are minor, but other times, particularly when valuable corporate data have been encrypted, consequences can be catastrophic. It is

imperative, therefore, to establish an effective key recovery capability, something that usually is not trivial to do. Many organizations escrow encryption keys, i.e., keep a "spare copy" of each secret and private key. Doing so also has its downfalls, however, because the more copies of a key there are, the more likely one copy will fall into unauthorized hands. Furthermore, attackers can subvert cryptographic programs than run on systems. Encryption should thus be regarded as an essential, but not all-encompassing form of control that should be incorporated into an organization's overall computer security program. In many countries, encryption is subject to governmental laws and regulations—thoroughly learning their provisions (especially the provisions of laws and regulations that apply to one's own country) is a must for every ISM.

3.8.8 Malicious Code (Malware)

Malicious code is software or firmware intended to perform an unauthorized function on a computing system. Malicious code can take several basic forms:

- **Logic bombs**—Malicious code designed to execute when certain conditions are fulfilled. For example, a logic bomb might be inserted into a payroll program that, upon processing a record for an employee for which the salary is under N dollars, automatically adds X dollars.
- **Time bombs**—Malicious code designed to execute at a certain time, e.g., when date equals yymmdd and time equals hhmm
- **Worms**—Self-replicating, malicious code that attaches itself to an application program or other executable system component and replicates independently of user actions
- **Viruses**—Self-replicating, malicious code that attaches itself to an application program or other executable system component and replicates when users engage in certain actions such as executing attachments and executables on CDs or memory sticks.

The term "Trojan horse" refers to any malicious program, regardless of the particular type that is hidden. The primary difference between logic and time bombs and worms and viruses, strictly speaking, is that logic and time bombs do not replicate themselves. However, they can be incorporated into a virus that causes the entire code, logic and time bombs included, to be replicated. Today, logic and time bombs do not generally exist by themselves, so this description of malicious code will focus on worms and viruses.

3.8.8.1 Worms

Worms are in effect programmed self-reproducing network attacks. Worms work in a variety of ways, but they have two things in common:

- They exploit vulnerabilities in systems, applications or network components and then attack other systems in an attempt to replicate themselves.
- They do not physically attach themselves to other programs.

3.8.8.2 Viruses

The term virus is a generic term applied to a variety of malicious computer programs that send out requests to the operating system, of the host system under attack, to append the virus to other programs. In this way, viruses are self-propagating to other programs that can be relatively benign, such as web application defacement, or malicious, such as deleting files, corrupting programs or causing a denial of service.

Generally, viruses infect any or all of the following:

- Executable program files
- The file-directory system, which tracks the location of all the computer's files
- Boot and system areas, which are needed to start the computer
- Data files

Because worms work independently of human intervention, when they first surface, they quickly infect a multitude of hosts that are not patched for the vulnerabilities they exploit. Some, such as the Slapper and MSBlaster worms, were so active in attempting to spread that they caused networks to slow down to the point they became unusable. Viruses, on the other hand, are often transmitted as attachments to e-mail, so that when a user opens the attachment, the system becomes infected. Shortly after the system becomes infected, it creates a mail engine that spews messages with

infected attachments to e-mail addresses it has found in files within the infected systems, an action that is actually more worm-like than virus-like. E-mail-borne viruses usually also spoof the identity of the sender based on e-mail addresses found in infected systems, something that substantially increases the likelihood that naive users will open attachments. Other methods of virus infection include downloads from web sites and running shrink-wrapped software—vendors have more than a few times unwittingly included viruses in the products they have distributed.

3.8.8.3 Worm and Virus Controls

To effectively reduce the risk of computer viruses infiltrating an organization, a comprehensive and dynamic antivirus program needs to be established. There are two major ways to prevent and detect worms and viruses. The first is implementing management controls by putting in place sound policies and procedures. The second is implementing technical controls, including antivirus software. Neither is effective without the other.

The management policy and procedural controls that should be in place to help prevent/detect worms and viruses are:

- Keep systems patched. Remotely scanning systems to identify vulnerabilities in them needs to be an integral part of the information security program.
- Build any system from original, clean master copies. Boot only from original diskettes in which write-protection has always been in place.
- Update antivirus software scanning definitions/signatures frequently (in today's environment, they should be updated on a daily basis) by enabling automatic updates; run virus detection scans at least once a week.
- Set up a virus wall that detects and eradicates malicious attachments.
- Have vendors run demonstrations on their machines, not the organization's.
- Enforce a rule of not using shareware without first scanning the shareware thoroughly for malware.
- Scan commercial software before it is installed.
- Insist that field technicians scan their disks and CDs on a test machine before they use them on the system.
- Ensure that network administrators use workstation and server antivirus software.
- Ensure all servers are equipped with an activated current release of antivirus detection software. Because backups are a vital element of an antimalware strategy, implement a sound and effective backup plan. This plan should account for scanning selected backup files for worm and virus infection once an infection has been detected.
- Educate users so they will heed policies and procedures related to proventing virus and worm infections. Every user should at a mimimum know not to open an e-mail attachment that is not expected, even if it appears to be sent from someone the user knows.
- Review antivirus policies and procedures at least once a year.
- Prepare malware eradication procedures and identify a contact person.

Antivirus software is by far the most common antivirus, antiworm tool and is considered the most effective means of protecting PCs and Macintosh systems from infection. Antivirus software will not be an effective tool against viruses and worms on these platforms, however, unless it is frequently updated.

Antivirus software contains a number of components that address the detection of viruses via scanning technologies from different angles. Antivirus software incorporates scanners that look for symptoms of virus and worm infections. Scanners can use:

- **Virus/worm masks or signatures**—Scanners check files, sectors, executables, data files and memory for known and new (unknown to the scanner) malware on the basis of virus or worm masks or signatures, specific code strings within virus/worm code. Some viruses mutate as they propagate. These viruses, known as polymorphic viruses, cannot be detected by a static set of virus signatures. For polymorphic viruses, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.
- **Heuristics**—Analyzing the instructions in the code being scanned and deciding on whether it could contain malicious code on the basis of statistical probability. Heuristic scanning results could indicate that a virus or worm may be present, i.e., possibly infected. Heuristic scanners tend to generate a high level of false-positive errors (i.e., they indicate that a virus or worm may be present, when in fact none is present).

Once a virus has been detected by antivirus software, an eradication program can be used to delete it. Sometimes eradication programs can kill the virus without having to delete the infected program or data file, while other times the infected files must be deleted. Still other programs, sometimes called inoculators, will not allow a program to be run if it contains malware.

Organizations must develop virus implementation strategies to effectively control and prevent the spread of worms and viruses throughout their information systems infrastructure. An important means of controlling the spread of viruses is to detect a worm or virus at its point of entry—before it has the opportunity to cause damage. This includes everything from networks, server platforms and end-user workstations.

The user server or workstation level could include screening of software and data as it enters the machine, where antivirus programs can be set to perform:
- Scheduled virus scans (daily, weekly, etc.)
- Manual/on-demand scans, where the virus scan is requested by the user
- Continuous/on-the-fly scanning, where files are scanned as they are processed

Fighting viruses and worms on a system-by-system basis is a losing cause, except in very small organizations. It is thus best to use a management console to push updates to clients and to remotely initiate detection scans.

At the corporate network level in cases of interconnected networks, virus scanning software is used as an integral part of firewall technologies, referred to as virus walls. Virus walls scan incoming traffic with the intent of detecting and removing viruses before they enter the protected network. Virus walls normally work at the following levels:
- **SMTP protection**—Scanning inbound and outbound SMTP traffic for viruses in mail server mail queues
- **HTTP protection**—To prevent virus infected files from being downloaded and to offer protection against malicious Java and ActiveX programs
- **FTP protection**—To prevent infected files from being downloaded

Virus walls are most often updated automatically with new virus and worm signatures by their vendors on a scheduled basis or on an as-needed basis, when dangerous new virus or worm strains emerge. Vendors also provide facilities to log virus and worm incidents and deal with them in accordance with preset rules. The presence of virus walls does not preclude the necessity for virus and worm detection software on individual computers within a network, because the virus wall only addresses one channel through which viruses and worms enter the network. Virus detection software should be loaded on all PCs and Macintosh computers within the network. Signature files should be updated daily. The facility of automatic, live update has become fairly popular and allows organizations to update the virus scanner signature files soon after updates are available.

3.9 LIFE CYCLES

3.9.1 Integrating Information Security Program Requirements

The most effective program for information security is one in which security is considered within each life cycle activity of the organization. Through awareness and security policies the information security manager should work to have information security considered during each business process life cycle.

Many organizations have developed and implemented consistent project management procedures for significant projects. Other organizations have more of an informal process. The information security manager should be interested in more than just IT application-type projects. For example, the organization's projects can include new product rollouts, merger- and acquisition-related activities, and process improvement.

The protection of the organization's information resources needs to be considered during every organizational life cycle activity. Combined with considering the security of the organization's information resources, the security requirements need to be defined. Understanding the requirements of the information resources will enable the ISM to design and implement an appropriate information security program.

3.9.2 Systems Development Life Cycle Methodologies

The ISM can design and implement the security program more effectively if security is considered during the systems development life cycle (SDLC). Organizations may employ a variety of development methodologies (e.g., traditional SDLC, prototyping, etc.). Where and how security can be considered during that process will vary depending upon that methodology.

Over the years, business application development has occurred largely through the use of the traditional SDLC phases shown in **figue 3.4**. Also referred to as the waterfall technique, this life cycle approach is the oldest and most widely used for developing business applications. The approach is based on a systematic, sequential approach to software development (largely of business applications) that begins with a feasibility study and progresses through requirements definition, design, development and implementation. The series of steps or phases have defined goals and activities to perform with assigned responsibilities, expected outcomes and target completion dates. This approach works best when a project's requirements are likely to be stable and it is possible to determine a system architecture relatively early in the development effort.

Figure 3.4—Traditional Systems Development Life Cycle Approach

SDLC Phase	General Description
Phase 1 Feasibility	Determine the strategic benefits of implementing the system either in productivity gains or in future cost avoidance; identify and quantify the cost savings of a new system; estimate a payback schedule for costs incurred in implementing the system. This business case provides the justification for proceeding to the next phase.
Phase 2 Requirements	Define the problem or need that requires resolution and define the functional and quality requirements of the solution system. This can be either a customized approach or vendor-supplied software package, which would entail following a defined and documented acquisition process. In either case, the user needs to be actively involved.
Phase 3 Design	Based on the requirements defined, establish a baseline of system and subsystem specifications that describe the parts of the system, how they interact and how the system will be implemented using the chosen hardware, software and network facilities. The design also generally includes program and database specifications and a security plan. Additionally, a formal change-control process is established to prevent uncontrolled entry of new requirements into the development process.
Phase 4 Development	Use the design specifications to begin programming and formalizing supporting operational processes of the system. Various levels of testing also occur in this phase to verify and validate what has been developed.
Phase 5 Implementation	The actual operation of the new information system is established, with final user acceptance testing conducted in this environment. The system also may go through a certification and accreditation process to assess the effectiveness of the business application in mitigating risks to an appropriate level and providing management accountability over the effectiveness of the system in meeting its intended objectives and in establishing an appropriate level of internal control.

The primary advantage of this approach is that it provides a template into which methods for the requirements—definition, design, programming, etc.—can be placed. However, there are problems encountered using this approach. Since real projects rarely follow the sequential flow prescribed, iteration always occurs and creates problems in implementing the approach. Obtaining an explicit set of requirements from the customer, as the approach requires, is often difficult. Also, under this approach a working version of the system's programs will often not be available until late in the project's life cycle.

Moreover, the actual phases for each project may vary, depending on whether a developed or acquired solution is chosen. For example, system maintenance efforts may not require the same level of detail or number of phases as application development. The phases and deliverables should be decided during the early planning stages of the project.

The information security manager needs to be involved at each stage in the SDLC to identify the security implications and potential solutions required to sustain the organization's security posture.

Web-based application development is an important emerging software development approach designed to achieve easier and more effective integration of code modules within and between enterprises. Software written in one language on a particular platform has historically used a dedicated application programming interface (API). The use of specialized APIs has caused difficulties in integrating software modules across platforms. Technologies, such as CORBA and COM that use remote procedure calls (RPCs) have been developed to allow real-time integration of code across platforms. However, using these RPC-based approaches for different APIs still remain complex. Web-based application development and associated Extensible Markup Language (XML) technologies are a recent development designed to further facilitate and standardize code module and program integration, although at a cost—XML has many associated security vulnerabilities.

3.9.3 Compliance With the Information Security Governance Framework

A recent development in the information security field involves certifying or accrediting the compliance of an organization's business applications and infrastructure to the enterprise's information security governance framework. Doing so has been a requirement by various regulatory bodies with which entities have had to comply for many years. Organizations have begun taking this approach internally and require that internal business applications, infrastructure and other business processes comply with its security program guidelines.

This approach requires a strong commitment by senior management to implement and enforce. However, it is a very effective process to use; it requires security to be addressed during most business activities. This increases awareness as well as the likelihood that an organization's business interests are completely covered by the security program, reducing the chance that changes in applications or infrastructure do not adequately address security.

A good model for conducting system security certification and accreditation is the National Information Assurance Certification and Accreditation Process (NIACAP), NSTISSI No. 1000, April 2000.[22] The NIST Computer Security Resource Center has a web site for certification and accredition (*http://csrc.nist.gov/sec-cert/*). In addition, NIST has published several documents that provide guidance for various components required for certification and accredition, such as the system security plan, the contingency plan, the incident response plan and others. These components are described in NIST special publications in the 800 series (i.e., NIST-SP-NN) and can be found at *http://csrc.nist.gov/publications/nistpubs/index.html.*

3.10 IMPACT ON END USERS

3.10.1 Meeting Information Security Policy Requirements and Recognizing the Impact on End Users

The impact of security on the end users is a key concern of any security program. The security policy requirements must be designed with consideration of the authorized end user's access to information resources. If business processes are adversely affected by the implementation of security procedures, the ISM must justify the impact. This usually means building a business case showing the cost of the time delay against the security benefits.

[22] See *www.nstissc.gov/Assets/pdf/4009.pdf.*

3.10.2 Planning, Conducting, Reporting and Following Up on Security Testing

A security program should include a process for the planning, conducting, reporting and following up on security testing. Testing of new or modified security technologies is imperative to ensure that an organization's authorized access to its information resources is maintained. Often a test environment is used to test new or modified security technologies. This gives the ISM the opportunity to observe how the change will affect access as well as response time. Any test environment needs to be separated from the operational environment to avoid operational disruption. The results of the tests should be documented and follow-up steps should be reported and archived. This will help provide an audit trail to assist in the problem-solving process should an error or undesirable results occur in the future.

3.10.3 Physical, Administrative and Technical Controls

The ISM in most organizations has a budget that needs to be managed. Since this budget is usually limited, the information security manager must make decisions concerning the number and amount of physical, administrative and technical controls to employ.

The ISM needs to prioritize the controls based on risk management and requirements of the organization. The ISM must look at the costs of the various controls and compare them against the benefit the organization will receive from it. This is similar to the business executive with profit and loss responsibilities.

The ISM needs to have knowledge regarding the development of business cases to illustrate the benefits and costs of the various controls. An understanding of benefit and cost analysis methods is beneficial. Considerations such as return on investment, total cost of management and risk vs. cost analysis need to be carefully considered.

3.11 ACCOUNTABILITY

3.11.1 Promoting Accountability in Managing Information Security Risks

Effective information security management requires that individuals be held accountable for fulfilling their security-related responsibilities. Different positions have different responsibilities and are thus accountable in different ways. The responsibilities associated with each position in the organization are presented in **figure 3.5**.

Figure 3.5—Security Responsibilities Within the Organization

Position	Responsibility
Executive management	Given overall responsibility for protection of information assets
Process owners	Ensure appropriate security measures are consistent with organizational policy and maintained.
Data owners	Determine data classification levels for information assets so that the security organization can provide the appropriate levels of control that will meet their confidentiality, integrity, availability and nonrepudiation requirements.
Security specialists/advisors	Promulgate and assist with the design, implementation, management and review of the organization's security policy, standards and procedures.
IT developers	Implement information security in products they develop and install.

Figure 3.5—Security Responsibilities Within the Organization (*cont.*)	
Position	**Responsibility**
Users	Comply with the organization's security policy and follow the organization's established practices and procedures to enforce the security policy, to include: • Keeping logon IDs and passwords secret • Keeping virus signature files updated • Reporting suspected security violations • Maintaining physical security by keeping doors locked, safeguarding access keys, not disclosing access door lock combinations and questioning unfamiliar people • Conforming to applicable laws (local and others) and regulations • Adhering to privacy regulations with regard to confidential information (e.g., health, legal, etc.)
IS auditors	Provide independent assurance to management on the appropriateness and effectiveness of information security objectives.
IS security committee	Because security guidelines, policies and procedures affect the entire organization, the end users, executive management, security administration, IS personnel and legal counsel should support the security program and offer suggestions concerning how security can be implemented within their respective domains to enforce the policy with minimal negative impact on functionality. Therefore, individuals representing various management levels should meet as a committee to discuss these issues and establish security practices. The committee should be established formally, with appropriate terms of reference, prescribed length of service and regular minutes of meetings recorded with action items that are followed up at each meeting.

The ISM should promote the accountability by business process owners and other stakeholders in managing information security risks. The business owners best understand the organization's needs for its information resources and can best evaluate the impact to the organization, because they are responsible for its business objectives.

The ISM should meet with key business process owners and other stakeholders to discuss their accountability for information security risks. This is an educational process; the information security manager needs to communicate how the security organization can assist the process owner and other stakeholders to manage information security risks. Additionally, if business process owners and other stakeholders are unwilling to make changes in systems and applications for the sake of security, it is imperative that they sign off on the risk—that is, accept the consequences if their failure to take the course of action necessary to properly protect information assets and IT resources results in loss and/or disruption.

3.11.2 Integrate Security Program Into the Enterprise

The ISM needs to understand and use the components of the security governance framework to gain acceptance of the security program. The information security governance framework sets the stage for the mechanisms to be used and the people responsible for promoting and operating the security program. Security principles, practices, management and awareness all need to be employed if a security program is to be effective, and the information security governance framework defines how those security aspects and tasks can be implemented. The stronger the framework is and the stronger the support is from senior management, the more effective the security program will be.

3.11.3 Integrating Information Security Requirements Into the Business Processes

The ISM should understand how to integrate information security requirements into the enterprise's business process. The ISM should have an overall understanding of the organization's business processes. With this knowledge, the ISM should meet with process owners and discuss not only the governance surrounding the business process, but also the required information resources and how they are accessed. The ISM should also understand how to work with process owners to suggest security solutions. The ISM can then plan, design, develop and test those security solutions with them. In addition, the ISM should understand how to impose a program in which security will be considered on a continuous basis, so that changes in the business process will result in appropriate modifications in the security program.

3.12 SECURITY METRICS

3.12.1 Establishing Metrics to Manage the Security Program

The ISM can best manage the security program by gathering and sharing measurable data about its performance. The ISM can then manage the information security governance framework against the security policy. The ISM needs to figure out how to measure the level of risk to systems and networks, to know what security controls to put in place, and to raise the security capability and awareness of employees and the improvement from one measurement to the next.

The biggest problems are determining what needs to be measured and how to measure it. Measurements such as the number of attacks launched against systems or the number of viruses and worms eradicated are only a few of the possibilities. A joint public/private-sector organization has developed the Systems Security Engineering Capability Maturity Model (SSE-CMM), based on the Carnegie Mellon University's Capability Maturity Model (CMM) system, to measure the maturity of an organization's processes. The US Department of Commerce's NIST has also developed an Information Technology Security Assessment Framework (ITSAF) based on the CMM system, the US Office of Management and Budget's Circular A-130 Appendix III and other federal guidelines. Documents for the ITSAF can be found at *http://csrc.nist.gov/publications/nistpubs/index.html*. In addition, a new standard, ISO/IEC 27004 *Information Security Management Metrics and Measurement*, is also expected to be published before long.

3.12.2 Security Metrics Design, Development and Implementation

The ISM needs data to continuously manage the security program; security-related metrics should play a critical role. Therefore, the ISM needs knowledge of the design, development and implementation of security metrics. Security metrics should be designed so that there is a relationship to the performance of the security program. The metrics should be designed so that, if they were evaluated over a period of time, the information security manager could determine whether or not the security program is meeting the organization's objectives. Security metrics can be developed based on a range of including quantifiable, qualitative, tangible and intangible attributes.

Security functions within software often provide information concerning performance. For instance, the software often logs attempted transactions that were not allowed based on the security controls in the system. This type of knowledge allows the ISM to determine whether or not the access controls are functioning as planned. This type of knowledge also lets the ISM identify if there are any trends in the unauthorized access attempts. This could potentially prompt the information security to investigate who the person who initiated the unauthorized attempts was and from where they were coming.

A few other metrics might include:
- Number of user sign-on changes by year or month
- Number of security incidents detected per week/month
- Time between security alerts and remediation
- Percentage of systems with all security patches installed

3.13 MANAGING INTERNAL AND EXTERNAL RESOURCES

3.13.1 Identify, Appropriate and Manage Information Security Resources

The ISM manager should take advantage of all reasonably available resources. These may include internal resources as well as services provided by vendors, consultants, and security research and standards bodies. As with any internal resource, the ISM needs to ensure that the requirements are defined and that the appropriated resources meet the requirements. Commonly offered external resources include security assessments, remote monitoring of firewalls, intrusion detection, background checks, etc. The ISM is also responsible for managing these resources, which include setting performance expectations and measuring the resource's performance against the performance goals. The ISM needs to have clear objectives and make sure that they are communicated to the internal or external resource.

In addition, the ISM must realize that, by utilizing internal or external resources, the responsibility for meeting requirements still resides with the ISM. The ISM must perform due diligence in selecting an external resource to execute part of the organization's security program. Furthermore, although external resources can often cost-effectively contribute expertise and effort that may not be available within the ISM s organization, the ISM needs to also ensure that internal staff, particularly the information security staff, does not lose its expertise or knowledge of the business by relying too much on outsourced resources.

Finally, in either case, the ISM should have a robust incident management process in place. If a security breech or other event is identified by the internal or external resource, the ISM needs to oversee the incident management process to deal with the event and to quickly react to protect the organization's information resources.

3.13.2 Acquisition Management Methods and Techniques

The ISM should have an understanding of acquisition management methods and techniques, since it is very common for the ISM to purchase security-related services and products. The ISM should investigate the acquisition process used by the organization to determine whether it is being done in compliance with those procedures. As an initial step, it is imperative that the ISM understands the organization's requirements for the service or product that is being acquired, so a detailed request can be prepared.

The ISM also may want to employ the assistance of the legal and/or purchasing department before signing any contracts. Part of that contract process should include ensuring that the security vendor's service levels are delineated satisfactorily.

Evaluating security vendors is another important aspect of the acquisition process. The information security manager may develop an evaluation matrix listing the requirements of the organization to rate each firm on how well they achieve each requirement. The ISM may also weigh certain requirements more heavily, based on their impact and importance to the organization.

3.14 CHAPTER 3 GLOSSARY

802.11
A family of IEEE standards for wireless LANs first introduced in 1997. The first standard to be implemented was 802.11b, that specifies communications for transmissions of from 1 to 11 Mbps in the unlicensed 2.4 GHz band using direct sequence spread spectrum (DSSS) technology. The Wireless Ethernet Compatibility Association (WECA) brands this standard as Wireless Fidelity (Wi-Fi).

Abend
Acronym for abnormal end. Abend generally refers to the unexpected and abrupt termination of an application program that can result in corruption of data files that were open when the program execution ended.

Acceptable use policy
A policy that establishes an agreement between users and the organization and defines for all parties ranges of use that are approved before gaining access to a network or the Internet

Access control
The set of rules and procedures implemented within hardware and software to provide for the identification of users, the granting and denying of access, the recording of access attempts, and the administrative tools necessary to manage and monitor access activities

Access path
The logical route an end user takes to access computerized information including networks, systems, authentication and authorized systems, applications and application controls

Access rights
Permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy

Access server
A server that provides centralized access control for management remote access dial-up services

Accountability
The ability to map a given activity or event to the responsible party to make the individual accountable for his/her actions

Accreditation
The management approval process required to certify that a system meets security standards and can be placed in the organization's operating environment

Administrative controls
The actions or controls dealing with operational effectiveness, efficiency and adherence to regulations and management policies

Advanced Encryption Standard (AES)
An encryption algorithm adopted as the US encryption standard by the NIST. With a variable key length of 128, 192 or 256 bits, it uses byte-wise substitution, then byte exchange, then an XOR operation when it encrypts data.

Anonymous File Transfer Protocol (AFTP)
A method of downloading public files using the File Transfer Protocol (FTP). Anonymous FTP is called anonymous because users do not need to identify themselves before accessing files from a particular server. In general, users enter the word "anonymous" when the host prompts for a username. Anything can be entered for the password, such as the user's e-mail address or simply the word guest. In many cases, an anonymous FTP site will not even prompt a user for a name and password.

Antivirus software
Application software deployed at multiple points in an IT architecture designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected

Applets
Programs downloaded from web servers that execute in web browsers on client machines to run web-based applications

Application controls
Manual or programmed activities intended to ensure the completeness and accuracy of records and the validity of entries made. The objective of application controls, either manual or programmed, is to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from manual and programmed processing.

Application-layer firewall
A firewall that works at the application level and allows or blocks traffic depending on rules based on what constitutes acceptable or unacceptable input for applications running on hosts within the security perimeter enforced by the firewall

Application service provider (ASP)
A third-party agent that delivers software licenses to business customers on a shared basis accessible by subscribers over the Internet; also known as managed service provider (MSP)

Asymmetric key (public key)
A cipher technique whereby different cryptographic keys are used to encrypt and decrypt a message

Audit trail
A series of records either in hard copy or in electronic format that provide a chronological record of user activity and other events that show the details of user and system activity. Audit trails can be used to document when users log in, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred.

Authentication
The verification of the authenticity of a person or system requesting access to a resource to establish their legitimacy before access to the requested resource is granted. During the authentication process, the user enters a name or account number (identification) and password (authentication).

Availability
Ensuring that information systems and data are ready for use when they are needed; often expressed as the percentage of time that a system can be used for productive work

Baseband
A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilizing a transceiver. In baseband, the entire bandwidth of the transmission medium (coaxial cable) is utilized for a single channel.

Bastion host
A system that has been hardened to resist attack and which is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls, or may be outside web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., LNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system. It is a very strongly defended host that provides a formidable barrier to a network attacker.

Biometric access control
Any means of authenticating the identity of users by analyzing physical characteristics such as facial recognition, finger printing, voice characteristics or retinal patterns

Bit-stream image
Bit-stream backups, also referred to as mirror image backups, involve the backup of all areas of a computer hard disk drive or another type of storage media. Such backups exactly replicate all sectors on a given storage device. All files and ambient data storage areas are thus copied.

Brute force
Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found

Certificate authority
A trusted third party that registers entities and issues digital certificates

Certification
The process whereby the functional and security requirements of a system or infrastructure component are verified to ensure that those requirements have been met

Channel Service Unit/Digital Service Unit (CSU/DSU)
Interfaces at the physical layer of the OSI reference model, data terminal, equipment (DTE) to data circuit terminating equipment (DCE) for switched carrier networks

Circuit-level firewalls
Work at the application level to create proxy connections from one host to another.

Cleartext
Data that is not encrypted also known as plaintext

COBIT
Control Objectives for Information and related Technology, the international set of IT control objectives published by the IT Governance Institute

Common gateway interface script (CGI)
An executable machine independent software program that performs a specific set of tasks, such as processing input received from a client who typed information into a form on a web page. CGI scripts provide an easy way of passing information between a web site and user application.

Confidentiality
The protection of sensitive or private information from unauthorized disclosure

Cookies
A small identifier file that is placed on a user's computer by a web site so that information about the user and the visit can be recorded and used for identifying users at a later time and possibly preparing customized web pages for them

COSO
A report titled *Internal Controls—An Integrated Framework* sponsored by the Committee of Sponsoring Organizations of the Treadway Commission in 1992. It provides guidance and a comprehensive framework of internal controls for all organizations.

Cryptanalysis
The analysis and compromise of a cryptographic system or encrypted message. Cracking cryptography is usually done by determining how the ciphering was done or the key that was used.

Cybercops
An investigator of computer-crime-related activities

Data classification
The assignment of a level of sensitivity to data that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the organization.

Data diddling
Changing data with malicious intent before or during input into the system

Data Encryption Standard (DES)
A private key cryptosystem developed by IBM in cooperation with the US National Security Agency and published in 1974 by the US National Bureau of Standards (the predecessor of the US National Institute of Standards and Technology). DES has been widely used for data encryption implemented in software or hardware. This encryption standard is no longer recommended by NIST, because it is now too vulnerable to cryptanalysis.

Data normalization
A process applied to all data in a set that produces a specific statistical property. It is also the process of eliminating duplicate keys within a database and is useful as organizations use databases to evaluate various security data.

Data warehouse
A generic term for a system that stores, retrieves and manages large volumes of data. Data warehouse software often includes sophisticated comparison and hashing techniques for fast searches, as well as advanced filtering.

Decryption key
A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption

Defense in-depth
The practice of layering defenses to provide added protection. Defense in-depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an organization's computing and information resources.

Degauss
The application of variable levels of alternating current (AC) for the purpose of demagnetizing magnetic recording media. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, leaving a very low residue of magnetic induction on the media. Degauss loosely means to erase.

Denial-of-service (DoS) attack
An Internet-based attack on an Internet site the result of which is denial of service to legitimate users. The results of the attack can range from poor performance or the total crash of systems. Well-known denial-of-service attacks include buffer overflow attacks, syn attacks and the ping of death attack.

Digital certificate
The electronic equivalent of an ID card that is established under the X.509 standard, which is used to provide sender authenticity, message integrity and nonrepudiation

Digital code signing
The process of digitally signing computer code so its integrity remains intact

Digital signature
The electronic equivalent of an individual's handwritten signature that provides for the authenticity of the message it is attached to and validates the authenticity of the sender. A digital signature promotes nonrepudiation by confirming that the content of a message has not changed since it was signed and provides when the message was sent through a digital time stamp.

Discretionary access control (DAC)
A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Disk mirroring
The practice of duplicating data in separate volumes on two hard disks to make storage more fault tolerant. Mirroring provides data protection in the case of disk failure because data are constantly updated to both disks.

Distributed denial-of-service (DDoS) attacks
DDOS attacks originate from multiple sources.

DMZ
The buffer zone between the Internet and the private network that is engineered using firewalls and other devices to prevent access by external parties to internal systems. The acronym is based on the military term "demilitarized zone" that is used to describe the buffer zone established between North and South Korea.

Domain name service (DNS)
A network service based on a hierarchical database system distributed across the Internet that translates the web address to IP addresses and vice versa

Dual control
A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource

Dynamic Host Control Protocol (DHCP)
A protocol used to dynamically assign IP addresses to devices on the network

Electronic signature
A technique based on public key cryptography designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data. Digital signatures are an example of electronic signatures.

Encryption
Transforming data in a manner so they are made unreadable or unintelligible unless an encryption key is applied to the data

Enterprise root
A certificate authority that grants itself a certificate and creates subordinate CAs. The root CA gives the subordinate CAs their certificates, but the subordinate CAs can grant certificates to users.

Exposure
The extent to which a vulnerability can result in adverse consequences; the potential loss to an area due to the occurrence of an adverse event

Extensible Business Reporting Language (XBRL)
An XML-based, royalty-free open standard being developed by a consortium of more than 170 companies and agencies delivering benefits to investors, accountants, regulators, executives, business and financial analysts, and information providers. It uses financial reporting standards and practices to exchange financial statements across all software and technologies, including the Internet.

Extensible Markup Language (XML)
Promulgated through the World Wide Web Consortium, XML is a web-based application development method that allows designers to cerate their own customized tags, thus enabling the definition, transmission, validation and interpretation of data passed between applications and organizations.

Fall-through logic
Predicting which way a program will branch when an application is presented. It is an optimized code based on a branch prediction.

Firewall
A system or combination of systems that enforces a boundary between two or more networks typically forming a barrier between a secure and an open environment such as the Internet

Frame Relay
A packet switched or virtual circuit implementation. It is a data link layer protocol for switched devices that uses a standard encapsulation technique to handle multiple virtual circuits between connected devices.

Guidelines
A suggested action or recommendation related to an area of information security policy that is intended to supplement a procedure. The implementation of guidelines is encouraged but not enforced.

Hash
The output of a hashing algorithm that takes any input and produces a standard length output that cannot be used to recreate the original message

Honeypot
A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems

Hypertext Transfer Protocol (HTTP)
A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML, XML or other pages to the client browsers.

Information security governance
The leadership, organizational structures and processes that safeguard information

Information security program
The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis

Integrated Services Digital Network (ISDN)
A circuit-switched implementation that provides point-to-point communications at 128 Kbps. This service integrates voice, data and video communications over digital public carrier lines.

Integrity
The accuracy, completeness and validity of information in accordance with business values and expectations

Internet Engineering Task Force (IETF)
The organization that helps plan the evolution and growth of the Internet by writing requests for comments (RFCs), which are *de facto* standards for the Internet's structure and functionality

Internet Inter-ORB Protocol (IIOP)
A protocol developed by the Object Management Group (OMG) to implement Common Object Request Broker Architecture (CORBA) solutions over the World Wide Web. CORBA enables modules of network-based programs to communicate with one another. These modules or program parts, such as table, arrays and more complex program subelements, are referred to as objects. Use of IIOP in this process enables browsers and servers to exchange both simple and complex objects. This significantly differs from HTTP, which only supports the transmission of text.

Internet service provider (ISP)
A third party that provides individuals and organizations access to the Internet and a variety of other Internet-related services

Intrusion detection
The process of monitoring the events occurring in a computer system or network to detect signs of security problems

Intrusion detection system (IDS)
An IDS inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack

IP Security (IPSec)
A protocol that supports two encryption modes: transport and tunnel. Transport mode encrypts the data portion (payload) of each packet but leaves the header untouched. Tunnel mode is more secure, since it encrypts the header and payload. On the receiving side, an IPSec-compliant device decrypts each packet.

ISO/IEC 17799
Originally released as part of the British Standard for Information Security in 1999 as the Code of Practice for Information Security Management, in October 2000 it was elevated by the International Organization for Standardization (ISO) to an international code of practice for information security management. This standard defines information confidentiality, integrity and availability controls in a comprehensive information security management system.

Kerberos
A network authentication protocol that allows one user or computer to prove its identity to another across an insecure network through an exchange of encrypted messages. Once identity is verified, Kerberos provides the two computers with special credentials called tickets for a secure session.

Mail relay server
An e-mail server that relays messages so that neither the sender nor the recipient is a local user

Mandatory access control (MAC)
A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf

Masqueraders
Attackers that penetrate systems by using the identity of legitimate users and their logon credentials

Message Authentication Code
An American National Standards Institute (ANSI) standard checksum that is computed using DES

Mirrored site
An alternate site that contains the same information as the original. Mirror sites are set up for backup and disaster recovery as well as to balance the traffic load for numerous download requests. Such download mirrors are often placed in different locations throughout the Internet.

Modem
Data communications equipment (DCE) devices that provide WAN connections for computers over a telecommunication network (generally the public telephone network). Modems convert computer digital signals into analog data signals that can be transmitted along the telecommunications lines. A modem on the other end of the line or ling then converts the analog back into a digital signal.

Monitoring policy
Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted

Multiplexer
A physical layer device that uses several communication channels at the same time and allows a physical circuit to carry more than one signal at a time when the circuit has more capacity (bandwidth) than required by individual signals

Nonrepudiation
Assurance that a party cannot later deny originating data. It is the provision of proof of the integrity and origin of the data and can be verified by a third party. A digital signature can provide nonrepudiation.

Nonintrusive monitoring
The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities

OSI 7 Layer Model
The Open Systems Interconnection 7 Layer Model is an ISO standard for worldwide communications that defines a framework for implementing protocols in seven layers. Control is passed from one layer to the next starting at the application layer in one station, proceeding to the bottom layer over the channel to the next station and back up the hierarchy.

Packet filtering
Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules

Packet filtering firewall
A firewall that screens incoming traffic using packet filtering

Passive response
A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action

Password cracker
A tool that tests the strength of user passwords searching for passwords that are easy to guess by repeatedly trying words from specially crafted dictionaries and often also by generating thousands (and in some cases even millions) of permutations of characters, numbers and symbols

Penetration testing
A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers

Point-to-Point Protocol (PPP)
The Internet standard for transmission of IP packets over serial lines. It supports asynchronous and synchronous lines.

Ports
An interface point between a CPU and a peripheral device. A port can also be a convention that allows remote services to connect to a host in an orderly manner.

Privacy
Freedom from unauthorized intrusion or disclosure of information about individuals

Private key
In asymmetric cryptography, the key that is held and used by one person or entity

Procedures
A detailed description of the steps necessary to perform specific operations in conformance with applicable standards; a portion of a security policy that states the general process that will be performed to accomplish a security goal

Proxy server
A server that acts on behalf of a user. Typically, proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps perform additional authentication, and then complete a connection to a remote destination on behalf of the user.

Public key
In an asymmetric cryptographic scheme, the key that may be widely published to enable the operation of the scheme

Public key encryption
Public key encryption sends secure data over unsecured networks such as the Internet. It makes data unreadable to prying eyes that might intercept the transmission. This encryption method utilizes two keys, the public key and the private key. One is used to encrypt plaintext; the other is used to decrypt the ciphertext.

Residual risk
The amount of risk that remains after countermeasures and controls are in place

Router
A device that operates at the network layer of the OSI reference model and interfaces outside of an organizations internal network environment via carrier networks

RSA
A public key cryptographic developed by R. Rivers, A. Shamir and L. Adleman. The RSA has two different keys, the public and private key. The strength of the RSA depends on the difficulty of the prime number factorization; RSA is used for both encryption and digital signatures.

Secure Sockets Layer (SSL)
A protocol developed by Netscape for transmitting private data via the Internet. SSL works by using a public key to encrypt data that are transmitted over the SSL connection. SSL can also help to ensure that the data comes from the web site from which they are supposed to have originated and that no one tampered with the data while they were being sent using digital certificates. Any web site URL that starts with https:// has been SSL-enabled.

Secret key
A key that is used to encrypt and decrypt data where one key is used for both operations and is shared between all parties to the communication

Secret key encryption
Symmetric encryption; a single key is used to encrypt and decrypt data the key is shared between two individuals or entities.

Security metrics
A standard of measure used to monitor information-security-related activity and evaluate the performance of security-related programs

Servlets
An applet that runs on a server without a direct user interface extending the functionality of the web server and providing access to existing business systems

Sniffing
An attack in which data traversing a network are captured and monitored without authorization. This is similar to the more traditional wire tap but is done without legal authority. Sniffing is commonly used to capture passwords and other interesting and sensitive information that traverses the network.

Social engineering
An attack based on deceiving users or administrators at the target site. Social-engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user in an attempt to gain illicit access to systems. A person who illegally enters computer systems by persuading an authorized person to reveal IDs, passwords and other confidential information.

Split knowledge
A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items; a condition under which two or more entities separately have key components which individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module

Spoofing
Faking the sending address of a network transmission

Stand-alone root
A certificate authority that signs its own certificates and does not rely on a directory service to authenticate users

Standards
Definition of the metrics used to determine the correctness of a thing or process; a set of rules or specifications that, when taken together, define a software or hardware device. A standard is also an acknowledged basis for comparing or measuring something

Stateful inspection firewall
A firewall that keeps track of the state of connections and blocks incoming traffic that is not part of an ongoing connection

Steering committee
A management committee assembled to sponsor and manage various projects such as an information security program

Steganography
A technology used to embed information in audio and graphical material to keep it from being found

Subordinate root
A certificate authority whose public key certificate is issued by another

Symmetric key encryption
See secret key encryption.

Terminal Access Controller Access Control System Plus (TACACS+)
An authentication protocol often used by remote access servers

Threat analysis
An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against information assets and information technology. The threat analysis usually also defines the level of threat and the likelihood of that threat to materialize.

Transmission Control Protocol/Internet Protocol (TCP/IP)
The TCP/IP suite is a set of communications protocols that encompass media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access and network management.

Two-factor authentication
The use of two independent mechanisms for authentication for example requiring a smart card and a password

Virus signature files
The file of virus patterns that are compared with existing files to determine if they are infected with a virus or worm

Virtual private network (VPN)
A secure private network that uses the public telecommunications infrastructure to transmit data. In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.

Web hosting
The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites. Most hosting is "shared" which means that web sites of multiple companies are on the same server in order to share costs.

Web Server
Using the client-server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.

Worm
A self-replicating program that does not attach itself to programs, but rather spreads independently of users' actions. Worms are in effect programmed network attacks.

3.15 CHAPTER 3 SAMPLE QUESTIONS

CISM exam questions are developed with the intent of measuring and testing practical knowledge in information security management. All questions are multiple choice and are designed for one best answer. Every CISM question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement.

In some instances, a scenario or a description problem may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided.

Many times a CISM examination question will require the candidate to choose the **MOST** likely or **BEST** answer. In every case the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked and how to study to gain knowledge of what will be tested will go a long way toward answering them correctly.

The sample questions contained below are designed to depict the type of question format on the CISM examination.

1. The **MOST** appropriate metric to measure how well information security is managing the administration of user access is:

   A. percent of accounts with configurations in compliance.
   B. ratio of actual accounts to actual end users.
   C. elapsed time to suspend accounts of terminated users.
   D. elapsed time to suspend accounts of users transferring.

2. Which of the following would present the **GREATEST** exposure if placed on a DMZ?

   A. Web server
   B. Mail relay
   C. Proxy server
   D. Access control list

3. Security baselines are usually established by:

   A. end users.
   B. developers.
   C. trade associations.
   D. software vendors.

4. Establishing accountability among business process owners and stakeholders requires displaying which of the following?

   A. Technical knowledge
   B. Interpersonal skills
   C. Business knowledge
   D. Authoritative behavior

5. Who is in the **BEST** position to develop the priorities and identify what risks and impacts would occur if there were a loss or corruption of the organization's information resources?

A. Internal auditors
B. Security management
C. Business process owners
D. External regulatory agencies

6. The most important single concept for an information security manager to keep in mind is:

A. ensure that baseline security requirements are met.
B. understand and work in concert with business goals.
C. implement state-of-the-art security technology.
D. ensure that all security-related risk is eliminated.

7. If the information security manager wants to establish an information security governance framework, he/she should first:

A. find out if the organization has a project support function.
B. prepare a budget estimate.
C. work with senior management to increase the size of the information security staff.
D. benchmark the existing information security practice to identify its strengths and weaknesses.

8. According to the OSI model, routing is done at which layer of networking?

A. Physical
B. Data link
C. Network
D. Transport

9. Wireless network has many security-related vulnerabilities. Which of the following is the best method of limiting the impact of these vulnerabilities?

A. Enable the Wired Equivalent Privacy (WEP) protocol in each wireless network.
B. Increase the amount of auditing on every host that connects to a wireless network.
C. Require that every host that connects to this network have a well-configured personal firewall.
D. Make a subnet out of the wireless network.

10 Which of the following is a type of active network attack?

A. Network analysis
B. Eavesdropping
C. Traffic analysis
D. Packet replay

11. Which of the following types of firewalls would be best for an organization if performance were the chief requirement?

A. Packet filtering
B. Stateful inspection
C. Application-level
D. Circuit

12. Suppose that the organization has a network-based IDS. It identifies packets that contain a command that, if executed on the target host, would give an attacker superuser privileges on that host. This IDS has used which of the following to identify this attack?

A. Signatures
B. Protocol anomalies
C. Statistical patterns
D. Neural networks

13. Which of the following types of cryptography is the slowest from a computational standpoint?

A. Secret key
B. Public key
C. Hashing
D. Elliptical curve

14. Suppose that one needs to prove that he/she, not someone else, have sent a message to a colleague. Assuming he/she is using public key encryption to prove one's identity, one must:

A. encrypt the message with one's private key, then send the private key to your colleague so that this person can decrypt it.
B. encrypt the message with one's public key, but there is no need to send this key to the colleague, since public keys are widely distributed.
C. encrypt the message with one's private key; the colleague will decrypt it with the public key, which is publicly available.
D. encrypt the message with one's public key, then send one's private key to the colleague so that this person can decrypt the message.

15. Which of the following **BEST** illustrates the principle of accountability?

A. Creating and distributing an acceptable usage policy to all employees of an organization
B. Having business owners who do not implement control measures such as patches for vulnerabilities formally acknowledge that they have done so and that they understand the potential consequences
C. Conducting frequent audits of systems and applications to ensure that they comply with baseline security measures
D. Creating and enforcing specific policies that cover a wide range of information security issues.

16. The impact of security on the end users is a key concern of any security program. If users are going to be adversely affected by security measures, the information security manager should (choose **BEST** answer):

A. initiate a security training and awareness effort that enables users to better understand the reasons these measures have been implemented.
B. roll back all of these measures until the reasons that users have been adversely affected can be better understood.
C. roll back the least essential of these measures until the reasons that users have been adversely affected can be better understood.
D. prepare and present the business case to justify the measures.

17. In which stage of the systems development life cycle (SDLC) should the information security manager create a baseline of system and subsystem specifications that describe the system components, their interaction and how the system will be built?

A. Feasibility
B. Requirements
C. Design
D. Development

18. To make client-server environments secure, which of the following needs to be done?

A. Identify all access points.
B. Use host-based intrusion detection on the server and all clients.
C. Assign private addresses to the server and all clients.
D. Place a firewall between the server and all clients.

19. Which of the following types of firewalls would be the **BEST** bastion host?

A. Personal
B. Packet filtering
C. Stateful inspection
D. Application-level

20. There are never enough resources to implement all the control measures that information security managers want. The fact that some information assets and IT resources will not receive sufficient protection refers most directly to which of the following?

A. Implied exposures
B. Residual risk
C. Uncontrollable exposures
D. Business risk

21. One notices that in a PC a critical executable was modified at the time the system became infected by some kind of malware. Knowing this, one can **RULE OUT** the possibility that this system was infected by what?

A. A virus
B. A worm
C. A Trojan horse
D. All of the above

22. Which of the following cryptographic algorithms is the best for checking whether files and directories have been modified?

A. Secret key
B. Public key
C. Hash functions
D. Quantum

23. A security-related incident occurs. The information security manager's primary goal should be which of the following?

A. To keep systems and network devices up and running
B. To keep the cost of the incident to a minimum
C. To gain valuable lessons learned that will improve the quality of your information security practice
D. To interfere with others who are responding to the incident as little as possible until the incident is over

24. An intrusion prevention system does which of the following?

A. Stops all network traffic that is part of an attack before that traffic can get to the intended victim(s)
B. Constantly modifies operating systems to make them a moving target
C. Prevents any attacks that occur from affecting the target system(s)
D. Launches attacks against attacking systems to bring them down or disable them

25. A certificate should contain which of the following types of information?

A. A distinguishing username
B. The name of the algorithm used in creating the digital signature inside the certificate
C. The certificate validity period
D. All of the above

26. Risk management requires that the information security manager pay close attention to three factors. Which of the following is **NOT** one of these three factors?

A. The value of each asset
B. The probability that an event affects an asset
C. The impact of loss
D. The relationship between different assets

27. If the organization decides to deal with security risk by taking out an insurance policy that pays whenever security-related breaches costing the organization US $1 million or more occur, the company's strategy can be be defined as which of the following?

A. Risk avoidance
B. Risk transfer
C. Risk management
D. Risk elimination

28. The due-care approach to risk management is based on which of the following assumptions?

A. By implementing the same controls as its peer organizations, an organization can counter the security risks that it probably also faces.
B. The annual loss expectancy provides the simplest and most direct estimate of the amount of security risk that an organization faces.
C. Achieving the appropriate level of security requires at a minimum that an organization thoroughly understand and follow the legal and regulatory requirements that apply to it.
D. Qualitative risk analysis provides a better indication of the real level of security risk that an organization faces than quantitative risk analysis.

3.16 CHAPTER 3 ANSWERS TO SAMPLE QUESTIONS

1. **A** The percent of accounts with configurations in compliance is the best measure of how well administration is being managed because this shows the overall impact. Elapsed time to suspend accounts is only part of the picture and does not address the volume of requests. The ratio of actual accounts to actual end users does not indicate that much in terms of how well security is administered.

2. **D** Storing access control lists (ACLs) on a DMZ is not advisable as the DMZ is subject to compromise and compromise of the ACLs would be very detrimental to system security. Web servers, mail relays, and proxy servers are all typically placed on a DMZ.

3. **D** Security baselines are often established by software vendors for the software they write. End user, developer and trade associations do not generally get involved in developing security baselines.

4. **B** Establishing accountability among business process owners and stakeholders requires significant exercise of communication and interpersonal skills to sell these groups on the merits of accountability. They will generally not be as influenced by a display of technical knowledge. Although knowledge of the business is good, this would be a secondary issue. Displaying authorative behavior would tend to evoke a negative reaction.

5. **C** Business process owners are in the best position to judge the risks and impacts, as they are most knowledgeable concerning their systems. Auditors, security management and regulators would not understand the impact on the business to the same degree as the owners of the business processes.

6. **B** Information security is successful only to the degree that it is in alignment with business drivers. Alternative D is the worst choice of all—it is impossible to eliminate all security-related risk.

7. **A** As stated in this chapter, the information security manager needs to determine if there is already a project support function. To move ahead blindly would not only put the information security function at risk, but would likely be career-limiting for the information security manager.

8. **C** Routers and switches work at the network layer. Routing and switching are in fact possible because of the layer three Internet protocol (IP), which contains the information needed to shunt packets off to the next "hop" of their destination.

9. **D** Making a wireless network into a subnet helps isolate other hosts and parts of the network from the many dangers of wireless networking. Answer A is not appropriate, because WEP encryption is so weak. Increasing auditing and using personal firewalls would help somewhat, but these solutions would be more cumbersome and less effective than simply isolating the wireless network in its own subnet.

10. **D** The other three alternatives—network analysis, eavesdropping and traffic analysis—are all types of passive attacks.

11. **A** Packet filtering firewalls are the fastest because they perform the least amount of analysis on traffic they receive. Stateful firewalls have to keep track of the state of connections, and application firewalls need to form and manage proxy connections, something that requires considerably more processing capacity.

12. **A** Commands that comprise attempts to attack systems (such as trying to gain unauthorized superuser privileges) are the most common type of signatures, although there are others. Protocol analysis would primarily examine OSI layer three and four activity. No statistical analysis of any type has been done here, and neural networks work in a completely different manner.

13. **B** Public key cryptography is the slowest because public key algorithms are based on complex mathematical relationships that require a multitude of steps to compute. Secret key cryptography is the fastest. Hash functions are somewhere in between secret key and public key encryption when it comes to performance. Elliptical curve cryptography is more computationally efficient than public key cryptography, but not as fast as secret key encryption.

14. **C** To prove one's identity means that one's signing the message with one's digital signature. To do this, one must encrypt the message with one's private key. The recipient must decrypt it with the public key, which the colleague can probably obtain from a publically accessible web server. Only the sender could have encrypted this message because the public key worked in decrypting it. The actions described in answers A and D are catastrophic. One should never share one's private key with anyone. If one does, all kinds of misuse can occur—someone could, for example, electronically impersonate the sender.

15. **B** Getting business owners and other stakeholders to sign off on their failure to implement controls that the information security manager has recommended is the best way to "get the point across" when it comes to accountability. Many business owners and other stakeholders will rethink their reluctance to comply with information-security-related recommendations, when they are directly confronted with the consequences that could occur.

16. **D** Assuming that the impact upon users has already been studied, presenting the business case for implementing the security measures that have adversely affected users is the appropriate thing to do. Alternative A is not realistic because security training and awareness is not likely to reverse user attitudes, and the cost needed to conduct this effort is likely to be high. Alternative B is not realistic—one can not just reverse everything one has done because users do not like it. Alternative C is pretty logical, but chances are a lot of time and resources will be required to determine exactly which measures need to be rolled back.

17. **C** This answer is a paraphrase of this manual's description of the design phase.

18. **A** The client-server environment is a distributed computing environment. It is thus critical to know all access points; any unknown access point could be a vector of attack. The other measures in alternatives B, C and D are nice to have, but none is as essential and knowing all access points.

19. **D** Application-level firewalls are much harder to defeat and/or bypass than the other types of firewalls listed in this item. This makes them ideal candidates to become bastion hosts.

20. **B** Residual risk means the risk the information security manager knows he/she cannot control. Alternative D is incorrect because business risk is a much more global concept. The terms in alternatives A and C may sound logical, but they are not used to refer to the risk that cannot be controlled.

21. **B** Worms do not change executables in systems that they infect.

22. **C** Hash functions produce hash output that uniquely identify a set of data. If just one character or number in the data is changed, the hash will change.

23. **B** The main goal is to cut the losses as much as possible, because business objectives must be given first priority in an information security practice. Alternatives A and C are plausible, but they are not primary goals. Alternative D, to interfere with others as little as possible, is wrong because to avoid interfering is to be out of the loop. The information security manager needs to know what is going on when incidents occur, because this person can provide advice and sometimes direction concerning procedures that should be followed and issues that should be considered.

24. **C** Intrusion prevention systems cannot prevent attacks from occurring over networks, but they can curb the effects of attacks by sending policies to machines that instruct them to ignore certain commands and avoid doing certain things that may cause damage or destruction. Alternative C sounds attractive, but constantly modifying operating systems so that they are harder to attack would be suicidal in computing environments—it would make hosts terribly unstable. Alternative D would be an extremely bad idea—something that would cause all kinds of disruption (especially considering that the source IP address may have been spoofed) and might even trigger lawsuits.

25. **D** All of the alternatives, A through C, plus more information not listed in the alternatives are needed in certificates.

26. **D** As stated in this chapter, risk management involves considering three factors:
- Asset value
- Impact of loss
- Likelihood of an event impacting that asset

27. **B** Alternative B illustrates classic risk tranference—transferring any large security-related losses to an insurance company if a major security breach occurs. Alternative A, risk avoidance, is incorrect because risk can never be avoided (at least not altogether). Alternative C, risk management, means determining what to do with information assets and IT resources based on factors such as asset value and likelihood of loss or compromise, something that is in many ways the opposite of risk transfer in that an organization that adopts the latter strategy is in effect refusing to manage risk. Alternative D, risk elimination, cannot be correct, because it is impossible to eliminate risk—there is just too much of it from too many sources in today's IT environments.

28. **A** Due care in its simplest form means matching what one's peers (e.g., a person in the transportation industry's, peers are others in the industry) do in securing their information assets and IT resources. Alternative B is something that someone who advocates quantitative risk analysis would advocate. Alternative C is not related to the practice of due care, although legal and regulatory requirements are something that the information security manager should always consider. Alternative D is also not related to the due care approach, which in effect says that formal risk analysis—whether quantitative or qualitative—is a waste of time.

3.17 CHAPTER 3 REFERENCES

Alga, Nadia; "Increasing Security Levels," *Information Systems Control Journal*, vol. 2, 2002, p. 35-41

Allen, Julie; *The CERT Guide to System and Network Security Practices*, Addison-Wesley, USA, 2001

Alles, Michael; Alexander Kogan; Miklos Vasarhelyi; "Black Box Logging and Tertiary Monitoring of Continuous Assurance Systems," *Information Systems Control Journal*, vol. 1, 2003, p. 37-40

Archer, Clark; Michael Stinson; *Object-oriented Software Measures*, Software Engineering Institute, CMU/SEI-95-TR-002, USA, April 1995

Ashbourn, Julian; *Biometrics: Advanced Identity Verification—The Complete Guide*, Springer-Verlag, UK, 2000

Ashbourn, Julian; Biometric Security and Controls, "Biometric White Paper," *homepage.ntlworld.com/avanti/whitepaper.htm*, 1999

Bace; R.; *Intrusion Detection,* MacMillan Technical Publishing, USA, 2000

Bachmann, Felix; Len Bass; Jeromy Carriere; Paul Clements; David Garlan; James Ivers; Robert Nord; Reed Little; *Software Architecture Documentation In Practice: Documenting Architectural Layers,* Software Engineering Institute, CMU/SEI-2000-SR-004, March 2000

Bernstein, Terry; Anish Bhimani; Eugene Schultz; Carol Siegel; *Internet Security for Business*, Wiley, USA, 1996

Blake, Ian; Gadiel Seroussi; Nigel Smart; *Elliptic Curves in Cryptography*, Cambridge University Press, USA, 1999

Brancik, Kenneth C.; "The Computer Forensics and Cybersecurity Governance Model," *Information Systems Control Journal*, vol. 2, 2003, p. 41-47

Bromba, Manfred; Bioidentification, "Biometrics," *http://home.t-online.de/home/manfred.bromba/biofaqe.htm*

Caldwell, Matthew; "The Importance of Event Correlation for Effective Security Management," *Information Systems Control Journal*, vol. 6, 2002, p. 37-38

Carasik, Anne; "Choosing the Best Solution for Your Network Security: Secure Shell, TLS or IPSec," *Information Systems Control Journal*, vol. 3, 2001, p. 33-39

Chappel, David; *The Next Wave: Component Software Enters the Mainstream*, Chappell & Associates, April 1997

Chappel, David; *Taking Stock of Component Technology*, Chappell & Associates, June 1999

Chief Security Officer Online, *www.csoonline.com* (Includes several white papers on evaluating the cost/benefit of security procedures.)

Coderre, David G.; *Fraud Detection: Using Data Analysis Techniques to Detect Fraud*, Global Audit, Canada, 1999

Deloitte & Touche, *e-Commerce Security—A Global Status Report*, Information Systems Audit and Control Foundation, USA, 2000

Dietel; *Introduction to Operating Systems, 2nd Edition*, Addison-Wesley, 1990

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

Dimitriadis, Christos K.; Despina Polemi; "Biometrics—Risks and Controls," ***Information Systems Control Journal*****, vol. 4, 2004, p. 41-43**

Doughty, Ken; "Implementing Enterprise Security: A Case Study (Part1)," ***Information Systems Control Journal*****, vol. 2, 2003, p. 34-39**

Doughty, Ken; "Implementing Enterprise Security: A Case Study (Part2)," ***Information Systems Control Journal*****, vol. 3, 2003, p. 60-63**

Down, Michael P.; Richard J. Sands; "Biometrics: An Overview of the Technology, Challenges and Control Considerations," ***Information Systems Control Journal*****, vol. 4, 2004, p. 53-56**

Ellis, Juanita; Timothy Speed; *The Internet Security Guidebook: From Planning to Deployment*, Academic Press, USA, 2001

Endorf, Carl; Eugene Schultz; Jim Mellander; ***Intrusion Detection and Prevention*****, McGraw-Hill, USA, 2004**

Farris, Greg; "Effective Encryption Requires an Integrated System," ***Information Systems Control Journal*****, vol. 4, 2004, p. 46-47**

Franzen, Michael; Florian Kirchbaum; Sonia Fahmy; Eugene Schultz; "A Framework for Understanding Vulnerabilities in Firewalls Using a Dataflow Model of Firewall Internals," *Computers and Security*, 20 (3), 2001, p. 263-270

Ford, Merilee; H. Kim Lew; Steve Spanier; Tim Stevenson, *Internetworking Technologies Handbook, 3rd Edition*, Cisco Press, 2000

Frownfelter-Lohrke, Cynthia; James E. Hunton; "New Opportunities for Information System Auditors: Linking SysTrust to COBIT," ***Information Systems Control Journal*****, vol. 3, 2002, p. 45-48**

Gallegos, Frederick; Daniel P. Manson; Sandra Allen-Senft; ***Information Technology Control and Audit, 2nd Edition*****, Auerbach, USA, 2004**

Garfinkel, Simson; Gene Spafford; Alan Schwartz; ***Practical Unix and Internet Security, 3rd Edition*****, O'Reilly, USA, 2003**

Garfinkle, Simson; Gene Spafford; ***Web Security, Privacy and Commerce, 2nd Edition*****, O'Reilly & Associates, 2002**

Gerdes, Michael; "An Exploration of Global Perceptions of Security and Privacy," ***Information Systems Control Journal*****, vol. 6, 2002, p. 27-30**

Ghosh, Anup K.; ***E-commerce Security: Weak Links, Best Defenses*****, John Wiley & Sons, USA, 1998**

Goldreich, Oded; *The Foundations of Cryptography*, Cambridge University Press, UK, 2001

Gorgoglione, Janice; Gilbert W. Joseph; "Laser Check Printing—How It Effects the Internal Control System," ***Information Systems Control Journal*****, vol. 4, 2002, p. 39-47**

Griss, Martin L.; Ivar Jacobson; "Component-Based Development: Approaching the Promised Land of Component Reuse," *ADTmag.com*, June 2001

Hale, Ron; "Helping Businesses Safeguard Information and Networks," ***Information Systems Control Journal*****, vol. 1, 2001, p. 23**

Note: Publications in bold are available in the ISACA Bookstore, ***www.isaca.org/pubs1.htm*****.**

Harrison, Robert M.; "Application Risk in a TCP/IP Environment," ***Information Systems Control Journal*****, vol. 6, 2002, p. 39-40**

Highsmith, Jim; Nancy R. Mead; Daniel J. Mosley; Balasubramaniam Ramesh; Lou Russell; Karl E. Wiegers; *Requirements Engineering and Management*, Cutter Information Corp., July 2000

Information Processing Limited, *Software Testing and Software Development Lifecycles*, 1996

International Engineering Consortium, *www.iec.org/online/tutorials* (Includes numerous research papers and descriptions of security technologies)

The Internet Society, RFC 2828, Internet Security Glossary, May 2000

IT Governance Institute, *www.itgi.org/resources* (Outlines critical components of information security governance.)

Jamieson, Rodger; Greg Stephens; Santhosh Kumar; "Fingerprint Identification: An Aid to the Authentication Process," ***Information Systems Control Journal*****, vol. 1, 2005,** ***www.isaca.org/jonline***

Johner, Heinz; Seiei Fujiwara; Alelia Yeung; Anthony Stephanou; Jim Whitmore. *Deploying a Public Key Infrastructure*, IBM, March 2000, p. 29-34, 49-52

Kaeo, Merike; *Designing Network Security*, Cisco Press, USA, 1999

Keating, Stephen; Richard M. Smith; "Top US Privacy Stories of 2000," ***Information Systems Control Journal*****, vol. 3, 2001, p. 29-31**

Kennedy, Susan; "Best Practices for Wireless Network Security," ***Information Systems Control Journal*****, vol. 3, 2004, p. 36-38**

King, Christopher M.; Curtis E. Dalton; Ertem Osmanoglu; *Security Architecture*, McGraw Hill, USA, 2001, chapter 2

Koblitz, Neil I.; *A Course in Number Theory and Cryptography*, Springer Verlag, USA, 1994

Koorn, Ronald; Peter van Walsem; Mark Lundin; "Auditing and Certification of a Public Key Infrastructure," ***Information Systems Control Journal*****, vol. 5, 2002, p. 28-31**

Lee, Elsa; "Combating Cyberthreats—Partnership Between Public and Private Entities," ***Information Systems Control Journal*****, vol. 3, 2002, p. 38-43**

Mahadevan, Chidambaram; "Intrusion, Attack, Penetration—Some Issues," ***Information Systems Control Journal*****, vol. 6, 2001, p. 52-57**

McConnell, Steve; *Software Project Survival Guide*, Microsoft Press, USA, 1998

McQuaide, Bill; "Identity and Access Management," ***Information Systems Control Journal*****, vol. 4, 2003 p. 35-37**

Mel, H.; Doris Baker; *Cryptography Decrypted*, Pearson, Canada, 2001

Menezes, Alfred; *Elliptic Curve Public Key Cryptosystems* (The Kluwer International Series in Engineering and Computer Science, Sec 234, Communications and Information), Kluwer Academic, USA, 1993

Merkow, Mark S; James Breithaupt; *Internet, the Complete Guide to Security*, American Management Association, USA, 2000

Note: Publications in bold are available in the ISACA Bookstore, ***www.isaca.org/pubs1.htm*****.**

Microsoft, Security & Privacy web site, *www.microsoft.com/security* (Includes security alerts and information on hardware and software security baselines.)

Mollin, Richard; *An Introduction to Cryptography*, Chapman&Hall/CRC Press, USA, 2000

Moody, Robert; "Ports and Port Scanning: An Introduction," *Information Systems Control Journal*, vol. 5, 2001, p. 34-39

Murhammer, Martin W.; Orcun Atakan; Stefan Bretz; Larry R. Pugh; Kazunari Suzuki; David H. Wood; *TCP/IP Tutorial and Technical Overview*, IBM, USA, 1998, p. 297 and 339

Nash, Duane; Joseph Brink; *PKI: Implementing and Managing E-security*, RSA Press, 2001

National Institute of Standards and Technology, "Guideline on Network Security Testing," SP 800-42, USA, October 2003, *http://csrc.nist.gov/publications/nistpubs/index.html*

National Institute of Standards and Technology, Computer Security Resource Center Special Publications (particularly the 800 series), *http://csrc.nist.gov/publications/index.html*

National Institute of Standards and Technology, "Security Considerations in the Information System Development Life Cycle," SP 800-64, USA, October 2003, *http://csrc.nist.gov/publications/nistpubs/index.html*

National Institute of Standards and Technology, "Recommended Security Controls for Federal Information Systems," 800-53, USA, 2005, *http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf*

National Institute of Standardards and Technology, "Security Self-Assessment Guide for Information Technology Systems," SP 800-42, USA, November 2001, *http://csrc.nist.gov/publications/nistpubs/index.html*

National Institute of Justice; *Electronic Crime Scene Investigation: A Guide for First Responders*, USA, 2001

New Architect, Internet Strategies for Technology Leaders, *http://research.newarchitectmag.com/data/rlist?t=1012401058_93372205* (A list of information security architecture white papers)

Nichols, Randall K.; Daniel J. Ryan; *Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves*, McGraw Hill, USA, 2000

Norifusa, Masaya; "Securing Emerging Internet Applications," *Information Systems Control Journal*, vol. 2, 2001, p. 36-39

Norris, Robert C.; "Virtual Private Networking: Confidentiality on Public Networks," *Information Systems Control Journal*, vol. 3, 2001, p. 23-26

Northcutt, S.; *Network Intrusion Detection: An Analyst's Handbook*, New Riders, USA, 1999

Paliotta, Allan R.; "Cybersecurity and the Future of E-commerce: The Role of the Audit Community," *Information Systems Control Journal*, vol. 2, 2001, p. 29-30

Patzakis, John M.; "Computer Forensics—From Cottage Industry to Standard Practice," *Information Systems Control Journal*, vol. 2, 2001, p. 25-27

Pidanick, Ryan; "An Investigation of Computer Forensics," *Information Systems Control Journal*, vol. 3, 2004, p. 47-51

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

Piper, Fred; Simon Blake-Wilson; John Mitchell; *Digital Signatures—Security and Controls*, Information Systems Audit and Control Foundation, USA, 1999

Project Management Forum, *www.pmforum.org* (Includes numerous articles on project management methods and techniques)

Project Management Institute, *www.pmi.org* (Includes numerous articles on project management methods and techniques)

Project Management Institute, *A Guide to the Project Management Body of Knowledge*, USA, 2000

Proctor, P.; *The Practical Intrusion Detection Handbook*, Prentice Hall, USA, 2000

Robb, Drew; "Protecting Ports—Using an Event Log Manager to Improve Network Security," *Information Systems Control Journal*, vol. 4, 2004, p. 44-45

Ross, Steven J.; "Mahogany Row Mail Call," *Information Systems Control Journal*, vol. 3, 2001, p. 9-10

Ross, Steven J.; "Standard Questions," *Information Systems Control Journal*, vol. 2, 2001, p. 11-12

Ross, Steven J.; "Why Passwords Persist," *Information Systems Control Journal*, vol. 1, 2001, p. 13-14

Ross, Steven; "Penetrating Questions," *Information Systems Control Journal*, vol. 4, 2001, p. 11-12

SANS Institute, Security Consensus Operational Readiness Evaluation (SCORE), *www.sans.org/SCORE* (A site for minimum security standards)

Scammell, Tim; "Security Architecture: One Practitioner's View," *Information Systems Control Journal*, vol. 1, 2003, p. 24-28

Schneier, Bruce, *Secrets & Lies: Digital Security in a Networked World*, New York: John Wiley and Sons, USA, 2000

Schultz, Eugene; "The MSBlaster Worm: Going From Bad to Worse," *Network Security*, October 2003, p. 4-8

Schultz, Eugene; *Windows NT/2000 Network Security*, New Riders, USA, 2000

Schultz, Eugene; Jim Mellander; Daniel R. Peterson; "The MS-SQL Slammer Worm," *Network Security*, March 2003, p. 10-14

Schultz, Eugene; E. Spafford; "Intrusion Detection: How to Utilize a Still Immature Technology," in H. Tipton and M. Krause, *Information Security Management Handbook, 4th Edition*, Auerbach, USA, 2000

Shue, Lily; "The Global Status of Electronic Signature Legislation," *Information Systems Control Journal*, vol. 5, 2002, p. 24-26

Shue, Lily; "Virtual Private Networking—New Issues for Network Security," *Information Systems Control Journal*, vol. 1, 2001, p. 20-21

Singh, Simon; *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor, UK, 2000

Skoudis, Edward; *Malware*, Prentice Hall PTR, USA, 2003

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

Smith, Gordon E.: *Network Auditing: A Control Assessment Approach*, John Wiley & Sons, USA, 1999

Software Engineering Institute, "Spiral Development: Experiences, Principles and Refinements," Spiral Development Workshop, Special Report CMU/SEI -2000-SR-008, 9 February 2000

Stanley, Richard A.; "Wireless LAN Risk and Vulnerabilities," *Information Systems Control Journal*, vol. 2, 2002, p. 57-61

Srinivas, Sarva; "Cost-effective Implementation of Identity Management," *Information Systems Control Journal*, vol. 1, 2005, p. 49-50

Srinivasan, S.; Alan S. Levitan; "Secure and Practical Smart Card Applications," *Information Systems Control Journal*, vol. 5, 2003, p. 27-30

Stasiak, Ken; "Web Application Security," *Information Systems Control Journal*, vol. 6, 2002, p. 44-46

Stephenson, Peter; *Investigating Computer-related Crime*, CRC Press, USA, 2000

Tannenbaum, Andrew; *Modern Operating Systems*, Prentice Hall, USA, 2001

Trappe, Wade; Lawrence Washington; *Introduction to Cryptography with Coding Theory*, Prentice Hall, USA, 2002

University of New Haven Center for Cybercrime and Forensic Computer Investigation and the University of Southern California Department of Mathematics; "Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security," *Information Systems Control Journal*, vol. 2, 2001, p. 32-34

Walker, Tony; "Fighting Security Breaches and Cyberattacks With Two-factor Authentication Technology," *Information Systems Control Journal*, vol. 2, 2001, p. 41-42

Weber, Ron; *Information Systems Control and Audit*, Prentice Hall, USA, 1999, chapters 4, 5, 6, 7, 8, 10, 12, 17, 21, 22 and 23

White House, National Strategy to Secure Cyberspace Report, USA, *www.whitehouse.gov/pcipb/* (Includes recently released US national security baseline guidance)

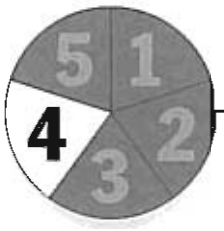
Willoughby, Mark K.; "Automated User Authentication: The Final Frontier of Information Security," *Information Systems Control Journal*, vol. 2, 2001, p. 21-23

Woodward, John D.; "Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint," University of Pittsburgh Law Review, USA, 1997, *www.pitt.edu/lawrev/59-1/woodward.htm*

Zwicky, Elizabeth D., et al; *Building Internet Firewalls, 2nd Edition*, O'Reilly, USA, 2000

Ziegler, Robert L.; *Linux Firewalls, 2nd Edition*, New Riders, USA, 2002

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.



Chapter 4:

INFORMATION SECURITY MANAGEMENT

4.1 DEFINITION

Direct, oversee and monitor information security related activities in support of organizational objectives.

Management is the process of achieving the objectives of the business organization by bringing together human, physical, and financial resources in an optimum combination and making the best decision for the organization while taking into consideration its operating environment.

4.2 OBJECTIVE

The objective of this job practice area is to focus on the tasks and knowledge necessary for the information security manager to effectively manage information security within an organization. A description of various techniques the information security manager can use and the areas the information security manager should focus on are discussed in this job practice area.

This job practice area represents 24 percent of the CISM examination (approximately 48 questions).

4.3 TASKS

There are eight (8) tasks within this job practice area:

1) Ensure that the rules of use for information systems comply with the enterprise's information security policies.
2) Ensure that the administrative procedures for information systems comply with the enterprise's information security policies.
3) Ensure that services provided by other enterprises, including outsourced providers, are consistent with established information security policies.
4) Use metrics to measure, monitor and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
5) Ensure that information security is not compromised throughout the change management process.
6) Ensure that vulnerability assessments are performed to evaluate effectiveness of existing controls.
7) Ensure that noncompliance issues and other variances are resolved in a timely manner.
8) Ensure the development and delivery of the activities that can influence culture and behavior of staff, including information security education and awareness.

4.3.1 Knowledge Statements

The CISM candidate must have a good understanding of each of the 16 areas delineated by the knowledge statements. These statements are the basis for the examination:

1) Knowledge of how to interpret information security policies into operational use
2) Knowledge of information security administration processes and procedures
3) Knowledge of methods for managing the implementation of the enterprise's information security program through third parties, including trading partners and security services providers
4) Knowledge of continuous monitoring of security activities in the enterprise's infrastructure and business applications

5) Knowledge of methods used to manage success/failure in information security investments through data collection and periodic review of key performance indicators
6) Knowledge of change and configuration management activities
7) Knowledge of information security management due diligence activities and reviews of the infrastructure
8) Knowledge of liaison activities with internal/external assurance providers performing information security reviews
9) Knowledge of due diligence activities, reviews and related standards for managing and controlling access to information resources
10) Knowledge of external vulnerability reporting sources, which provide information that may require changes to the information security in applications and infrastructure
11) Knowledge of events affecting security baselines that may require risk reassessments and changes to information security requirements in security plans, test plans and reperformance
12) Knowledge of information security problem management practices
13) Knowledge of information security manager facilitative roles as change agents, educators and consultants
14) Knowledge of the ways in which culture and cultural differences affect the behavior of staff
15) Knowledge of the activities that can change culture and behavior of staff
16) Knowledge of methods and techniques for security awareness training and education

4.3.2 Relationship of Tasks to Knowledge Statements

The task statements reflect what the CISM candidate is expected to be able to do within his/her position as an ISM. The knowledge statements delineate what the CISM candidate is expected to know to perform the tasks.

The task and knowledge statements are approximately mapped **figure 4.1**. Note that there is often an overlap. Each task statement will generally map to several knowledge statements as shown in the table below.

Figure 4.1—Knowledge and Task Statements Mapping

Task Statements	Knowledge Statements
1. Ensure that the rules of use for information systems comply with the enterprise's information security policies.	1. Knowledge of how to interpret information security policies into operational use
2. Ensure that the administrative procedures for information systems comply with the enterprise's information security policies.	1. Knowledge of how to interpret information security policies into operational use 2. Knowledge of information security administration process and procedures 9. Knowledge of due diligence activities, reviews and related standards for managing and controlling access to information resources
3. Ensure that services provided by other enterprises, including outsourced providers, are consistent with established information security policies.	1. Knowledge of how to interpret information security policies into operational use 3. Knowledge of methods for managing the implementation of the enterprise's information security program through third parties, including trading partners and security services providers 8. Knowledge of liaison activities with internal/external assurance providers performing information security reviews

Figure 4.1—Knowledge and Task Statements Mapping	
Task Statements	**Knowledge Statements**
4. Use metrics to measure, monitor and report on the effectiveness and efficiency of information security controls and compliance with information security policies.	4. Knowledge of continuous monitoring of security activities in the enterprise's infrastructure and business applications 5. Knowledge of methods used to manage success/failure in information security investments through data collection and periodic review of key performance indicators 7. Knowledge of information security management due diligence activities and reviews of the infrastructure
5. Ensure that information security is not compromised throughout the change management process.	6. Knowledge of change and configuration management activities
6. Ensure that vulnerability assessments are performed to evaluate effectiveness of existing controls.	10. Knowledge of external vulnerability reporting sources, which provide information that may require changes to the information security in applications and infrastructure 11. Knowledge of events affecting security baselines that may require risk reassessments and changes to information security requirements in security plans, test plans and reperformance
7. Ensure that noncompliance issues and other variances are resolved in a timely manner.	12. Knowledge of information security problem management practices
8. Ensure the development and delivery of the activities that can influence culture and behavior of staff, including information security education and awareness.	13. Knowledge of information security manager facilitative roles as change agents, educators and consultants 14. Knowledge of the ways in which culture and cultural differences affect the behavior of staff 15. Knowledge of the activities that can change culture and behavior of staff 16. Knowledge of methods and techniques for security awareness training and education

4.4 INFORMATION SECURITY MANAGEMENT OVERVIEW

In most organizations, the scope of responsibilities and range of activities of ISMs has increased dramatically during the past decade. Those now charged with protecting information hold a variety of titles ranging from chief information security officer at one end of the spectrum, to system administrator also in charge of information security at the other. Positions in the organizational hierarchy also vary greatly, from executive-level reporting to the CEO, to an ISM under the direction of an operations manager. In many organizations, the function of information security management is still seen primarily or entirely as technology related. In these organizations, information security is usually part of the IT department reporting directly or indirectly to the CIO.

The primary drivers for the growing role of the ISM have been the impact of a flurry of new laws and regulations coupled with the relentless growth in cybercrime and recognition of the near total dependence that organizations have on information assets. Legal requirements in many countries now demand that organizations provide for the protection of personal information, retention of certain types of information for specific periods, and the public disclosure of security- and financial-related information. Many of these regulations hold senior management personally responsible under the threat of heavy fines and potential imprisonment.

The increasing recognition by organizations of their near absolute dependence on their information is also driving information security issues to the highest levels of management. These factors have resulted in the elevation of ISMs in the organizational hierarchy. Studies over the past few years have shown a continuous increase in the number of CISO and executive level ISMs year over year.

4.4.1 Management Commitment

In some organizations, the level of management commitment may be less than complete and the ISM may be restricted in his/her effectiveness. Under these circumstances, it may be useful to make an effort to educate senior management in the areas of regulatory compliance and the organization's dependence on its information assets. It may also be useful to document risks and potential impacts faced by the organization, making sure senior management is informed of the results and find them acceptable.

If management is committed to adequate information security, it will be evident by:
- Clear approval and support for formal security strategies, policies, monitoring and measuring organizational performance in implementing security policies
- Supporting security awareness and training for all staff throughout the organization
- Providing adequate resources to implement and maintain security activities

Since information security is not necessarily a part of general management expertise, it may be productive to consider a special security awareness training program specifically for high-level managers.

4.4.2 IT Security and Information Security

Information security management in most organizations is becoming more about management than technology. There is often confusion over the difference between IT security and information security. The distinction is frequently blurred and the terms often used interchangeably. However, as these fields continue to grow in importance, the scope of responsibilities and skills required should be clarified.

Managers of IT security generally have substantial computer skills and a technical background. They generally will have knowledge of firewall configuration and server hardening, technical baselines, technical specifications, and vulnerability scans. Their charter is to ensure the secure operation of the technical infrastructure utilized in the organization's operations and will be technology centric.

Information security management is by necessity more generalized and encompasses a greater scope with less technology orientation. Responsibilities will include technical and nontechnical aspects of information security. Typically, there will be greater involvement in business processes and overall security strategy and far less direct involvement in the actual technology. The ISM will also be more involved in regulatory compliance, risk management and governance. Activities of an ISM will be information centric regardless of whether technology or physical processes are involved.

4.4.3 The Importance of Information Security Management

It has often been stated that security is a process not an event. A well-conceived strategy and the implementation of a security program must be well managed on an ongoing basis. Information security management is a continuous, ongoing requirement necessary to provide assurance that the organization's vital information assets are protected and that legal and regulatory obligations are met

Many organizations have not implemented security governance and have failed to clearly identify the objectives of information security. Without an understanding of the goals, it will be difficult or impossible to determine whether the information security program and its management are successful. It will be guesswork for the ISM on what goals to manage and whether protection efforts are adequate or excessive. For security management to be effective, the objectives for the organization's security activities must be clearly identified. Typically, these objectives will be stated in terms of a desired state described by a series of attributes. These can include acceptable levels of impact, maturity based on the CMM, key performance indicators, and many others, as identified in chapter 1.

4.4.4 Outcomes of Information Security Management

Effective security management can be gauged by the extent that the governance objectives defined in chapter 1 are achieved. In organizations where a security strategy has not been defined, managing information security to achieve the six following outcomes can be a reasonable and effective alternative.

The outcomes of effective security governance are defined as:
1. Strategic alignment
2. Risk management
3. Value delivery
4. Resource management
5. Performance measurement
6. Integration of assurance functions

4.5 EFFECTIVE INFORMATION SECURITY MANAGEMENT

As responsibilities of the ISM have increased, the number of tasks and skills needed have grown as well. Security budgets have been generally increasing as has security staff in most organizations. Where once the predominant focus was on technical skills, ISMs increasingly need traditional management skills in addition to understanding security concepts and technology.

To be effective, information security must be pervasive affecting every aspect of the enterprise to some extent. As a consequence, the range of responsibilities for effective security management is broad and in most cases exceeds the direct authority of the ISM. As a result, the ISM is most likely to be successful operating in a collaborative fashion, being a good communicator and by developing a persuasive business case for security initiatives.

4.5.1 Scope of Responsibilities

As the scope of responsibilities of the ISM has mushroomed, a risk is that important security elements may be overlooked or neglected. A comprehensive, well-managed security program will normally address the following issues including:
- A security strategy with senior management acceptance and support
- A security strategy intrinsically linked with business objectives
- Security policies that are complete and consistent with strategy
- Complete standards for all relevant policies
- Complete and accurate procedures for all important operations
- Clear assignment of roles and responsibilities
- Information assets that have been identified and classified by criticality and sensitivity
- Effective controls that have been designed, implemented and maintained
- Effective monitoring processes in place
- Effective compliance and enforcement processes
- Tested, functional, incident and emergency response capabilities
- Tested business continuity/disaster recovery plans
- Appropriate security approval in change management processes
- Risks that are properly identified, evaluated, communicated and managed
- Adequate security awareness of all users and training as needed
- The development and delivery of the activities that can positively influence security orientation of culture and behavior of staff
- Understanding and addressing regulatory and legal issues
- Addressing security issues with third-party service providers
- Resolving noncompliance issues and other variances in a timely manner

A number of useful standards and approaches are available that can be useful in managing a security program. These standards and approaches can be categorized as utilizing one of five perspectives:
- **Process-oriented**—ISO 9001:2000, BS7799-2:2002, CMM, ITIL/ITSM, ISM3
- **Controls-oriented**—ISO 13335-4, BSI-ITBPM, COBIT
- **Product-oriented**—Common Criteria
- **Risk analysis-oriented**—Octave, Magerit
- **Best practices-oriented**—ISO/IEC 17799:2002, COBIT, ISF-SGP

An effective ISM should be familiar with many of these approaches and utilize relevant elements in selecting the management approach best suited to the organization. Some may prove more cost-effective and provide better form, fit and function depending on organizational structure, culture, available resources, business sector, etc.

Regardless of standards or methods used, as with other aspects of information security, to be effective, information security management requires senior management commitment and support. Rarely, if ever, are security programs successful without it.

4.5.2 Roles and Responsibilities

The ISM has the responsibility for managing the information security program to achieve the outcomes listed in section 4.3. It is the responsibility of senior management to support those objectives and provide adequate resources to ensure that objectives are achieved. The roles and responsibilities of other assurance providers must also be clearly defined to prevent gaps in protection. A part of those responsibilities must be to provide defined interfaces between functions and clear channels of communication. For example, the activities of an organizational risk manager should dovetail with information security risk management to ensure continuity of efforts. Business continuity planning is often a separate function that must integrate with incident response activities.

4.6 INFORMATION SECURITY MANAGEMENT CONCEPTS

There are core concepts essential to effective security management. The ISM should be familiar with these concepts and understand how to put them into practice.

4.6.1 Concepts

4.6.1.1 Strategic Alignment

Aligning information security with business strategy to support organizational objectives is critically important for information security to achieve its objectives. Even if the strategy has been successfully aligned with business objectives, it will require ongoing processes to ensure continued alignment as business strategies change and adapt to market conditions.

Successful ongoing alignment is often accomplished through an active steering committee with representation of all the organizations major lines of business. Business alignment may also be improved through active relationships with leaders of business units and regular contact.

If the organization has a strategic business planning unit, active participation in its activities may also provide insight into future business directions and ensure security considerations are included in the planning process. This may provide opportunities to orient security activities to support those objectives and identify potential risks.

Efforts to align security with business objectives must include consideration of security solutions that are a good fit for existing enterprise processes and take into account the culture, governance, style, technology and structure of the organization.

4.6.1.2 Risk Management

Risk management for information assets is a primary responsibility of the ISM and an ongoing activity. The topic has been reviewed in chapter 2. The ISM must develop a comprehensive understanding of threats the organization faces, its vulnerabilities and its risk profile. The potential impacts if threats materialize must be evaluated and protection priorities established based on criticality and sensitivity of information assets. Risks must be managed to a level acceptable to the organization.

4.6.1.3 Value Delivery

Security investments should be managed to optimize support of business objectives. The ISM should direct efforts at achieving a standard set of security practices and establish security baselines and practices proportionate to risk. Protection efforts must be prioritized to allocate limited resources to provide protection to areas of greatest impact and business benefit.

Security solutions should be institutionalized and use standards-based approaches. Solutions must be complete covering technical and physical elements based on an understanding of the end-to-end business processes of the organization. Security management cannot remain static and must strive to attain a culture of continuous improvement.

4.6.1.4 Resource Management

The ISM must endeavor to utilize security knowledge and infrastructure efficiently and effectively. This can be accomplished by ensuring that knowledge is captured and made available to those that need it. Security processes and practices must be documented, they must be consistent with standards and policies, and security architectures should be developed to define and utilize infrastructures to achieve security objectives efficiently.

4.6.1.5 Performance Measurement

The ISM must develop monitoring and metrics to provide continuous reporting on the effectiveness of information security processes and controls. The metrics utilized should be defined, agreed on by management and be aligned with strategic objectives. Care must be taken to ensure that metrics provide useful information relevant to security objectives. These measurement processes will help identify shortcomings and failures of security activities and provide feedback on progress made in resolving issues. The ISM should always seek independent assurance from periodic external assessments and both internal and external audit.

4.6.1.6 Business Process Assurance

It is important for the ISM to understanding and integrate all organizational assurance functions to ensure business processes operate as intended and are adequately protected from compromise from end to end. The ISM should develop formal relationships with other assurance providers and endeavor to integrate those activities with information security activities. In the typical organization, this might include physical security, risk management, privacy office, quality assurance, audit, change management, insurance, human resources, business continuity, disaster recovery and perhaps others.

4.6.2 Technologies

The elevation of information security management is relatively new and often requires the ISM to have a foot in each of two worlds—security technology as well as traditional management. The technology elements generally required in implementing a security program have been covered in chapter 3 and include:

- Firewall technology
- User account administration
- Intrusion detection and intrusion prevention technology
- Antivirus technology
- Certificate authority technology (PKI)
- Biometric technology
- Encryption technology
- Privacy compliance technology
- Remote access technology
- Digital signature technology
- EDI and EFT technology
- VPN technology

- SET technology
- Forensics technology
- Monitoring technologies
- Log reading and correlation technologies
- Data labeling technologies
- Document and e-mail content scanning technologies

4.7 IMPLEMENTING INFORMATION SECURITY MANAGEMENT

When a security program has been implemented, it must be managed on an ongoing basis.

It may be important to consider that many ISMs have their beginnings in technical fields, such as system administration, and as security becomes more critical, they find themselves with increasing requirements to develop management skills. To be effective as they move from the technical realm to an increasingly managerial role, ISMs would be well advised to consider training in management skills covering topics such as leadership, budgeting and general administration.

A working definition of management is: "Effective utilisation and coordination of resources such as capital, plant, materials, and labour to achieve defined objectives with maximum efficiency."[23]

If a formal strategy, as discussed in chapter 1, has been developed, consideration of resources and priorities has already been worked into an action plan, which translated into the information security program discussed in chapter 3.

Many organizations have not developed detailed security strategies linked to overall business objectives. In this case, priorities can be determined best based on a risk assessment and a business impact analysis as discussed in chapter 2.

As a practical matter, some ISMs manage security by utilizing good or best practices and standards of due care sometimes coupled with security baselines. While this can yield acceptable results in some situations, information security is not likely to be optimal or achieve any degree of alignment with business objectives. The level of protection will not be proportional to risk, potential impact or asset value.

If resource or other constraints do not allow for a comprehensive impact analysis, a business dependency assessment may be a less costly alternative to provide the basis for allocating available resources. A business dependency assessment reviews what resources are used to conduct business. The critical assets and resources are identified and provide the basis for allocating protection efforts.

4.7.1 Integrating Assurance Activities

As has been discussed in previous chapters, a major objective for security activities is to provide assurance to business operations that adverse events will not significantly impact the ability to achieve objectives. However, the objective of security is to provide an acceptable level of predictability of operations in terms of confidentiality, integrity and availability of information assets. Organizations usually have numerous assurance functions that are relevant to information security management efforts. It is important for the ISM to identify these functions and develop an approach to utilizing them as resources and find ways to integrate them with information security activities.

Elements of security are, or should be, provided by a number of departments as a part of their normal operations. For example, most larger organizations will have functions that include, but are not limited to:
- Risk management
- Audit
- Privacy
- Compliance
- Strategic planning
- IT, including IT security

[23] Leitner, Andreas; "Concepts of Leadership and Management," Wales Business School, 2004

- Human resources
- Legal
- Physical security
- Change management
- Quality assurance
- Project office
- Business continuity and disaster recovery

There may be a number of others as well, and the functions will often have different names. Nevertheless, all of these functions normally have information security responsibilities and implications for overall security in the organization. They all constitute potential resources for the ISM in managing a security program to secure information assets.

Usually, security across these functions will not be integrated, and security often will be inconsistent with gaps in protection. Integrating the security-related activities of these various departments can do a great deal to improve the overall security posture of the organization.

Generally, there are two ways to approach achieving integration of these diverse activities. One will be by formation of a security steering committee consisting of representatives from these areas in addition to members of the business units and/or operations. The steering committee should have a clear charter of its responsibilities, authority and obligations, and meet on a consistent basis.

The other approach is through complete, well-crafted policies and standards. Policy and standards development is covered in chapter 1. Policies backed by standards that capture the intent and direction of senior management and are aligned with the organization's business objectives will provide the basis for effective management of information security. They can be used to achieve better practices in securing information assets through persuasion, audits, security reviews and compliance enforcement.

Once comprehensive policies have been created and approved by senior management, standards provide the ISM with a powerful tool to promote the security agenda. Required compliance with properly written standards that support the policies can be used to influence the organization into functioning in a manner that supports security objectives.

Many organizations use the ISM in a consultative mode to advise other departments on appropriate security measures in the performance of their functions. This can be an effective way to promote the security agenda and provides an opportunity to monitor the organization's security posture.

4.7.2 Controls

A major part of security management is the design, implementation, monitoring, testing and maintenance of controls. Controls are defined as the policies, procedures, practices, technologies and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesirable events will be prevented or detected and corrected.

Controls can be physical, technical or procedural. The choice of controls can be based on a number of considerations including ensuring their effectiveness, that they are not unduly expensive or restrictive to business activities, and what the optimal form of control will be. Extensive information is available on developing control objectives and implementing specific controls from COBIT and other sources.

Controls are one of the primary methods of managing information security risk and a major responsibility of information security management. It is important to understand that controls for physical elements, such as administrative processes and procedures, are just as critical as controls applied to technology. Most security failures can ultimately be attributed to failures of management, and it must be remembered that management problems typically do not have technical solutions. Inevitably, people and physical processes exist at each end of technical processes and may constitute the greatest risks to information security. As a consequence, the ISM must be careful not to place excessive focus and reliance on technology.

It must also be considered that security policies, standards or procedures that are too restrictive and do not enable the organization to meet its business objectives and restrict access to information resources too stringently will be quickly circumvented. The objective is to balance the need for controls with the requirements of the business.

Therefore, it is vital that the information security manager have a good business perspective, understand the risks to the organization's information resources, interpret the information security policies and implement security controls that consider all of these aspects.

The ISM must be aware that information security controls must be developed for IT- and non-IT-related information processes. This will include secure marking, handling, transport and storage requirements for physical information. It must include considerations for handling and preventing social engineering. Environmental controls must also be taken into account, so that otherwise secure systems are not subject to simply being stolen, as has occurred in some well-publicized cases.

There are a number of standards and guides available for information security management that should be familiar to the ISM. One of the most accepted for technical and nontechnical components of information security is the ISO/IEC 17799 Code of Practice, now ISO 27001.

Numerous other sources of guidance include COBIT, FIPS Publication 200 and NIST 800-53, and a number of excellent standards from Australia.

ISO 27001 is a standard setting out the requirements for an information security management system. It helps identify, manage and minimize the range of threats to which information is regularly subjected.

IT is organized into 10 sections:
- **Security policy**—This provides management direction and support for information security
- **Organization of assets and resources**—To help manage information security within the organization
- **Asset classification and control**—To help identify assets and appropriately protect them
- **Personnel security**—To reduce the risks of human error, theft, fraud or misuse of facilities
- **Physical and environmental security**—To prevent unauthorized access, damage and interference to business premises and information
- **Communications and operations management**—To ensure the correct and secure operation of information processing facilities
- **Access control**—To control access to information
- **Systems development and maintenance**—To ensure that security is built into information systems
- **Business continuity management**—To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
- **Compliance**—To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement

ISO/IEC 27001:2005 is the updated version of BS 7799-2:2002. The main change to the standard is that it is now international. This means that in addition to international recognition and acceptance of the British standard, organizations can develop and implement a global framework for managing the security of their information. The final version of this standard was released on 15 October 2005.

4.7.3 Security Policies

4.7.3.1 Managing Information Security to Comply With Policies

A well-defined security strategy, as discussed in chapter 1, will provide the basis for effective, consistent and complete security policies. From a security management perspective, policies providing a clear statement of management intent, consistent with the objectives of the strategy, are essential. Topics addressed may include the importance of information assets, need for security, importance of defining sensitive and critical assets to protect in regards to confidentiality, and integrity and availability of those assets. Policies should also be consistent with and mapped to a standard such as ISO 27001. This can serve as a checklist to ensure that all relevant topics are covered.

4.7.3.2 Interpreting Information Security Policies for Operational Use

Policies, to be of any use, must be implemented at the operational level and a process for monitoring and ensuring compliance must be put in place. The completion of comprehensive standards and procedures for all important operations coupled with defined roles and responsibilities will provide the tools for managing an effective security program. Procedures at the operational level must be developed by, or with the involvement of, the operational units that will use them. This will ensure that they are functional and accurate while the security department ensures that they comply with policy and standards.

4.7.4 General Rules of Use/Acceptable Use Policy

While specific procedures will provide the detailed steps required for many functions at the operational level, there will still be a large group of users that will benefit from a user-friendly summary of what they should and should not do to comply with policy.

An effective way of assisting these general users in understanding security-related responsibilities is the development of an acceptable use policy. This policy can detail in everyday terms, the obligations and responsibilities of all users in a straightforward and concise manner. Obviously, it is then necessary to effectively communicate the use policy to all users and ensure it is read and understood. The use policy should be provided to all new personnel that will have access to information assets regardless of employment status.

Typically, these rules of use for all personnel will include the policy and standards for access control, classification, marking and handling of documents and information, and reporting requirements and disclosure constraints. They may also include rules on e-mail and Internet usage as well as other information resources and assets. The rules of use provide a general security baseline for the entire organization. It is often necessary to provide supplemental or additional information to specific groups in the organization consistent with their responsibilities.

4.7.5 Security Standards

Standards are an important tool for security management. They provide the basis for determining that a procedure or, set of procedures, meet policy requirements. A standard provides the unambiguous allowable limits for any set of procedures and processes whether manual or automated.

By providing the concise allowable parameters for procedures, they can serve to enhance the effectiveness of the security manager, reduce his/her workload and make the development of procedures more consistent and easier to generate at the operational level.

For example, the standard for encryption might specify that triple DES or AES must be used for the protection of information categorized as confidential and may also specify the minimum (and maximum if applicable) key lengths and other attributes as needed. Key requirements might be specified elsewhere under access control, but for ease of use, it would be a good idea to duplicate that part of the relevant encryption standard within corporate standards to assist a software engineer utilizing it for preparing technical specifications.

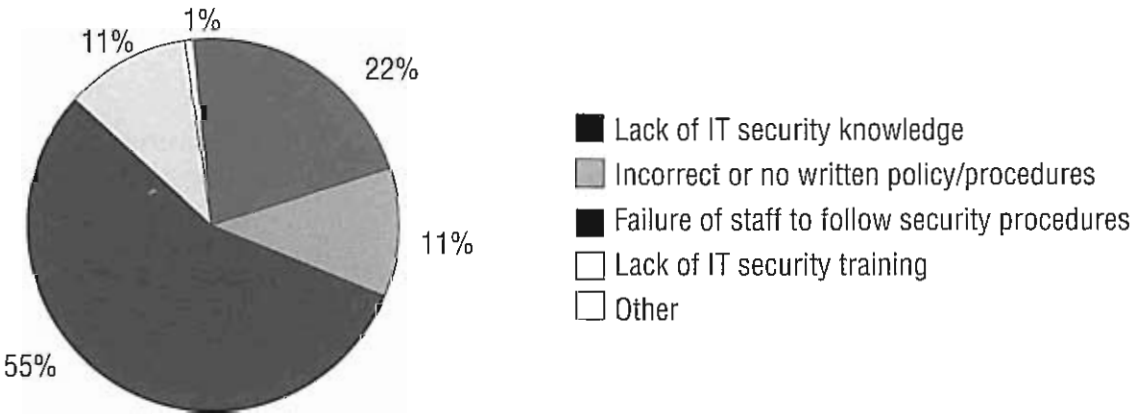
Well-devised standards are also important for the security manager in compliance auditing, since they will make it clearly evident whether a particular process or procedure is consistent with policy.

4.7.6 Security Procedures

Procedures must be developed for all important processes. They must be clear and unambiguous. The terms used must include 'must', 'shall', 'will' to specify required actions. 'Should' must only be used to specify a desired action that is not mandatory. 'May' and 'can' must only be used to denote purely discretionary actions. Procedures whether technical, physical, manual or automated must meet standards and comply with the enterprise's information security policies.

The research data from 2003 CompTIA study suggests that there over half of the errors creating information security problems is caused by failure to follow procedures. This may be because they do not understand the procedures, influences from daily operations do not focus on procedure compliance, or procedures are not easily available when needed. The second largest error is cause by lack of security knowledge.

Figure 4.2—Analysis of IT Security



Source: CompTIA, "Analysis of IT Security and the Workforce," March 2003

The information security manager must be intimately familiar with the various information security administration processes and procedures that an organization may employ. The administration of security is a critical part of maintaining the overall security program and ensuring its effectiveness.

Security administration processes are continually being automated and many of the activities involved in granting access authority to staff are performed through security-related software applications. Often those responsible for the information resource use applications to request that various staff are granted access authority. The request is then approved and the tasks involved in granting the authority are performed automatically. It is important that this activity is securely logged and that logs are reviewed on a regular basis to determine that there are no irregularities. Various automated log readers are available that can, to some extent, automate the chore.

It should be noted that while automated systems improves responsiveness, the risks involved with authentication of the responsible party and the appropriateness of the access granted must be considered and addressed by the information security manager.

Since authentication is the first line of defense, it is important that all methods of granting system access are subject to specific controls and monitoring to minimize the risks associated with unauthorized access.

The standards will provide the basis for ensuring procedures meet policy requirements. The following example shows how a policy, standard and procedure should be related:

- **Access policy**—Access controls must be implemented that ensure only authorized access to information assets.
- **Password standard**— Password shall be comprised of not less than eight different alphanumeric upper and lower case characters and include one punctuation mark. Passwords shall be changed every three months or less and reuse shall be precluded.
- **Procedure**—Users will be issued a one-time password upon dialing the help desk. They must log on within 24 hours and follow on-screen directions for changing the password. The password must:
  - Be at least eight characters
  - Be upper and lower case
  - Contain at least one number and one punctuation mark
  - Not have been used before
  - Must not be written down

The user will be notified on-screen when the password has been successfully changed.

It should be noted that to comply with this policy, physical access standards and procedures must also be developed. There might be just one physical access standard for the entire organization, while there could be numerous sets of procedures depending on the facilities.

It is more likely that each policy will have a number of standards, which, in turn, may control numerous procedures.

Procedures that meet the standards can also be developed to define the steps necessary to develop minimum-security baselines, measures, and specific requirements and practices with which individual systems are integrated into the network and subsequently maintained.

4.7.7 Assignment of Roles and Responsibilities

To manage security, it must be clear who does what and who is accountable. Failure to do so will invariably lead to a failure of security and pieces "falling between the cracks."

Each of the areas identified (and perhaps others not mentioned) in section 4.3 at the beginning of the chapter must be someone's specific responsibility. In larger organizations, each of the items stated may be a separate department, while in smaller companies, one individual may be responsible for a number of the items. In either case, specific responsibility must be assigned to an individual and processes and procedures for discharging those responsibilities must be developed.

4.7.7.1 Managing Security Roles and Responsibilities

From a management perspective, it is important to carefully consider security roles and responsibilities. It is not uncommon to see organizations attempt to reduce cost by using specialist that are also expected to perform a variety of nonrelated tasks. For example, hiring a security architect that is also expected to configure firewalls and administer databases. Information security efforts are complex specialties.

The ISM should consider that some security activities are sporadic and intermittent, whereas others are ongoing and continuous. For example, design work such as architecture will only need to be done periodically, whereas system administration and compliance efforts will be ongoing. To be effective, the ISM should consider these elements when staffing a security organization. Periodic activities may be more effectively accomplished by consultants and contractors, while ongoing administrative activities are likely to be accomplished on a more cost-effective basis by permanent staff.

4.7.8 Trading Partners and Security Providers

4.7.8.1 Services Provided by Other Enterprises Align With Established Policies

Enterprises often have services provided by departments, divisions, subsidiaries and outside providers. This does not relinquish the security responsibility of the organization, nor does it imply delegated responsibility. The information security manager should take steps necessary to ensure that trading partners are in compliance with the enterprise's established information security policies. It should be noted that this is often a difficult undertaking, but the effort must be made as malicious code is often introduced through outside entities. To the extent it is not possible to ensure the security of external parties, it may be necessary to introduce specific internal countermeasures and controls to minimize the risks posed.

Outsourced providers are a viable strategy that the information security manger can use to asssist in the design and operation of the organization's information security program. However, to the extent possible, the information security manager needs to ensure that the outsourced provider complies with the organization's established information security policies.

If the organization's security relies primarily on perimeter defenses, extending the perimeter through external providers can pose a substantial risk and appropriated mitigation measures must be considered.

During the proposal and evaluation process that the ISM undertakes in assessing and contracting with security vendors, the ISM should discuss the requirements and parameters of the organization's information security policies with the vendors. The vendor's compliance with these security policies should be high on the list of decision factors when selecting a vendor. The information security manager should understand any variances that may exist and whether or not the service provider can comply with the security policies. Often this same proposal and evaluation process is used when evaluating whether to use an organization's autonomous division or subsidiary for select services.

The ISM should also ensure that the compliance factors are clearly defined in the service level agreement with the security provider (whether internal or external). This will help the ISM to manage the performance of the security provider and ensure that they are meeting their agreement to comply with the organization's security policies.

4.7.8.2 Implementing Information Security Program Through Third Parties

The ISM should have an understanding of the security posture of trading partners and security services providers. This will help identify risks that may exist in connecting to their systems. There are two aspects involved here:

- Trading partners that do not have a robust information security program may present a security risk. One common example is the ability for vendors to review stock inventories at retailers. In the design and development of this type of application access, security should be addressed and controls put into place to limit the risk that this type of connectivity may present.
- A key concern to the information security manager is how a security services provider will maintain the organization's information security program. The service level agreement (SLA) is a key tool the ISM can use to ensure that the security services provider complies with internal security requirements. Risks, including commingling of data with other customers, are a concern that any third-party service provider should be able to address.

In addition, the ISM should have crisis management mechanisms in place to react to incidents that may occur due to the use of trading partners or security services providers. The mechanisms should include processes to react to those warnings that security service providers may communicate to the organization.

4.7.9 Security Metrics and Monitoring

A requirement of effective security management is to ensure continuous feedback on a variety of security-related elements. It is axiomatic that what cannot be measured, cannot be managed. Without feedback, it will be difficult to determine if the information security program is achieving its objectives and whether trends are in the right direction.

To assess the effectiveness of an organization's security program(s), the ISM must have a thorough understanding of how to monitor security programs and controls on an ongoing basis.

Monitoring processes are required to ensure compliance with applicable laws and regulations to which the organization is subject. A number of industries in recent years have become subject to specific regulations to ensure the security and privacy of sensitive information especially in financial and health care organizations and to reduce operational risks in national critical infrastructure organizations. Failure of compliance in these cases can have adverse legal implications, so adequate monitoring is a requirement.

Some monitoring will be technical and quantitative in nature while other aspects will, by necessity, be imprecise and qualitative.

Technical metrics can be used to provide quantitative monitoring and can include elements such as:
- Number of unremediated vulnerabilities
- Number of closed audit items
- Number or percentage of user accounts in compliance with standards
- Perimeter penetrations
- Unresolved security variances

Qualitative metrics can be used to determine trends and can include such things as:
- CMM maturity levels at periodic intervals
- Key performance indicators
- Key goal indicators
- Balanced business scorecard
- Six Sigma quality indicators
- ISO 9001 quality indicators

Other relevant measures of significance can include the cost-effectiveness of controls, the extent of control failures, etc.

Other monitoring activities relate to organizational compliance with security policies and procedures established by the organization as a security baseline in reducing risk to acceptable levels for established information security programs. As information resources change over time, it is important to be aware that both the security baseline and the resources must adapt to changing threats and new vulnerabilities. It is important that all stakeholders are aware of these changes and an appropriate consensus is reached.

4.7.9.1 Monitoring Approaches

It is important for the security manager to develop a consistent, reliable method to determine the overall ongoing effectiveness of the program. One way is to regularly conduct risk assessments and track improvements over time. Another standard tool is the use of external penetration testing to determine perimeter vulnerability. Internal penetration testing is of value in determining configuration and other weaknesses. Doing so on a regular basis and tracking the results can be a useful indicator of trends. Most organizations conduct regular vulnerability scans to determine if open vulnerabilities are addressed and to see if new ones appear. Steady improvement is the hallmark of an effective program

Many other metrics are possible and may include technical and behavioral measures (i.e., patch status, virus infections, password resets, social engineering)

In designing metrics, a baseline should be established for each measurement. Good metrics should have **SMART** attributes (i.e., specific, measurable, attainable, repeatable and time-dependent). The metrics can then be used to chart progress.

In addition to monitoring automated security activities, the organization's change management activities also should feed the ISM's monitoring program. Metrics are important, but of little use if adverse trends are not dealt with in a timely manner.

The ISM should have a process in place whereby metrics are reviewed on a regular basis and any unusual activity is reported. An action plan to react to the unusual activity should be developed as well as a proactive plan to address trends in activity that may lead to a security breach or failure.

4.7.9.2 Monitoring Security Activities in Infrastructure and Business Applications

Since the organization's vulnerability to security breaches likely exists 24/7, continuous monitoring of security activities is a prudent business process that the ISM should implement.

Continuous monitoring of IDSs and firewalls can provide real-time information of attempts to breach perimeter defenses. Training help desk personnel to escalate suspicious reports that may signal a breach or an attack can serve as an effective monitoring and early warning system. This information can be critical to taking corrective action in a timely manner.

IDSs are becoming increasingly more intelligent, as they may detect direct, unauthorized access attempts and may provide intelligent analysis to indicate trends. This may allow proactive steps to be taken to prevent successful attacks against the organizations information systems.

Other after-the-fact monitoring techniques include event logging, log reviews, compliance assessments, network- and host-based intrusion systems, and penetration testing.

The greatest achievement for information security managers is to consolidate various security event-monitoring techniques into a single console that the security team monitors. While improvements in this direction are taking place, it is unlikely that a complete "security dashboard" will be available in the near future. As a result, a variety of methods and techniques must be employed to monitor security that is tailored to the organization.

4.7.9.3 Determining Success of Information Security Investments

It is important for the security manager to have processes in place to determine the overall effectiveness of security investments and the extent to which objectives have been met. There is always competition for resources in organizations and senior management will seek to obtain the best returns on investment and justify costs.

During the design and implementation of the security program, the ISM should ensure that key performance indicators are defined and agreed to and that a mechanism to measure progress against those indicators is implemented. This way the ISM can assess the success or failure of various components of the security program and whether or not they are cost justifiable. This will be helpful when developing a business case for other elements of a security program.

Actual costs for various components of a security program need to be accurately determined to determine cost-effectiveness. It is useful to use the concept of TCO for evaluating the various components of a security program. In addition to initial procurement and implementation costs, it is important to include the staff needed to administer controls, maintenance fees, update fees, consultant or help desk fees, and fees associated with other interrelated systems that may have been modified to accommodate security objectives.

4.7.10 The Change Management Process

Virtually all organizations employ some form of change management process. In some cases, it may not be formal. The ISM should identify all change management processes used by the organization to tap into them for notification that changes are taking place that may impact security.

4.7.10.1 Protect Information Security in Change Management Process

The information security manager needs to implement processes, whereby security implications are considered in each change management process that the organization supports. Security needs to be monitored and maintained continuously, as new vulnerabilities may be introduced as a result of system or process changes.

A common risk is the development or implementation of a new application that accesses outside networks. If those networks are not compliant with the requirements of the organization's security policies and procedures, it may introduce new risks to information resources.

If an application is developed internally, it is important that security elements are introduced early in development cycle to minimize vulnerabilities and ensure compliance with the organizations security standards. It will be important to ensure that technical specifications include the security requirements set forth in the organization's standards comply with policy. Testing and quality assurance plans must also be subject to review by the security manager to ensure that the security elements are properly tested and certified. In some cases, for software developed for critical operations, it may be necessary to perform a proper code review in addition to the QA process. Code reviews are often outsourced for an independent review where high assurance is required.

As changes are made to systems and processes over time, there is often a tendency for security controls to become less effective. Therefore, it is critical for the security manager to be involved with the change management process and ensure that new vulnerabilities are not introduced during the change process. It is also important that security controls and countermeasures are updated regularly and are adapted to organizational changes.

Decentralized organizations can pose a special challenge to the security manager. Often, many of these divisions are highly autonomous and it may be difficult to monitor and ensure compliance with corporate policies and procedures. It is important to understand the organizational structure during development and implementation of a security program to develop an effective approach.

4.7.10.2 Change and Configuration Management Activities

Change and configuration management approaches vary widely between different organizations, as do roles and responsibilities. It is important for the security manager to understand how the process works and who is responsible for the required actions, so that processes and events with security implications can be managed early in the process. This will help prevent new risks from being introduced into production systems.

4.7.11 Vulnerability Assessments

Vulnerability assessments are one of the key tools that the ISM has available to assess the effectiveness of the information security program in managing risk. Vulnerability assessments typically include:
- Scanning various security controls to determine if there are vulnerabilities
- Testing the controls in place to determine their effectiveness
- Penetration testing to locate vulnerabilities
- Developing recommendations to reduce vulnerabilities and improve security
- Remediation activities and tracking progress

Vulnerability assessment tools are an effective method to identify the exploitable vulnerabilities and allow proactive and preventive measures to be taken to protect the networks and systems.

This approach is often used because it may be the most cost-effective way to manage risks to IT systems. It should be understood, however, that a vulnerability for which no threat exists is not a risk and may not need to be addressed, or its priority for remediation can be lowered. Likewise, it must be remembered that a vulnerability, even if exploited, that has no impact is not significant either. This is important to consider in order for the ISM with limited resources to properly prioritize remediation efforts.

The most common vulnerability assessment tools include host-based, network-based, modem detection and password cracking tools. Network-based vulnerability assessment tools use the network as a medium to scan individual hosts to determine if there are exploitable vulnerabilities. The primary goal of vulnerability assessment is to detect known deficiencies in a particular environment that potentially could lead to a system compromise.

A vulnerability assessment typically will include the assessment of:
- System utilities
- Operating systems weaknesses
- Network deficiencies
- Applications (including databases, web applications, e-mail)

The information security manager may also employ a third party, typically a security consultant, to perform vulnerability assessments. This provides an independent view of vulnerabilities that may pose a risk to the organization. Vendors have begun to provide managed vulnerability assessments, whereby the assessments are performed on a regular basis. This can be useful since new vulnerabilities are constantly being identified. The assessments should include recommendations on how to mitigate the vulnerability or other options for managing the risk posed by the identified vulnerabilities.

Vulnerability assessments are useful to determine weaknesses in the system but are just one component of a risk. It is important to keep in mind that there must be a threat to exploit a vulnerability that must, in turn, cause an impact. Vulnerabilities for which no threat exists are not important. A threat that exploits a vulnerability that causes no impact are not important either.

The ISM must also remember that vulnerability scans do nothing to determine weaknesses in physical facilities, processes, procedures or personnel. Other methods must be developed to ensure these vulnerabilities are assessed on an ongoing basis.

4.7.12 Due Diligence

Due diligence is essentially a term related to the notion of the "standard of due care." It is the idea that there are steps that would be taken by a reasonable person of similar competency in similar circumstances. In the case of an ISM, this would mean ensuring that the basic components of a reasonable security program are in place. Some of these components might include among others:

- Senior management support
- Comprehensive policies, standards and procedures
- Appropriate security education, training and awareness throughout the organization
- Periodic risk assessments
- Effective backup and recovery processes
- Implementation of adequate security controls
- Effective monitoring and metrics of the security program
- Effective compliance efforts
- Tested business continuity and disaster recovery plans

It is also important to take into consideration that the third parties the organization uses and relies upon can present risk to information resources. Due diligence regarding contracts and agreements must also take place.

Periodic reviews of the infrastructure, preferably by an independent knowledgeable third party, may be a reasonable requirement as well. The infrastructure is a critical component the organization relies upon to meet its business objectives and risks must be identified and reasonably addressed.

4.7.12.1 Liaison Activities With Internal/External Assurance Providers

Assurance in security can be provided by several types of commercial monitoring services that can determine potential compromise or its absence. Typical providers of assurance include firewall and IDS monitoring on a continuous basis.

The ISM, having primary responsibility for the organization's security program, should act as a liaison with internal and external assurance providers, so their activities can be effectively integrated into the overall security program.

The assurance process is a key component in the information security program and the overall security effort may benefit by the periodic reviews and recommendations made by assurance providers.

4.7.12.2 Managing and Controlling Access to Information Resources

The ISM must be aware of the various standards for managing and controlling access to information resources. It should also be considered that, depending upon the organization's industry sector, specific regulatory bodies may have defined standards that must be addressed.

The following list, while not meant to be complete, shows the more prevalent standards and/or standard-setting bodies:
- *Control Objectives for Information and related Technology* (COBIT)
- ISO/IEC 17799
- BS 7799:1
- Commonly Accepted Security Practices and Recommendations (CASPR)
- Federal Energy Regulatory Commission (FERC)
- National Institutes of Science and Technology NIST
- AS/NZS 4360
- National Fire Protection Association (NFPA), Occupational Safety & Health Administration (OSHA)
- American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS No.70)
- AICPA and Canadian Institute of Chartered Accountants (CICA) SysTrust
- Sarbanes-Oxley Act of 2002
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Gramm Leach Bliley Act of 1999 (GLBA)
- Office of the Comptroller of the Currency (OCC), Circular 235 and Thrift Bulletin 30
- Security statutes, covering areas of computer fraud, abuse and misappropriation of computerized assets, e.g., US Federal Computer Security Act
- Federal Financial Institution Examination Council (FFIEC) guidelines, which replace previously issued Banking Circulars BC-177, BC-226, etc.
- COSO
- CoCo
- Cadbury
- King
- IT Baseline Protection Manual, German Federal Office for Information Security
- Organization for Economic Cooperation and Development (OECD) Security Guidelines
- US Foreign Corrupt Practices Act (FCPA)
- US Vital Records Management Statutes, specifications for the retention and disposition of corporate electronic and hard copy records, e.g., the US Internal Revenue Service (IRS) records retention requirements

4.7.12.3 Internal Vulnerability Reporting Sources

Today, threats to information systems are global. Requirements for rapid time to market and other issues has resulted in a variety of vulnerabilities in both hardware and software. These vulnerabilities are constantly being discovered and reported by a variety of organizations. It is an important part of any effective security program to maintain daily monitoring of relevant entities that publish this information, which includes Computer Emergency Response Team (CERT) at Carnegie Mellon, SANS, most equipment manufacturers and others

Having this knowledge enables the ISM to modify the security program, as necessary, ensuring that information resources are continually protected to meet the business needs of the organization.

4.7.13 Resolution of Noncompliance Issues

Noncompliance issues usually result in risks to the organization, so it is important to develop specific processes to deal with them in an effective and timely manner. Depending on how significant the risk is, various approaches can be taken to address them. If a particular noncompliance event is a serious risk, it is obvious that resolution needs to occur quickly. The security manager will benefit from a method of determining criticality and then having a risk-based response process.

Typically, a timetable is developed to document each noncompliance item and responsibility for addressing it is assigned and recorded. Regular follow-up is key to ensure that the noncompliance issue and other variances are satisfactorily addressed in a timely manner. Noncompliance issues and other variances can be identified through a number of different mechanisms including:
- Normal monitoring
- Audit reports

- Security reviews
- Vulnerability scans
- Due diligence work

4.7.13.1 Risk Reassessment of Events Affecting Security Baselines

ISMs need to monitor and assess events that affect security baselines and thus might affect the organization's security program. Based on this assessment, the ISM must determine if the organization's security plans, test plans and reperformance (revalidation) require modification.

Security baselines may be changed for various reasons including a vendor who identifies that a parameter in their software or hardware must be changed to achieve the desired protection. Others can be outside events that require increased baselines. For instance, if there was a protest or other civil unrest near the organization's facility, the baseline for physical security may need to be increased for a period of time until that threat passes.

4.7.13.2 Information Security Problem Management Practices

In addition to crisis or event management practices, the ISM needs to understand the various aspects of an effective problem management approach. Problem management typically requires a systematic approach to break down the issue, define the problem and design an action program along with assigning those responsible and assigning due dates for resolution. A reporting process should also be implemented for tracking the results and ensuring that the problem is indeed resolved.

As the information systems environment is continually going through changes via updates and additions, it is not unusual for the security controls in place to occasionally develop a problem and not work as intended. It is at this point that the ISM must identify the problem and assign a priority to it.

The ISM should also be familiar with mitigating controls that may have to be employed if the primary security control fails. Rather than allowing the security vulnerability to put the organization at risk, it may be necessary for the ISM to take alternative actions to protect the information resources until the problem is resolved. For example, if a firewall fails, the ISM may elect to disconnect the system from the outside until the firewall problem is resolved. While this would protect the information resources from outside risks, it would likely affect the organization's ability to perform business. Therefore, it is important that specific authority and limits are established by management.

4.7.14 Culture, Behavior and Security Awareness

People present the greatest risk to any organization. To manage security in an organization, it is important for the ISM to consider the culture and behavior of personnel. It is unlikely that security will be adequate if personnel are indifferent, careless or demoralized or if the culture is not supportive of good practices. The challenge must be addressed by promoting the support and commitment of senior management and implementing activities that can effect change of the culture over time to be more conducive to good security practices.

4.7.14.1 Influencing Behavior of Staff to Improve Security

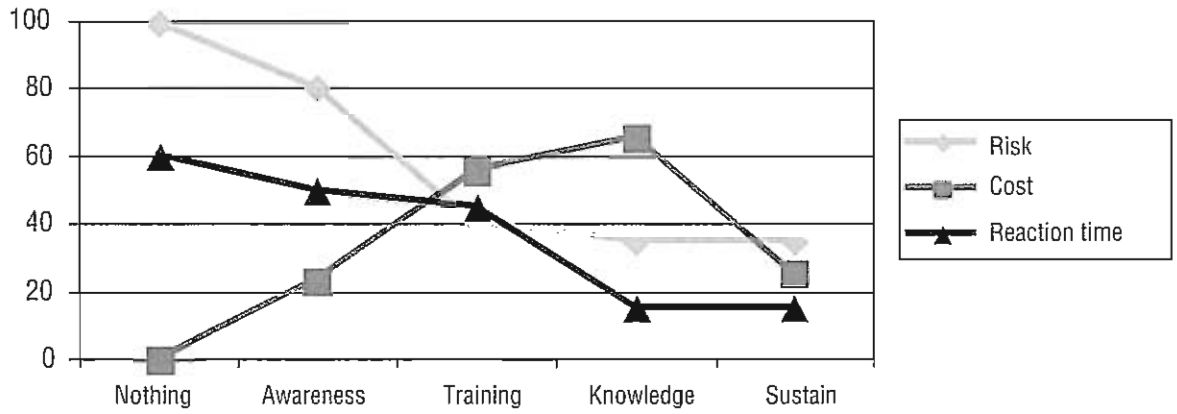
One of the critical success factors in having an effective security program is ensuring adequate information security education and awareness throughout the organization. Security awareness and training has recently been mandated by a number of regulatory bodies and is a requirement in certain industry segments in some parts of the world.

Recent studies conducted by the US Military have also shown that by far, the most cost-effective improvements in overall security have come from user education and training.

Based upon direct experience with the US Military Regional Computer Emergency Response Team (RCERT) in Europe from 1994-2002, personnel was determined to be the weakest link in the security chain. Security technology was purchased and implemented, but evidence indicated that the risk to information remained a personnel problem. Reduction of risk was achieved only after the RCERT initiated an awareness and training program that covered all 90,000 users and the 2000 IT staff personnel.

Figure 4.3 depicts the relationship between risk, cost and the awareness program. As awareness and training of the personnel took place, the risk was reduced as they were taught the value of assets, the risks and appropriate actions to take. Once the personnel became aware of the problems, they were then trained on security issues and procedures. As a result, the reaction time decreased when vulnerabilities occurred in the organizations. As can be seen in **figure 4.3**, the cost of the program increased until the program was stabilized, at which point it decreased.

Figure 4.3—Risk Optimization



Information security education and awareness includes everything from the specialist skills employed by security staff to the general skills applied by everyone in the organization. The organization must be aware of its own culture, the attitude of staff toward information security and its objectives in getting all personnel to behave in a secure manner. Delivery of education and awareness must be an ongoing process and the ISM must carefully plan how this can be achieved in the most effective manner.

4.7.14.2 ISM Facilitative Role as Change Agent, Educator and Consultant

The ISM has many responsibilities and many of them are as a facilitator. As an active facilitator, the ISM gains senior management support and organizational acceptance and compliance for the information security program's policies, standards and procedures.

An important aspect of ensuring compliance with the information security program is the education and awareness of the organization regarding the importance of the program. In addition to the need for information security, all personnel must be trained in their specific information security-related responsibilities.

Awareness should start from the point of joining the organization (e.g., through induction training) and continue regularly. Techniques for delivery will need to vary to prevent them from becoming stale or boring and may also need to be incorporated into other organizational training programs.

Another very important role of the ISM is as an internal consultant to the various departments within the organization. Through a facilitative approach, the ISM should be able to work with the different departments to discuss the information security risks and suggest solutions. These solutions must comply with the security policies and standards and be focused on adequately protecting information resources. Through this consultative role, the ISM also needs to ensure that the organization's change management processes consider information security. By working in this consultative role the ISM can effectively facilitate the enterprise's information security program and stay informed as to the organization's activities that may impact information security.

4.7.14.3 Addressing Cultural Differences

The ISM should be aware that what is viewed as reasonable in one culture may not be acceptable in another. In addition, laws in different countries restrict certain sharing of personal information. The ISM needs to be aware of these complications and work to develop an information security program that meets the individual needs of the organization.

The ISM needs to identify the audience and who will be affected by the information security activities. The ISM should work with the organization's legal and human resources departments to identify conflicts and work toward solutions.

4.7.14.4 Activities to Encourage Understanding

Information security policy statements are often misinterpreted by staff. If the security policies are not complete and concise, it is possible they will be circumvented. For an information security program to be effective and to ensure proper understanding by the entire organization, the ISM must clearly define and communicate it to staff.

4.7.14.5 Information Security Awareness Training and Education

All employees of an organization and, where relevant, third-party users must receive appropriate training and regular updates on the importance of security policies, standards and procedures in the organization. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities, e.g., logon procedures, use of software packages. For new employees, this should occur before access to information or services is granted and be a part of new employee orientation.

The ISM should take a methodical approach to developing and implementing the education and awareness program and needs to consider various aspects including:
- Who is the intended audience (senior management, business managers, IT staff, users)?
- What is the intended message (policies, procedures, recent events)?
- What is the intended result (improved policy compliance, behavioral change, better practices)?
- What communication method will be used [computer-based training (CBT), all-hands meeting, intranet, newsletters, etc.]?
- What is the organizational structure and culture?

A number of different mechanisms available for raising information security awareness include:
- Computer-based security awareness and training programs
- E-mail reminders and security tips
- Written security policies and procedures (and updates)
- Nondisclosure statements signed by the employee
- Use of different media in promulgating security (e.g., company newsletter, web page, videos, posters, logon reminders)
- Visible enforcement of security rules
- Simulated security incidents for improving security procedures
- Rewarding employees who report suspicious events
- Periodic reviews
- Job descriptions
- Performance reviews

While developing information security training and awareness programs, ISMs should include methods of measuring the effectiveness of education and awareness on staff. Feedback gained should be used for continuous improvement.

4.8 CHAPTER 4 GLOSSARY

Acceptable use policy
A policy that establishes an agreement between users and the organization and defines for all parties ranges of use that are approved before gaining access to a network or the Internet

Access control
The set of rules and procedures implemented within hardware and software to provide for the identification of users, the granting and denying of access, the recording of access attempts, and the administrative tools necessary to manage and monitor access activities

Access path
The logical route an end user takes to access computerized information including networks, systems, authentication and authorized systems, applications and application controls

Access rights
Permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy

Accountability
The ability to map a given activity or event to the responsible party to make the individual accountable for his/her actions

Administrative controls
The actions or controls dealing with operational effectiveness, efficiency and adherence to regulations and management policies

Application layers
They refer to the transactions and data relating to each computer-based application system and are therefore specific to each such application.

Application service provider (ASP)
A third-party agent that delivers software licenses to business customers on a shared basis accessible by subscribers over the Internet; also known as managed service provider (MSP)

Audit trail
A series of records either in hard copy or in electronic format that provide a chronological record of user activity and other events that show the details of user and system activity. Audit trails can be used to document when users log in, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred.

Authentication
The verification of the authenticity of a person or system requesting access to a resource to establish their legitimacy before access to the requested resource is granted. During the authentication process, the user enters a name or account number (identification) and password (authentication).

Availability
Ensuring that information systems and data are ready for use when they are needed; often expressed as the percentage of time that a system can be used for productive work

COBIT
Control Objectives for Information and related Technology, the international set of IT control objectives published by the IT Governance Institute

Confidentiality
The protection of sensitive or private information from unauthorized disclosure

COSO
A report titled *Internal Controls—An Integrated Framework* sponsored by the Committee of Sponsoring Organizations of the Treadway Commission in 1992. It provides guidance and a comprehensive framework of internal controls for all organizations.

Criticality analysis
An analysis to evaluate resources or business functions to identify their importance to the organization and the impact if a function cannot be completed or a resource is not available

Data classification
The assignment of a level of sensitivity to data that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the organization.

Data normalization
A process applied to all data in a set that produces a specific statistical property. It is also the process of eliminating duplicate keys within a database and is useful as organizations use databases to evaluate various security data.

Data warehouse
A generic term for a system that stores, retrieves and manages large volumes of data. Data warehouse software often includes sophisticated comparison and hashing techniques for fast searches, as well as advanced filtering.

Defense in-depth
The practice of layering defenses to provide added protection. Defense in-depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an organization's computing and information resources.

Discretionary access control (DAC)
A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Dual control
A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource

Due care
The minimum and customary practice of responsible protection of assets that reflects a community or societal norm

Due diligence
The prudent management and execution of due care

Exposure
The extent to which a vulnerability can result in adverse consequences; the potential loss to an area due to the occurrence of an adverse event

Guidelines
A suggested action or recommendation related to an area of information security policy that is intended to supplement a procedure. The implementation of guidelines is encouraged but not enforced.

Information security governance
The leadership, organizational structures and processes that safeguard information

Information security program
The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis

Integrity
The accuracy, completeness and validity of information in accordance with business values and expectations

Internet service provider (ISP)
A third party that provides individuals and organizations access to the Internet and a variety of other Internet-related services

Intrusion detection
The process of monitoring the events occurring in a computer system or network to detect signs of security problems

ISO/IEC17799
Originally released as part of the British Standard for Information Security in 1999 as the Code of Practice for Information Security Management, which in October 2000 was elevated by the International Organization for Standardization to an international code of practice for information security management. This standard defines information confidentiality, integrity and availability controls in a comprehensive information security management system.

Mandatory access control (MAC)
A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf

Masqueraders
Attackers that penetrate systems by using the identity of legitimate users and their logon credentials

Monitoring policy
Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted

Nonrepudiation
Assurance that a party cannot later deny originating data. It is the provision of proof of the integrity and origin of the data and can be verified by a third party. A digital signature can provide nonrepudiation.

Nonintrusive monitoring
The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities

Open Source Security Testing Methodology
An open and freely available methodology and manual for security testing

Passive response
A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action

Penetration testing
A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers

Ports
An interface point between a CPU and a peripheral device. A port can also be a convention that allows remote services to connect to a host in an orderly manner.

Privacy
Freedom from unauthorized intrusion or disclosure of information about individuals

Procedures
A detailed description of the steps necessary to perform specific operations in conformance with applicable standards; a portion of a security policy that states the general process that will be performed to accomplish a security goal

Security metrics
A standard of measure used to monitor information-security-related activity and evaluate the performance of security-related programs

Sniffing
An attack in which data traversing a network are captured and monitored without authorization. This is similar to the more traditional wire tap but is done without legal authority. Sniffing is commonly used to capture passwords and other interesting and sensitive information that traverses the network.

Social engineering
An attack based on deceiving users or administrators at the target site. Social-engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user in an attempt to gain illicit access to systems. A person who illegally enters computer systems by persuading an authorized person to reveal IDs, passwords and other confidential information.

Split knowledge
A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items; a condition under which two or more entities separately have key components which individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module

Spoofing
Faking the sending address of a network transmission

Standards
Definition of the metrics used to determine the correctness of a thing or process; a set of rules or specifications that, when taken together, define a software or hardware device. A standard is also an acknowledged basis for comparing or measuring something.

Steering committee
A management committee assembled to sponsor and manage various projects such as an information security program

Threat analysis
An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against information assets and information technology. The threat analysis usually also defines the level of threat and the likelihood of that threat to materialize.

4.9 CHAPTER 4 SAMPLE QUESTIONS

CISM exam questions are developed with the intent of measuring and testing practical knowledge in information security management. All questions are multiple choice and are designed for one best answer. Every CISM question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement.

In some instances, a scenario or a description problem may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. Many times a CISM examination question will require the candidate to choose the **MOST** likely or **BEST** answer.

In every case the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked and how to study to gain knowledge of what will be tested will go a long way toward answering them correctly.

The sample questions contained below are designed to depict the type of question format on the CISM examination.

1. The change management procedure **MOST** likely to cause concern to the ISM is when:

   A. fallback processes are tested the weekend immediately prior to when the changes are made.
   B. users are notified via electronic mail of major scheduled system changes.
   C. a manual process is used by operations for comparing program versions.
   D. development managers have final authority for releasing new programs into production.

2. Which of the following would indicate that an automated production scheduling system has inadequate security controls?

   A. Control statements are frequently changed to point to test libraries.
   B. Failure of a process will automatically initiate resetting of parameters.
   C. Developers have read access to both production and test schedules.
   D. Scheduling personnel have the ability to initiate an emergency override.

3. When a trading partner who has access to the corporate internal network refuses to follow corporate security policies, the ISM should initiate which of the following?

   A. Revoke their access.
   B. Provide minimal access.
   C. Send a breech of contract letter.
   D. Contact the partner's external auditors.

4. Which of the following is **MOST** important in writing good information security policies?

   A. Ensure that they are easy to read and understand.
   B. Ensure that they allow for flexible interpretation.
   C. Ensure that they describe technical vulnerability issues.
   D. Ensure that they change whenever operating systems are upgraded.

5. Which of the following would be the **BEST** approach when conducting a security awareness campaign?

A. Provide technical details on exploits.
B. Target system administrators and the help desk.
C. Provide customized messages for different groups.
D. Target senior managers and business process owners.

4.10 CHAPTER 4 ANSWERS TO SAMPLE QUESTIONS

1. **D** Development managers should not have final authority for releasing new programs into production. This would present a conflict of interest. Testing fallback processes the weekend before the change is appropriate, as is notifying users via e-mail that a major change is pending. Also, in some cases, a manual process of comparing versions may be necessary.

2. **A** Frequently having production control statements point to test libraries is a problem, since test libraries are not subject to the same level of security controls. Resetting parameters to their original settings when a process fails is desirable in order to back out any changes. Developers will often require read access to production and test schedules and emergency overrides are usually performed by scheduling personnel.

3. **B** To preserve the business relationship, it would be inappropriate to revoke access or contact the partner's external auditors. Similarly, sending a breech of contract letter would be excessive until other remedies, including discussions with management, have been attempted. To minimize the exposure until the situation can be corrected, access to the corporate internal network should be minimized.

4. **A** Security policies should be easy to read and understand to promote and encourage acceptance. Allowing for flexible interpretation is inadvisable as this would dilute the effectiveness of the policies. Similarly, describing technical vulnerabilities could expose the systems unnecessarily. Policies should be high level; therefore, they should not change every time the operating system is upgraded.

5. **C** Different groups have differing levels of expertise and, accordingly, each should receive a customized message based on their role and level of understanding. Providing technical details on exploits is not advisable since this could teach individuals how to circumvent controls. Also, specific groups should not be singled out for training at the exclusion of others, since all groups have a role to play in strengthening security.

4.11 CHAPTER 4 REFERENCES

American Institute of Certified Public Accountants, SysTrust, *http://www.aicpa.org/assurance/trustservices/index.asp*

Bunker, Eva; "Optimizing an Organization's Security Effectiveness by Using Vulnerability Management to Support the Audit Function," ***Information Systems Control Journal*****, vol. 4, 2003, p. 28-30**

Byrne, Jim; "Large-scale Biometric Management: Centralized, Policy-based Approach to Reducing Organizational Identity Chaos," ***Information Systems Control Journal*****, vol. 6, 2003, p. 41-44**

Caldwell, Matthew; "The Importance of Event Correlation for Effective Security Management," ***Information Systems Control Journal*****, vol. 6, 2002, p. 37-38**

Certified Information Systems Security Professionals, *www.cissp.com* (Search for security awareness and education tips here.)

Chapin, David A.; Steven Akridge; "How Can Security Be Measured?" ***Information Systems Control Journal*****, vol. 2, 2005, p. 43-47**

Chief Security Officer Online, *www.csoonline.com*

Change Management, *www.change-management.org/tools2.htm*

De Beaupré, Adrien; "Know Yourself: Vulnerability Assessments," SANS Institute, 21 June 2001, *www.giac.org/practical/gsec/Adrien_Beaupre_GSEC.pdf*

Driml, Scott; "Enhancing Security With an IT Network Awareness Center," ***Information Systems Control Journal*****, vol. 4, 2003, p. 51-52**

Gallegos, Frederick; Daniel P. Manson; Sandra Allen-Senft; ***Information Technology Control and Audit, 2nd Edition*****, Auerbach, USA, 2004**

Garfinkel, Simson; Gene Spafford; ***Web Security, Privacy and Commerce, 2nd Edition*****, O'Reilly & Associates, USA, 2002**

German Federal Office for Information Security, *IT Baseline Protection Manual*, *www.bsi.bund.de/gshb/english/menue.htm*

Held, Robert; "Security Awareness—Are Your Users 'Clued in' or 'Clueless?'," SANS Institute, May 2001, *www.giac.org/practical/gsec/Robert_Held_GSEC.pdf*

Herzog, Peter; *Open Source Security Testing Methodology*, ISECOM, 30 November 2003, *www.isecom.org/projects/osstmm.shtml*

Information Systems Audit and Control Association, *www.isaca.org*

Information Systems Audit and Control Association, K-NET, *www.isaca.org/knet*

Information Technology Committee, *International Information Technology Guidelines—Managing Security of Information*, International Federation of Accountants (IFAC), January 1998

Insecure, *www.insecure.org*

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

Insecure, Mailing List Archive, *http://lists.insecure.org/#vuln-dev*

International Organization for Standardization (ISO), "Guidelines for the Management of IT Security," ISO/IEC 13335, *www.iso.org*

International System Security Engineering Association (ISSEA), "System Security Engineering Capability Maturity Model," *www.issea.org/sse_cmm/sse_cmm.html*

Internet Security Systems, *https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp*

Internet Storm Center, *http://isc.incidents.org* (Contains reports on Internet incidents)

ISECOM, *www.isecom.org* (Contains information on security assessment tools and assessment methods)

King, Christopher M.; Curtis E. Dalton; Ertem Osmanoglu; *Security Architecture*, McGraw Hill, USA, 2001, chapter 2

Krause, Micki; Harold Tipon*; Handbook of Information Security Management, 5th Edition*, Auerbach Publications, 2003

McClure, Stuart; Joel Sambray; George Kurtz; *Hacking Exposed, 5th Edition*, McGraw Hill, USA, 2005

Microsoft, Security & Privacy web site, *www.microsoft.com/security*

Microsoft, "Microsoft Security Program," Microsoft Security Bulletin, MS99-032, *www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms99-032.asp*

National Institute of Standards and Technology, Vulnerability and Threat Portal, USA, *http://icat.nist.gov/vt_portal.cfm*

Pauls, Nicole; "Security Information Management: Not Just the Next Big Thing," *Information Systems Control Journal*, vol. 5, 2005, *www.isaca.org/jonline*

Payne, Shirley C.; "A Guide to Security Metrics," SANs Insititute, 11 July 2001, *www.sans.org/rr/papers/index.php?id=55*

Ross, Steven J.; "Information Security and the Resilient Enterprise," *Information Systems Control Journal*, vol. 2, 2005, p. 8-9

Security Focus, *www.securityfocus.com*

Software Engineering Institute, CERT Coordination Center, *www.cert.org/nav/index_red.html*

Weber, Ron; *Information Systems Control and Audit*, Prentice Hall, USA, 1999, chapters 4, 5, 6, 7, 8, 10, 12, 17, 21, 22 and 23

White House, National Strategy to Secure Cyberspace Report, USA, *www.whitehouse.gov/pcipb/*

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

Chapter 5:

RESPONSE MANAGEMENT

5.1 DEFINITION

Developing and managing a capability to respond to and recover from disruptive and destructive incidents

5.2 OBJECTIVE

The objective of this job practice area is to enable an organization to continue operations in the event of a disruption to or failure in information processing functions, restore normal services as quickly and efficiently as possible, and detect and effectively respond to security breaches to reduce their impact.

This job practice area represents 13 percent of the CISM examination (approximately 26 questions).

5.3 TASKS

There are seven tasks within this job practice area:
1) Develop and implement processes for detecting, identifying and analyzing security-related events.
2) Develop response and recovery plans, including organizing, training and equipping the teams.
3) Ensure periodic testing of the response and recovery plans where appropriate.
4) Ensure the execution of response and recovery plans as required.
5) Establish procedures for documenting an event as a basis for subsequent action, including forensics when necessary.
6) Manage post-event reviews to identify causes and corrective actions.

5.3.1 KNOWLEDGE STATEMENTS

The information security manager should know:
1) Knowledge of the components of an incident response capability
2) Knowledge of information security emergency management practices (for example, production change control activities, development of computer emergency response team)
3) Knowledge of disaster recovery planning and business recovery processes
4) Knowledge of disaster recovery testing for infrastructure and critical business applications
5) Knowledge of escalation processes for effective security management
6) Knowledge of intrusion detection policies and processes
7) Knowledge of help desk processes for identifying security incidents reported by users and distinguishing them from other issues dealt with by the help desks
8) Knowledge of the notification process in managing security incidents and recovery (for example, automated notice and recovery mechanisms for example in response to virus alerts in a real-time fashion)
9) Knowledge of the requirements for collecting and presenting evidence, rules for evidence, admissibility of evidence, and quality and completeness of evidence
10) Knowledge of postincident reviews and follow-up procedures

5.3.2 Relationship of Tasks and Knowledge Statements

The task statements reflect what the CISM candidate is expected to be able to do within their position as an ISM. The knowledge statements delineate what the CISM candidate is expected to know to perform the tasks.

The task and knowledge statements are approximately mapped in **figure 5.1**. Note that there is often an overlap. Each task statement will generally map to several knowledge statements as shown.

Figure 5.1—Knowledge and Task Statements Mapping

Task Statements	Knowledge Statements
1. Develop and implement processes for detecting, identifying and analyzing security-related events.	1. Knowledge of the components of an incident response capability 2. Knowledge of information security emergency management practices 5. Knowledge of escalation processes for effective security management 6. Knowledge of intrusion detection policies and processes 7. Knowledge of help desk processes for identifying security incidents reported by users and distinguishing them from other issues dealt with by help desks 8. Knowledge of the notification process in managing security incidents and recovery 9. Knowledge of the requirements for collecting and presenting evidence, rules of evidence, admissibility of evidence, and quality and completeness of evidence
2. Develop response and recovery plans including organizing, training and equipping the teams.	1. Knowledge of the components of an incident response capability 2. Knowledge of information security emergency management practices 3. Knowledge of disaster recovery planning and business recovery processes 9. Knowledge of the requirements for collecting and presenting evidence, rules of evidence, admissibility of evidence, and quality and completeness of evidence
3. Ensure periodic testing of the response and recovery plans where appropriate.	3. Knowledge of disaster recovery planning and business recovery processes 4. Knowledge of disaster recovery testing for infrastructure and critical business applications 6 Knowledge of intrusion detection policies and processes
4. Ensure the execution of response and recovery plans as required.	10. Knowledge of postincident reviews and follow-up procedures
5. Manage postevent reviews to identify causes and corrective action.	10. Knowledge of postincident reviews and follow-up procedures

5.4 INTRODUCTION TO RESPONSE MANAGEMENT

5.4.1 Response Management Overview

The purpose of response management is to enable a business to continue operations in the event of a disruption and/or failure to restore normal services as quickly and efficiently as possible, and to detect and respond to actual and possible security breaches to reduce impact. Rigorous planning and commitment of resources are necessary to adequately plan for such an event.

Business continuity planning (BCP) is a process designed to reduce the organization's business risk. Such risks generally arise from an unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organization. Incident response planning (IRP) is very similar to BCP, except that IRP focuses on security-related breaches that threaten the integrity of systems, networks, applications and data as well as confidentiality of critical information and nonrepudiability of electronic transactions. Allocating human/material resources supporting business functions/operations, assuring the continuity of the minimum level of services necessary to support business operations and containing security breaches are major IRP considerations. Business functions include all critical, vital, sensitive and nonsensitive functions. Response priorities differ according to the type of function. On the other hand, business continuity focuses on outages and disruptions regardless of their causes.

Defining requirements expectations is primarily the responsibility of senior management, as members of senior management are entrusted with safeguarding the assets and the public image of the organization they serve. The plan should address all functions and assets required for an organization to remain viable as a business entity. This includes continuity procedures determined necessary to survive and minimize the consequences of business interruption.

A business continuity plan includes the disaster recovery plan (DRP) and the plan for the continuity of operations. Additionally, the DRP is generally the plan followed by IS to recover an IT processing facility or by business units to recover an operational facility. The IS recovery plan must be consistent with and support the overall IT plan of the organization. Overall, response management is equal to the combination of BCP, disaster recovery planning plus continuity of business operations, and incident response, although each part, depending on the complexity of the organization, does not necessarily have to be integrated into one single plan. To have a viable response management planning strategy, however, each must be consistent with the other.

Business continuity/disaster recovery planning is a major component of an organization's overall business continuity/disaster recovery plan. Information systems are strategically important; almost all business processes are dependent on the use of automated information resources to achieve an organization's objectives. Therefore, the ISM should ensure that there are procedures and redundant systems, network devices and facilities to support these key processes in case of a disruption in which the business cannot function without ongoing information processing functions. If separate from the business continuity and disaster recovery plans, the IS plans must be consistent with and support these plans.

To ensure continuous service, a response and recovery plan should be clearly documented and accessible to minimize the effect of disruptions. This plan should be based on the long-range IT plan and should comply with the overall business continuity and security strategies. The process of developing and maintaining an appropriate plan should thus include:
- Preparing business impact analysis of the effect of the loss of critical business processes to the organization
- Identifying and prioritizing the systems and other resources required to support critical business processes in the event of a disruption
- Choosing appropriate strategies for recovering at least sufficient IS facilities to support critical business processes until full facilities are available
- Developing a detailed plan for recovering IS facilities (disaster recovery plan)
- Developing a detailed plan for the critical business functions to continue to operate at an acceptable level (business continuity plan)
- Training staff how to follow the plans
- Testing the plans
- Maintaining the plans as the business changes and systems develop
- Storing the plans so that they can be accessed despite computer and network failures
- Auditing the plans

5.4.2 Importance of Response Management

There is no guarantee that even the best possible controls will prevent disruptive and sometimes even catastrophic incidents from occurring. Adverse events such as security breaches, power outages, fires and natural disasters can bring IT operations to a halt. Response management enables a business to respond effectively when a potential or real incident occurs, continue operations in the event of disruption, and survive any interruption or security breach in information systems.

5.4.3 Outcomes of Response Management

Response management helps keep critical business processes going by minimizing the impact of incidents, such as security breaches, and events, such as natural disasters, that may adversely affect the organization's information resources. Response management efforts are successful if the following outcomes result:
- The appropriate people are notified of what has occurred and what has been done to intervene.
- Incident recovery occurs rapidly and efficiently.
- The impact of the incident is minimal.
- The likelihood of reoccurrence is systematically diminished.
- Both operational and security processes are balanced.
- Legal issues are adequately addressed.

5.4.4 Key Elements

Key elements of response management include those listed in **figure 5.2**.

Figure 5.2—Key Elements of Response Management

Performing a business impact analysis	The beginning point in response management is performing a BIA, a systematic activity designed to assess the impact of disruption, unauthorized access and/or tampering, or total loss of availability of the support of any critical information resource (system, network device, application, and/or data) to an organization
Creating response and recovery plans	Once the business impact has been defined, a response and recovery plan specific to each type of incident needs to be created and put in place. Each plan, which must be based on the BIA, must delineate processes for detecting, identifying and analyzing incidents. Response-related roles and responsibilities need to be specified. Specific objectives for each type of incident that may adversely affect the organization's information resources must be defined.
Preparation	Preparation includes obtaining and testing necessary software, equipment and facilities; training teams and personnel to perform their assigned duties; performing mock scenarios to provide practice and validate procedures; and much more.
Documentation	All facets of a response management effort need to be documented, including specific actions that have been taken in responding to incidents.
Evaluation	All elements of response management should be continuously evaluated; changes should be made as needed. Metrics should be used to measure success in meeting objectives. A follow-up evaluation of each incident should be conducted to produce valuable "lessons learned" that result in improvements in the process of responding to incidents. The response management program should also be regularly audited.

5.5 PERFORMING A BUSINESS IMPACT ANALYSIS

5.5.1 Definition of BIA

It is often said that the first step in a sensible response management process is to consider the potential impact of each type of incident that may occur. The argument is that one cannot properly plan for an undesirable event if there is little idea of the likely impacts of different possible incident scenarios on one's business/organization. The first step in response management, therefore, is to conduct a BIA, a systematic activity designed to assess the impact of disruption, unauthorized access and/or tampering, or total loss of availability of the support of any critical information resource (system, network device, application, and/or data) to an organization. A BIA should:
- Establish the escalation of loss over time
- Identify the minimum resources needed for recovery
- Prioritize the recovery of processes and supporting systems

Another way of viewing a BIA is that it is an exercise designed to identify the resources that are most important to an organization and the impact resulting from disruption, unauthorized access and/or tampering, or availability loss. If conducted properly, a BIA facilitates comprehending the amount of potential loss (and various other unwanted effects) that could occur from certain kinds of events. Potential loss includes not only direct financial loss, but other less-tangible types of loss, such as reputational damage, failure to achieve regulatory compliance, and so on.

Despite the extremely high level of importance that understanding the business impact of incidents on the business process has, many organizations lamentably bypass this step. Another common problem is that organizations too often do not update their BIAs. BIAs need to be updated whenever systems and business functions are added or changed.

A BIA is based to a large degree on risk assessment (both qualitative and quantitative risk assessment). A BIA is *not*, however, the same as a risk assessment. A BIA is a more specialized function that involves identifying the kinds of events related to disruption, unauthorized access and/or tampering, and total loss of availability, and what the impact would be on business processes. Risk assessment, on the other hand, examines all sources of threat and their probability, leading to estimates of the expected cost of each.

5.5.2 Elements of BIAs

The way in which BIAs are conducted typically vary from organization to organization. At the same time, however, BIAs often have the following elements in common in that they:
1. Describe the business mission of each particular business/cost center
2. Identity the functions that characterize each center
3. Identify critical processing cycles (in terms of time intervals) for each such function
4. Estimate the impact of each type of incident on business operations
5. Estimate the amount of time that recovering from each type of incident is likely to take

For example, suppose that the ISM of a public utilities company has conducted a BIA on the supervisory control and data acquisition (SCADA) system at a large electrical power plant. **Figure 5.3** provides a sample BIA analysis sheet.

Figure 5.3—Key Elements of Response Management

Outage Duration	(US $) Cost	Recovery Resources Needed	Priority of Recovery Process
8 hours	$80,000	Electrical technicians	7
16 hours	$160,000	Electrical technicians, applications support	8
24 hours	$250,000	Electrical technicians, applications support	8
36 hours	$1,000,000	Electrical technicians, applications support, computer support	9
48 hours	$2,000,000	Electrical technicians, applications support, computer support, outside consultants	9
72 hours	$4,000,000	Electrical technicians, applications support, computer support, outside consultants	10
96 hours	$8,000,000	Electrical technicians, applications support, computer support, outside consultants	10

5.5.3 Benefits of Conducting BIAs

Conducting BIAs produces several important major benefits, including:
1. (As mentioned previously) increasing the understanding of the amount of potential loss (and various other undesirable effects) that could occur from certain types of incidents
2. Facilitating all response management activities
3. Raising the level of awareness for response management within an organization/business

5.6 DEVELOPING RESPONSE AND RECOVERY PLANS

5.6.1 Organizing, Training and Equipping the Response Staff

No matter how good controls may be, the risk of occurrence of every type of incident cannot be completely eliminated. It is, thus, possible for any significant adverse event to jeopardize any organization's information resources. Accordingly, the ISM should oversee the development of response and recovery plans (generally called business continuity plans) to ensure that they are properly designed and implemented. These plans should, as described previously, be based on the BIA. If a business interruption occurs, resources required to continue the business must be identified and recorded.

Response and recovery strategies should next be identified and validated and then approved by senior management. Once senior management approves these strategies, the ISM should oversee the development of comprehensive response and recovery plans. During this process, response and recovery teams (as discussed more fully shortly) should be identified and team members mobilized. The plans must provide the teams guidance concerning the steps to be taken to recover business processes.

Training the teams is imperative; the ISM should develop event scenarios and test the response and recovery plans to ensure that the team participants are familiar with their tasks and responsibilities. Through this process the teams will also identify the resources they require for response and recovery; the information security manager can equip the teams with needed resources. An added value of training is detecting and modifying ambiguous or not easy-to-manage procedures and recovery resources.

5.6.2 Recovery Planning and Business Recovery Processes

The ISM should understand the processes of recovery from incidents, such as DoS attacks and natural disasters, as well as recovery planning. The reason is that information resources are very much affected by business interruption events, regardless of their cause.

Disaster recovery has traditionally been defined as the recovery of IT systems when disastrous events such as hurricanes and floods have severely disrupted information processing capabilities. Business recovery is defined as the recovery of the critical business processes necessary to achieve the key business processes. Business recovery includes not only disaster recovery, but also a wider range of considerations related to an organization's business processes and resources.

Additionally, not all critical disruptions are classified as disasters, but they are nevertheless of a high-risk nature. For example, disruption in service can be caused by system malfunctions, accidental file deletions, denial-of-service (DoS) attacks, intrusions, worms and viruses. These events may require prompt action to recover operational status. Actions may among other things necessitate restoration of hardware, software and/or data files. Thus, a well-defined, risk-based classification system needs to be in effect to guide business recovery planning efforts.

Each of these planning processes typically includes several main phases, including:
- Risk assessment and business impact assessment
- Response and recovery strategy definition
- Documenting response and recovery plans
- Training covering response and recovery procedures.
- Updating response and recovery plans.
- Testing response and recovery plans
- Auditing response and recovery plans

Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives (as explained shortly) to be determined, which in turn affects the location and cost of offsite recovery facilities and the composition and mission of individual response and recovery teams.

It is important to anticipate the cost of planning. An effective recovery strategy identifies the best way to restore the normal operating condition of a system in case of interruption and/or unauthorized access and/or subversion and provides guidance based on detailed procedures. A wide variety of response and recovery planning techniques and standards that can assist the ISM exist.

Different strategies should thus be developed; all alternatives should be presented to senior management. Senior management should select the most appropriate strategies from the alternatives provided. The selected strategies should be used to further develop the detailed business recovery plan.

The selection of a recovery strategy depends on a number of factors, including:
- Criticality of the business process and the applications that support it
- Cost
- Time required to recover (as explained in more detail shortly)
- Security-related considerations, such as exposure of valuable and/or sensitive information to unauthorized persons
- Reliability

Various strategies for recovering critical information resources exist. The appropriate strategy is the one with a cost for an acceptable recovery time that is also reasonable compared to the impact and likelihood of occurrence, as determined by a BIA. The cost of recovery is the cost of preparing for possible disruptions (i.e., purchasing, maintaining and regularly testing redundant computers; maintaining alternate network routing; blocking the network addresses of machines that are launching attacks against corporate computing resources; etc.) and the cost of putting these into effect in the event of an incident. The latter costs can often be insured against, but the former generally cannot. However, the premiums for disruption-related insurance usually are lower if there is a suitable plan.

As in the case of threats of any nature, a possible strategy might be to:
- **Eliminate or neutralize a threat altogether.** Although removing or neutralizing a threat might superficially seem like the best alternative, doing so is almost without exception not a realistic goal because each threat has so many potential manifestations. An attempt to eliminate the threat of unauthorized external access, for example, could be substantially reduced by the use of well-configured and well-maintained firewalls, the use of intrusion detection systems, and strong authentication. Despite these very effective security controls, there could be other ways that external attackers could gain unauthorized access to internal computing resources. Attackers could, for example, use social engineering methods to discover and then exploit ways to gain external access that are intended for the exclusive use of employees and contractors. Again, removing or neutralizing threats is not a realistic alternative.
- **Minimize the likelihood of a threat's occurrence.** The best alternative is often to minimize the likelihood of a threat's occurrence. This goal can be achieved by implementing the appropriate set of physical, environmental and/or security controls. In the previous example, deploying firewalls, IDSs and strong authentication methods might substantially reduce the risk of a successful attack launched from outside an organization's internal network(s).
- **Minimize the effects of a threat if an incident occurs.** Another viable approach is to minimize a threat's impact if an incident occurs. In the case of DoS attacks and interruptions to computing systems, networks and applications, the first step in connection with this approach should be to assess whether built-in resilience can be implemented. For example, in the case of the failure of a business-critical server, provisions should be in place for having this server's functions roll over to a redundant server should this server fail due to a fire, electrical outage, natural disaster or DoS attack. Despite provisions for this server's functionality, rolling over to another server in the case of an interruption, business continuity plans (and in the event of a disaster, disaster recovery plans) should nevertheless be in place to ensure the restoration of lost or damaged facilities, especially those not covered by resilience strategies.
- **Transfer risk.** A final possible strategy is to transfer risk to another entity that agrees to reimburse an organization for losses incurred if an incident occurs. Most often this takes the form of an organization obtaining insurance against computer-related losses.

Generally, each IT platform that runs an application supporting a critical business function will need a recovery strategy in case a disruption occurs. There are many alternative strategies. The most appropriate alternative in terms of cost to recover and impact cost should be selected according to the relative risk level identified in the BIA. Lengthier and more costly outages, particularly disasters that impair the primary physical facility, are very likely to require offsite backup alternatives. The types of offsite backup hardware facilities available are:

- **Hot sites**—Hot sites are configured fully and ready to operate within several hours. The equipment, network and systems software must be compatible with the primary installation being backed up. The only additional needs are staff, programs, data files and documentation.
- **Warm sites**—Warm sites are complete infrastructures, but partially configured in terms of IT, usually with network connections and selected peripheral equipment, such as disk drives, tape drives and controllers, but without the main computer. Sometimes a warm site is equipped with a less-powerful CPU than the one generally used. The assumption behind the warm site is that a substitute computer can usually be obtained quickly for emergency installation (provided it is a widely used model) and, since the computer is the most expensive unit, such an arrangement is less costly than a hot site. After the installation of the needed components, the site can be ready for service within hours; however, the location and installation of CPUs and other missing units could take several days or weeks.
- **Cold sites**—Cold sites have only the basic environment (electrical wiring, air conditioning, flooring, etc.) to operate an information processing facility. The cold site is ready to receive equipment, but does not offer any components at the site in advance of the need. Activation of the site may take several weeks. Portable centers belong to this category.
- **Mobile sites**—These are specially designed trailers that can be quickly transported to a business location or an alternate site to provide a ready-conditioned information processing facility. These mobile sites can be attached to form larger work areas and can be preconfigured with servers, desktop computers, communications equipment, and even microwave and satellite data links. They are a useful alternative when there are no recovery facilities in the immediate geographic area. They are also useful in case of a widespread disaster and are a cost-effective alternative for duplicate information processing facilities for a multioffice organization.
- **Duplicate information processing facilities**—These are dedicated, self-developed recovery sites that can back up critical applications. They range from a standby hot site to facilities available through a reciprocal agreement with another company. (Note that although in the past reciprocal agreements were common, they are now seldom used.) The assumption is that there are fewer problems in coordinating compatibility and availability in the case of duplicate information processing facility sites. However, larger organizations may experience problems similar to those encountered when reciprocal agreements between unrelated companies are in place. This is particularly true whenever departmental or divisional information processing facilities are managed separately, or when hostile in-house political factions exist. Adhering to several principles will help ensure the viability of this approach:
  - The site chosen should not be subject to the same natural disaster(s) as the original (primary) site. If, for example, the primary site is in a geographical area that is subject to hurricanes, the recovery site should not be subject to this type of natural disaster.
  - Coordination of hardware/software strategies is necessary. A reasonable degree of hardware and software compatibility must exist to serve as a basis for backup.
  - Resource availability must be assured. The workloads of the sites must be monitored to ensure that sufficient availability for emergency backup use exists.
  - There must be agreement concerning the priority of adding applications (workloads) until all the recovery resources are fully utilized.
  - Regular testing is necessary. Even though duplicate sites are under common ownership and even if the sites are under the same management, testing of the backup operation is necessary.

In many respects, the ultimate duplicate site solution is a "mirror site" in which real applications are launched by an automatic scheduler that balances the computers' loads, so that applications can be executed in one or another site. Provided that sufficient reserve capacity exists, applications can be immediately switched between one site and another without any loss in continuity.

In general, the selection of an alternate site, the computing resources and the recovery plans should be determined by the BIA and the particular response and recovery strategy chosen for meeting the business needs.

The response and recovery strategy should be based on the following considerations:
- **Interruption window**—The time the organization can wait from the point-of-failure to the restoration of critical services/applications. After this time, the cumulative losses caused by the interruption are unaffordable.
- **RTOs**—The maximum time to return completely to normal operations, in other words, from the point-of-failure to the resumption of full operations (business and technology). This is generally not a well-defined, well-understood construct; some organizations express it as partial moments, i.e. from point-of failure to technical recovery, or point-of-disaster-declaration to full operations.
- **RPOs**—RPOs refer to the age of the data the organization needs to be able to restore in the event of a disaster.
- **Services Delivery Objectives (SDOs)**—Level of services to be supported during the alternate process mode until the normal situation is restored. This must be directly related to business needs.
- **Maximum Tolerable Outages (MTOs)**—The maximum time the organization can support processing in alternate mode. After this time, different and important problems may arise, especially if the alternate SDOs are lower than usual SDOs, and the amount of information needed to be updated can grow to the point that it is unmanageable.

To prepare a suitable recovery strategy, the ISM must balance all of these parameters, the different types of recovery sites and their costs.

The complexity and cost of the response and recovery plans as well as the type and cost of the recovery site are proportionally inverse to the previously cited time objectives. An interruption window of two hours, for instance, dictates a hot or mirrored solution, something that is generally very expensive, but the corresponding recovery plan is likely to be simple and cheap. In contrast, an interruption window of a week permits the use of a cold site (very inexpensive), but the associated recovery plan is likely to be complex and very expensive.

Reciprocal agreements between two or more organizations with similar equipment or applications must be made. Under the typical agreement, participants promise to provide computing time and network operations to each other when an emergency arises.

Although the principles concerning recovery strategies are intuitive, they seldom work as planned in real-world settings. IT resources are generally used in a manner that approaches their maximum capacity; organizations do not generally have sufficient reserve resources to satisfy even fairly small requirements related to CPU, network bandwidth or storage capacity. In addition, having the right number of external people near or in a building is anything but reality. Extra expenses, integrating external personnel into operations and additional threats to physical security are some of the difficult and immediate problems inherent in this type of solution. Additionally, creating a contract that provides this type of situation is difficult, and the cost of dealing with changes over time is likely to be significant. It is extremely important that contractual provisions for the use of third-party sites should cover important issues such as configuration of third-party hardware and software, speed of availability, reliability, duration of usage, nature of inter-site communications and period of usage.

There are several alternatives available for securing backup hardware and physical facilities, including:
- **A vendor or third party**—Hardware vendors are usually the best source for replacement equipment. However, this may often involve a waiting period that is not acceptable for critical operations. It is unlikely that any vendor will guarantee a specific reaction to a crisis. Vendor arrangements are utilized best when an organization plans to move from a hot site to a warm or cold site, so advance planning is critical. Another source of equipment replacement is the used hardware market. This market can supply critical components or entire systems on relatively short notice, often at a substantially reduced cost. Establishing relationships with dealers well in advance of any actual emergency is critical.
- **Off-the-shelf**—Such components are readily available from the inventory of suppliers on short notice and with minimum need for special arrangements. To make use of this approach, several strategies must be utilized, including:
  - Avoiding the use of unusual and hard-to-get equipment
  - Regularly updating equipment to keep current
  - Maintaining software compatibility to permit the operation of newer equipment
  - Ensuring that the recovery plans include instructions concerning how such equipment is to be paid for. This could be by a credit agreement with suppliers or by the provision of an emergency credit card with a sufficiently high credit limit.

As data and software are required for these strategies, special arrangements need to be considered for their backup to removable media and their safe, secure storage offsite.

Additionally, part of the recovery of IT facilities will involve telecommunications, for which the strategies that are usually considered include network disaster prevention, which includes:
- Alternative routing
- Diverse routing
- Long-haul network diversity
- Protection of local resources
- Voice recovery
- Availability of appropriate circuits and adequate bandwidth
- Availability of out-of-band communications in case of failure of primary communications methods

Once a strategy for the recovery of sufficient IT facilities to support critical business processes has been developed, it is critical that the strategies work for the entire period of recovery until all facilities are restored. They may include:
- Doing nothing until recovery facilities are ready
- Using manual procedures
- Focusing on the most important customers, suppliers, products, systems, etc., with the resources that are still available
- Using PC-based systems to capture data for later processing or perform simple local processing

Based on the response and recovery strategy selected by management, a detailed response and recovery plan should be developed. It should address all issues involved in recovering from a disaster. Various factors should be considered while developing the plan, including:
- Preincident readiness
- Evacuation procedures
- How to declare a disaster
- Identifying the business processes and IT resources that should be recovered
- Identifying the responsibilities in the plan
- Identifying the persons responsible for each function in the plan
- Identifying contact information
- The step-by-step explanation of the recovery options
- Identifying the various resources required for recovery and continued operations

The response and recovery plan should be documented and written in simple language that is understandable to all. It is also common to identify teams of personnel who are responsible for specific tasks in case of disasters. Teams that should be formed and their responsibilities are explained below. Copies of the plan should be maintained offsite. Access to the plan and their documents must be on a need-to-know basis.

The plan should identify teams and define their assigned responsibilities in the event of an incident. To implement the strategies that have been developed for business recovery, key decision-making, technical and end-user personnel to lead teams responsible for critical functions or tasks defined in the plan need to be designated and trained. Depending on the size of the business operation, these teams may in some cases consist of only a single person. The involvement of these teams depends on the level of the disruption of service and the types of assets lost, compromised, damaged or endangered. It is a good idea to develop a matrix that indicates the correlation between the teams' functionality to facilitate estimating the magnitude of the effort and activating the appropriate combination of teams. Examples of the kinds of teams usually needed include the:
- The emergency action team (designated fire wardens and "bucket crews" whose function is to deal with fires or other emergency response scenarios)
- Damage assessment team
- Emergency management team (responsible for coordinating the activities of all other recovery teams and handling key decision making)
- Relocation team (responsible for coordinating the process of moving from the hot site to a new location or to the restored original location)

- Security team (often called a computer security incident response team) responsible for monitoring the security of systems and communication links, containing any ongoing security threats, resolving any security issues that impede the expeditious recovery of the system(s), and assuring the proper installation and functioning of every security software package.

The following should be agreed upon in the planning, implementation and evaluation phases of the response and recovery plan:
- Goals/requirements/products for each phase
- Alternate facilities in which tasks and operations can be performed
- Critical information resources to deploy (e.g., data and systems)
- Persons responsible for completion
- Available resources (including human) to aid in deployment
- Scheduling of activities with established priorities

Most business continuity plans are created as procedures that accommodate system, user and network recovery strategies. Copies of the plan should be kept offsite, at the recovery facility, at the media storage facility, and possibly at the homes of key decision-making personnel for a variety of reasons, including the possibility that onsite copies could be destroyed in the event of a fire, flood or other similar event. Components of this plan include key decision-making personnel, a backup of required supplies, the organization, and the assignment of responsibilities, telecommunication networks and insurance provisions.

The plan should also cover notification of key decision-making IS and end-user personnel required to initiate and carry out response efforts. A telephone directory of people to notify in the event of an incident is a necessary component of this notification process. This directory should contain the following information:
- A prioritized list of contacts, i.e., who gets called first on a phone tree
- Primary and emergency telephone numbers and addresses for each critical contact person. Key team leaders should be responsible for contacting the members of their team.
- Phone numbers and addresses for representatives of equipment and software vendors
- Phone numbers of contacts within companies that have been designated to provide supplies and equipment or services
- Phone numbers of contact persons at recovery facilities, including hot site representatives or predefined network communications rerouting services
- Phone numbers of contact persons at offsite media storage facilities and the contact persons within the company who are authorized to retrieve media from the offsite facility
- Phone numbers of insurance company agents
- Phone numbers of contacts at human relations and/or contract personnel services
- Phone numbers of law enforcement contacts in case of a very serious security-related incident. Please note that the decision to bring in law enforcement during such an incident rests solely with senior management. It is not the role of an ISM to reach directly out to external organizations, except perhaps in the context of a cross-organizational response team that includes members of an organization's legal and, possibly, media relations functions. The ISM is instead expected to provide information security expertise as well as evidence when called on to do so during organization-endorsed communication with external entities, such as clients, law enforcement and media. The ISM should also help to identify and escalate law-enforcement and legal issues; an appropriate escalation process is thus imperative.

The plan should have provisions for all supplies necessary for continuing normal business activities during the recovery effort. This includes detailed, up-to-date hard copy procedures that can be followed easily by staff and contract personnel who are unfamiliar with the standard and recovery operations. Also, a supply of special forms, such as check stock, invoice forms and order forms, should be secured at an offsite location.

If the data entry function is dependent on certain hardware devices and/or software programs, these programs and equipment, including specialized EDI equipment and programs, should be provided at the hot site.

The plan should contain the organization's telecommunication networks. Because telecommunication networks are essential to business processes in large and small organizations, the procedures to ensure continuous telecommunication capabilities should be given a high priority. Telecommunication networks are susceptible to the same natural disasters as data centers, but also are vulnerable to several types of disastrous events unique to telecommunications. These include central switching office disasters, cable cuts, communication software glitches and errors, security breaches from hacking (phone hackers are known as "phreakers") and a host of other human mishaps. It is the responsibility of the organization and not the local exchange carriers to ensure constant communication capabilities. The local exchange carrier is not responsible for providing backup services, although many carriers back up main components within their systems. The organization should make provisions for backing up its own telecommunication facilities.

To maintain critical business processes, the information processing facility's business continuity plan should provide for adequate telecommunications capabilities. Telecommunications capabilities to consider include telephone voice circuits, WANs (connections to distributed data centers), LANs and third-party electronic data interchange providers. Critical capacity requirements should be identified for the various thresholds of outage, such as two hours, eight hours or 24 hours, for each telecommunications capability. Uninterruptable power supplies (UPSs) should be sufficient to provide backup for telecommunications equipment, as well as computer equipment.

Methods for providing continuity of network services include:

- **Redundancy**—Achieving redundancy involves a variety of solutions, including:
  - Providing extra capacity with a plan to use the surplus capacity should the normal primary transmission capability not be available. In the case of a LAN, a second cable could be installed through an alternate route for use in the event that the primary cable is damaged.
  - Providing multiple paths between routers
  - Using special dynamic routing protocols, such as the Open Shortest Path First (OSPF) and External Gateway Routing Protocol (EGRP)
  - Providing for failover devices to avoid single point of failures in routers, switches, firewalls, etc.
  - Saving configuration files for recovery of network devices, such as routers and switches, in the event that they fail
- **Alternative routing**—Alternative routing means routing information via an alternate medium, such as copper cable or fiber optics. This involves use of different networks, circuits or end points, if the normal network is unavailable. Most local carriers are deploying counter-rotating fiber-optic rings. These rings have fiber-optic cables that transmit information in two different directions and in separate cable sheaths for increased protection. Currently, these rings connect through one central switching office. However, future expansion of the rings may incorporate a second central office in the circuit. Some carriers are offering alternate routes to different points of presence or alternate central offices. Other examples include dial-up circuits as an alternative to dedicated circuits, a cellular phone and microwave communications as alternatives to land circuits, and couriers as an alternative to electronic transmissions.
- **Diverse routing**—The method of routing traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. However, acquiring this type of access is time-consuming and costly. Most carriers provide facilities for alternate and diverse routing, although most services are transmitted over terrestrial media. These cable facilities are usually located in the ground or the basement of buildings that house computer equipment. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share room with mechanical and electrical systems that can impose great risks due to human error and disastrous events.
- **Long-haul network diversity**—Many recovery facilities' vendors provide diverse long-distance network availability, utilizing T1 circuits among the major long-distance carriers. This ensures long-distance access if any single carrier experiences a network failure. Several of the major carriers have now installed automatic rerouting software and redundant lines that provide instantaneous recovery if a break in their lines occurs. The ISM should confirm that the recovery facility has these vital telecommunications capabilities.
- **Last-mile circuit protection**—Many recovery facilities provide a redundant combination of local carrier T1s, microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also utilized.

- **Voice recovery**—With many service, financial and retail industries dependent on voice communication, redundant cabling and alternative routing should be provided for voice communication lines as well as data communication lines.

The loss or disruption of servers managing sensitive and critical business processes could have catastrophic effects on an organization. Plans should include operational failover methods to prevent servers from going offline for an extended period of time. Server recovery should also be included in the disaster recovery plan. Some of the techniques for providing failover or fault-tolerant capabilities include UPSs and the use of failover systems to prevent power failures of varying levels.

Redundant Array of Inexpensive Disks (RAID) provides performance improvements and fault-tolerant capabilities via hardware or software solutions, breaking up data and writing them to a series of multiple disks to improve performance and/or save large files simultaneously. These systems provide the potential for cost-effective continuous data availability onsite or offsite.

Fault-tolerant servers provide for fail-safe redundancy through mirrored images of the primary server. Using this approach also may entail distributed processing of a server load, a concept referred to as "load balancing" or "clustering," where all servers take part in processing. In this arrangement, there is an intelligent "cluster" unit that provides for load balancing for improved performance. This type of server architecture is transparent to users. The only thing that may be noticeable to a user is performance degradation if a server fails.

The plan should also contain key information concerning the organization's insurance. The information systems processing insurance policy is usually a multiperil policy designed to provide various types of IT coverage. It should be constructed modularly, so it can be adapted to the insured's particular IT environment.

Specific types of coverage that are available include:

- **IT equipment and facilities**—This type provides coverage of physical damage to the information processing facility and owned equipment. An organization should also insure leased equipment if it is obtained when the lessee is responsible for hazard coverage. The ISM should review these policies very carefully; many policies are worded such that insurers are obligated to replace nonrestorable equipment with "like kind and quality," not necessarily with new equipment by the same vendor as the damaged equipment.
- **Media (software) reconstruction**—This covers damage to computer-related media that are the property of the insured and for which the insured may be liable. Insurance is available for on-premises, off-premises or in-transit disasters and covers the actual reproduction cost of the property. Considerations in determining the amount of coverage needed are programming costs to reproduce the media damaged, backup expenses and physical replacement of media devices, such as tapes, cartridges and disks.
- **Extra expense**—This is designed to cover the extra costs of continuing operations following damage or destruction at the information processing facility. The amount of extra-expense insurance needed is based on the availability and cost of backup facilities and operations. Extra expense can also cover the loss of net profits caused by computer media damage. This provides reimbursement for monetary losses resulting from suspension of operations due to the physical loss of equipment or media, such as in a situation in which the information processing facilities were on the sixth floor and the first five floors were burned out. In this case, operations would be interrupted even though the information processing facility remained unaffected.
- **Business interruption**—This covers the loss of profit due to the disruption of the activity of the company caused by any covered IT malfunction or security-related event in which an attacker or malicious code causes loss of availability of computing resources
- **Valuable papers and records**—This covers the actual cash value of papers and records (not defined as media) on the insured's premises against unauthorized disclosure, direct physical loss or damage
- **Errors and omissions**—This provides legal liability protection in the event that the professional practitioner commits an act, error or omission that results in financial loss to a client. This insurance originally was designed for service bureaus, but it is now available from several insurance companies for protecting against actions of systems analysts, software designers, programmers, consultants and other IS personnel.
- **Fidelity coverage**—This usually takes the form of banker's blanket bonds, excess fidelity insurance and commercial blanket bonds, and covers loss from dishonest or fraudulent acts by employees. This type of coverage is prevalent in financial institutions operating their own information processing facility.

- **Media transportation**—This provides coverage for potential loss or damage to media in transit to off-premises information processing facilities. Transit coverage wording in the policy usually specifies that all documents must be filmed or otherwise copied. When the policy does not specifically require that data be filmed prior to being transported and the work is not filmed, management should obtain from the insurance carrier a letter that specifically describes the carrier's position and coverage in the event data are destroyed.

Since organizations are dynamic and subject to constant changes, the response and recovery process must assure that plans are continuously updated and adapted to ensure that they reflect the current objectives and conditions of the organization. It is also important to gain senior management approval for the various aspects of this process; a response and recovery strategy is an ongoing process that consumes resources to achieve and sustain an acceptable level of recovery capability.

The ISM also needs to ensure that information security is incorporated in any response and recovery strategy that is implemented to ensure that the information resources are protected even in the event of a business interruption. In some cases, systems and/or network devices may have to be temporarily disconnected from the network or even shut down to prevent a security-related incident from spreading out of control.

5.6.3 Understand Response and Recovery Practices

The ISM should understand the various activities involved in a response and recovery program. The ISM should meet with emergency management officials (federal, state/provincial, municipal/local) to understand what governmental capabilities exist. These officials are likely to have information concerning the nature of risks to which the location or area is susceptible. Most countries and governments have civil defense and/or emergency management agencies that are tasked with advising and assisting the population in dealing with a wide range of natural and human-initiated threats.

Emergency management activities typically focus around the activities immediately after an incident. This can include activities during or after after a physical disaster, fire, electrical failure or security-related incident. These events may require prompt action to recover operational status. Actions may necessitate restoration of hardware, software and/or data files. Emergency management activities typically also include measures to assure the safety of personnel, such as evacuation plans and creation of a command center from which emergency procedures can be executed. It also is important that information about an incident only be communicated on a need-to-know basis.

5.7 INCIDENT RESPONSE PROCESSES

5.7.1 Detecting, Identifying and Analyzing Security-related Events

So far this chapter has focused on planning for recovery from interruptions and outages, regardless of their origins (fires, electrical outages, hurricanes, DoS attacks, and so on). Although BCP often addresses security-related risks, BCP does not in and of itself normally deal with the full range of security-related threats and incidents. BCP instead normally focuses on events that can cause disruptions and outages, regardless of their origin. Furthermore, most security-related incidents that occur are not disasters *per se*. Based on the needs of the organization as defined in the risk assessment, the ISM should thus also engage in IRP designed to implement processes for detecting, identifying, analyzing and reacting to security-related events that may also adversely affect the organization's information resources but that do not necessarily directly affect continuity of computing operations. Another way of viewing this issue is that incident response efforts are more geared toward limiting the effects of confidentiality breaches, loss of integrity, loss of availability of systems and information, and bogus repudiation of electronic transactions. Examples of events likely to be covered in IRP but not in BCP include unauthorized access to files that contain business critical information or accounts on systems and false repudiation of electronic transactions. At the same time, however, the great degree of commonality that BCP and IRP have in terms of strategies and planning dictates that, whenever feasible, the two should be integrated to the maximum extent possible or, in many cases, combined into a single process.

The ISM should access and employ a number of different mechanisms to **detect** security-related events, such as deploying and examining the output of intrusion detection systems, enabling and analyzing the output of system auditing, monitoring changes in files and directories, looking for the presence of suspicious executables, and monitoring incident reporting websites. Various vendor services that provide notifications of security-related events within organizations also are available. In addition, the ISM can implement monitoring and detection services, such as in-house or managed intrusion detection services, to monitor attempts to access the organization's systems and information resources. Furthermore, the ISM should implement a process in which detection-related activities take place on a regular basis, helping ensure early detection, analysis and correction of security incidents.

The ISM should assemble the information gathered through the detection process to **identify** security-related events. This identification process can take place using a criterion defined by the ISM. By categorizing and prioritizing security events, ISMs or designees can take quick and effective action with respect to important security events, so they will not be lost among the noise of other security events.

Through the **analysis** of the security events, the ISM can now assess their impact upon the organization's information resources and modify the security program as necessary. Through triggering the correct response(s) (e.g., shutting a compromised system down, disinfecting a worm-infected system and updating its anti-virus software, and so on) in each incident, the ISM can contain the amount of loss that occurs. Please note that in the case of severe incidents (e.g., when customer information has been stolen), the correct response is often to escalate the response process. Personnel and/or consultants with special expertise related to the particular incident that has occurred may have to be brought in to handle some part(s) of the incident.

5.7.2 Components of an Incident Response Capability

The ISM should understand the components of an effective incident response capability. When defined and managed properly, this capability facilitates reaction to incidents. Additionally, this capability can also be used proactively, because by dealing with the incident in a timely and effective manner and assessing the results, recommended changes may be made to improve the organization's security program.

The approach to incident response may vary depending on the situation, but the goals are constant. These goals can include:
- Containing the effects of the incident so that damage and loss does not escalate out of control
- Notifying the appropriate people for the purpose of recovery or to provide needed information
- Recovering quickly and efficiently from security incidents
- Minimizing the impact of the security incident
- Responding systematically and decreasing the likelihood of reoccurrence
- Balancing operational and security processes
- Dealing with legal and law enforcement-related issues

The ISM also needs to define what constitutes a security-related incident. Typically, security incidents include:
- Malicious code attacks
- Unauthorized access to IT/IS resources
- Unauthorized utilization of services
- Unauthorized changes in systems, network devices, or information
- Denial of service
- Misuse
- Surveillance and espionage
- Hoaxes/social engineering

Please note, however, that many incidents that initially appear to be security-related turn out to be the result of human error instead. Over the years in fact studies have shown that organizations experience nearly double the number of incidents due to human error than to security breaches.

5.8 TESTING RESPONSE AND RECOVERY PLANS

5.8.1 Periodic Testing of the Response and Recovery Plans

The ISM helped by the recovery team's organization should implement periodic testing of response and recovery plans. Testing should include:
- Developing test objectives
- Executing the test
- Evaluating the test
- Developing recommendations to improve the effectiveness of testing process as well as response and recovery plans
- Implementing a follow-up process to ensure that the recommendations are implemented

Response and recovery plans that have not been tested leave an organization with an unacceptable likelihood that plans may not work, even though care usually is taken in developing and documenting these plans. Because testing plans cost time and resources, an organization should carefully plan tests and develop test objectives to be methodical and help ensure that measurable benefits can be achieved.

Once test objectives have been defined, the ISM should ensure that an independent third party is present to monitor and evaluate the test. Internal or external audit or other assurance personnel can often assume this role. A result of the evaluation step should be a list of recommendations that an organization should complete to improve its response and recovery plans. It is extremely unlikely that no recommendations would result and that everything would work as planned. If everything were to work perfectly, the ISM should construct a more robust test with more challenging test objectives.

The ISM should also implement a tracking process to ensure that any recommendations resulting from testing are implemented in a timely fashion. Personnel should be tasked with making any necessary changes.

5.8.2 Testing for Infrastructure and Critical Business Applications

The ISM needs to understand that testing recovery and response plans needs to include infrastructure and critical applications. With today's organizations heavily reliant on information technology, the ISM is not only tasked with securing these systems during normal operations, but also during disaster events.

Based on the risk assessment and business impact information, the ISM should identify critical applications that the organization requires and the infrastructure needed to support them. To ensure that these will be recovered in a timely fashion, the ISM needs to perform appropriate recovery tests.

The ISM generally performs tests that will progressively challenge the recovery plans. Examples include:
- Table-top walk-through of the plans
- Table-top walk-through with mock disaster scenarios
- Testing the infrastructure and communication components of the recovery plan
- Testing the infrastructure and recovery of the critical applications
- Testing the infrastructure, critical applications and involvement of the end users
- Surprise tests

Most recovery and response tests fall short of a full-scale test of all operational portions of the corporation. This should not preclude performing full or partial testing, because one of the purposes of the business continuity test is to determine how well the plan works or the portions of the plan that need improvement.

The test should be scheduled during a time that will minimize disruptions to normal operations. Weekends are generally a good time to conduct tests. It is important that the key recovery team members are involved in the test process and are also allotted the necessary time to devote their full effort. The test should address all critical components and simulate actual primetime processing conditions, even if it is conducted during off hours.

The test should strive to, at a minimum, accomplish the following tasks:
- Verify the completeness and precision of the response and recovery plan.
- Evaluate the performance of the personnel involved in the exercise.
- Appraise the demonstrated level training and awareness of individuals who are not part of the recovery/response team.
- Evaluate the coordination among the team members and external vendors and suppliers.
- Measure the ability and capacity of the backup site to perform prescribed processing.
- Assess the vital records retrieval capability.
- Evaluate the state and quantity of equipment and supplies that have been relocated to the recovery site.
- Measure the overall performance of operational and information systems processing activities related to maintaining the business entity.

To perform testing, each of the following test phases should be completed:
- **Pretest**—The pretest consists of the set of actions necessary to set the stage for the actual test. This ranges from placing tables in the proper operations recovery area to transporting and installing backup telephone equipment. These activities are outside the realm of those that would take place in the case of a real emergency, in which there is generally no forewarning of the event and thus no time to take preparatory actions.
- **Test**—This is the real action of the business continuity test. Actual operational activities are executed to test the specific objectives of the plan. Data entry, telephone calls, information systems processing, handling orders, and movement of personnel, equipment and suppliers should take place. Evaluators should review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.
- **Post-test**—The post-test is the cleanup of group activities. This phase comprises assignments such as returning all resources to their proper place, disconnecting equipment, returning personnel to their normal locations and deleting all company data from third-party systems. The post-test cleanup also includes formally evaluating the plan and implementing indicated improvements.

In addition, the following types of tests may be performed:
- **Paper tests**—Paper tests are an on-paper walk-through of the plan involving major players in the plan's execution who reason out what might happen in a particular type of service disruption. They may walk through the entire plan or just a portion. The paper test usually precedes preparedness tests.
- **Preparedness tests**—Preparedness tests are usually localized versions of a full test, wherein actual resources are expended in the simulation of a system crash. These tests are performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about how good the plan is. They also provide a means to improve the plan in increments.
- **Full operational tests**—These are one step away from an actual service disruption. An organization should have tested the plan well on paper and locally before endeavoring to completely shut down operations. For purposes of the business continuity plan testing, the full operational testing scenario is the disaster.

During every phase of the test, detailed documentation of observations, problems and resolutions should be maintained. Each team should have a diary with specific steps and information recorded. This documentation serves as important historical information that can facilitate actual recovery during a real disaster. Also, the documentation aids in performing detailed analysis of the strengths and weaknesses of the plan.

Just as in nearly everything else in information security, metrics should be developed and used in measuring the success of the plan and testing against the stated objectives. Results must thus be recorded and evaluated quantitatively, as opposed to an evaluation based only on verbal descriptions. The resulting metrics should be used not only to measure the effectiveness of the plan, but more importantly also to improve it. Although specific measurements vary depending on the test and the organization, the following general types of metrics usually apply:
- **Time**—Elapsed time for completion of prescribed tasks, delivery of equipment, assembly of personnel and arrival at a predetermined site. This is essential to refine the response time estimated for every task in the escalation process.
- **Amount**—Amount of work performed at the backup site by clerical personnel and the amount of information systems processing operations
- **Percentage and/or number**—The number of vital records successfully carried to the backup site versus the required number, and the number of supplies and equipment requested versus actually received. Also, the number of critical systems successfully recovered can be measured with the number of transactions processed.

- **Accuracy**—Accuracy of the data entry at the recovery site versus normal accuracy (as a percentage). Also, the accuracy of actual processing cycles can be determined by comparing output results with those for the same period processed under normal conditions.

This testing process enables the ISM to achieve initial successes and modify the plan based on information gained from the initial tests. This is important; performing a robust test costs resources and requires coordination between various departments. A minor error or mishap (e.g., a missing set of backup media) could make completing the full test impossible.

In case normal business operations are destroyed or inaccessible, the ISM needs to have alternative operating strategies based on the response and recovery strategy. The ISM needs to test these alternate capabilities and should also report the response and recovery capability of the organization to senior management.

5.9 EXECUTING RESPONSE AND RECOVERY PLANS

5.9.1 Ensuring the Execution as Required

To ensure the response and recovery plans are executed as required, the plans will need a facilitator or director to direct the tasks within the plans, oversee their execution, liaise with senior management and make decisions as necessary. The ISM may or may not be the appropriate person to act as the recovery plan director or coordinator, but should assure the role is assigned to someone who can perform this important function.

Defining appropriate response and recovery strategies and alternatives is important in the overall process of executing the response and recovery plans. Developing appropriate recovery strategies and alternatives and implementing them will help ensure that an organization can recover its key business functions in the event of a disruption and that it responds appropriately to a security-related incident.

Testing the plans also helps ensure that plans can be executed as required. By testing the plans in a scenario designed to mimic real-life conditions as much as possible, personnel become more familiar with the tasks and their responsibilities, as defined within the plan. This familiarity will help ensure that the plan is executed as required during an actual incident.

The ISM should also appoint an independent observer to record progress and document any exceptions that occur during the actual execution of the plan. Through a postevent review, the ISM and key recovery personnel can then review the observations and make adjustments to the plan accordingly.

Finally, since organizations constantly evolve and change, the response and recovery plans also need to change. The ISM must establish a process in which recovery plans are updated as changes occur within an organization. Assessing the response and recovery plan requirements during the change management process within an organization is an essential part of effective response management.

Plans and strategies for response and recovery should be reviewed and updated according to a schedule to reflect continuing recognition of changing requirements. The following factors as well as others may impact requirements and the need for the plan to be updated:

- A strategy that is appropriate at one point in time may not be adequate as the needs of an organization change.
- New applications may be developed or acquired.
- Changes in business strategy may alter the significance of critical applications or result in additional applications being deemed as critical.
- Changes in the software or hardware environment may make current provisions obsolete or inappropriate.

The responsibility for maintaining the business continuity and disaster recovery plan often falls on the business continuity plan coordinator. The ISM is often responsible for maintaining the incident response plan. Specific plan maintenance responsibilities include:

- Developing a schedule for periodic review and maintenance of the plan and advising all personnel of their roles and the deadline for receiving revisions and comments
- Calling for revisions out of schedule when significant changes have occurred
- Reviewing revisions and comments and updating the plan within a reasonable period (e.g., 30 days) after the review date
- Arranging and coordinating scheduled and unscheduled tests of the plan to evaluate its adequacy
- Participating in scheduled plan tests, which should be performed at least once per year on specific dates. For scheduled and unscheduled tests, the coordinator should write evaluations and integrate changes to resolve unsuccessful test results into the response plan within a reasonable period (30 days).
- Developing a schedule for training personnel in emergency and recovery procedures, as set forth in the plan. Training dates should be scheduled within a reasonable period (e.g., 30 days) after each plan revision and scheduled plan test.
- Maintaining records of plan maintenance activities—Testing, training and reviews
- Updating, at least quarterly, the notification directory to include all personnel changes, including phone numbers and responsibilities or status within the company

5.9.2 Escalation Process for Effective Security Management

The ISM should implement an escalation process for effective security management. The escalation process establishes the events to be managed (i.e., in the event of a telecommunications shutdown). Events that appear routine can be related to a security compromise (e.g., data corruption might not be due to an application problem, but rather to a virus or worm infection). As part of the emergency management and incident management policies and procedures, a detailed description of the escalation process should be documented.

For every event, a list of actions should be described in the logic sequence to be performed. Every action has associated a responsible person and an estimated time for execution. When the action is finished successfully, the process should continue in the section dedicated to "end of emergency." If the action cannot be executed or the estimated time is reached, the process should continue in the next action, usually performed by other person. Each unsuccessful action wastes time. If the accumulated elapsed time reaches a predetermined limit, the emergency status may change to an alert condition (low, medium, high). An alert situation prompts notifying individuals and organizations with executive responsibilities. Alert notification may include senior management, response and recovery teams, human resources, insurance companies, backup facilities, vendors and customers.

The process should continue until the emergency is resolved or the last alert has occurred. At this point, the emergency management team must convene a meeting to evaluate the damages and mitigation alternatives, determine whether to declare a disaster, and/or launch the response and recovery plan and the appropriate strategy. A disaster declaration may be made to authorities, the public, shareholders and stakeholders. The ISM should develop a communication plan in consultation with public relations, legal counsel and other appropriate senior management.

After the escalation process, numerous tasks such as notifying personnel, activating backup facilities, containing security threats to information resources, making transportation arrangements and carrying them out, retrieving and unloading data, testing, etc., must be executed. The total elapsed time must be in accordance with the RTO.

The escalation process should include prioritizing event information and the decision process for determining when to alert various groups, including senior management, the public, shareholders and stakeholders, legal counsel, human resources, vendors, and customers. The ISM should develop processes through consultation with public relations, legal counsel and other appropriate senior management. Assessing the situation is typically the first step in such a process.

An escalation process should also include vendors and utility services. An escalation process that involves these entities should be approved, so that appropriate notification/information sharing takes place during and after an event.

Many organizations define the level of events and define the escalation procedures differently for each level. These levels can be based on the severity of the event as well as the number of organizations that may be affected by the event and their specific need to be notified.

The ISM also should have mechanisms to communicate crisis or event information. These mechanisms may include using e-mail if computing systems and networks are operational, cell phones, faxes, electronic pagers, web sites or an emergency phone number on which a message can be placed. Note, however, that some types of communication, such as e-mail, are by default in cleartext, making them subject to potential capture by perpetrators. The ISM should also develop methods to encrypt e-mail, PDAs and other communications used in communicating crisis or event-related information.

5.9.3 Intrusion Detection Policies and Processes

The ISM should understand and manage intrusion detection policies and procedures, including basic requirements such as ensuring that:
- Systems on which intrusion detection software runs are fault tolerant and are secure against attack
- Personnel who run and monitor intrusion detection systems have adequate training
- Intrusion detection software and hardware runs continuously
- Intrusion detection software can be easily modified and can adapt to changing environments
- Intrusion detection systems do not impose excessive overhead, especially excessive network overhead
- Intrusion detection systems detect a high percentage of anomalies

Ideally, a company should use an IDS that combines both host- and network-based sensors suitably placed to provide adequate coverage of the network topology (as discussed more fully in chapter 3). Most systems can be configured to automatically contact the security staff in the event suspicious activity is detected. If suspicious activity is identified, the organization should initiate procedures to respond.

Intrusion detection policies and procedures should also address the following issues related to incidents that are identified:
- Identifying any vulnerabilities exploited by the perpetrator
- Adequately protecting data obtained from intrusion detection systems against unauthorized disclosure, modification and destruction
- Copying and archiving logs and making a backup of systems that are impacted when appropriate and, in cases in which legal prosecution of any perpetrators is a real possibility, using forensics methods to preserve the integrity and admissibility of data in a court of law
- Identifying any apparent motivation(s) for attack
- Determining how many systems have been compromised
- Determining if any viruses, worms and/or Trojan horse programs remain in compromised systems
- Documenting steps taken to respond to incidents
- Assigning responsibilities for various aspects of the intrusion detection process

If a system has been compromised at the superuser level ("root" in UNIX and Linux systems and "administrator" in Windows and Novell systems), it should be rebuilt from the original installation medium, because one can never be sure of all the changes a superuser may have made. Additionally, all passwords on the system should be changed before users are allowed to access the system again.

The ISM should define goals, objectives and priorities for the intrusion detection effort and assess the alternatives that best fulfill these requirements. The ISM should understand the complete costs of implementing intrusion detection; resources to implement, monitor and respond to the output generated by these tools need to be allocated. Additionally, intrusion detection policies should also address actions to be taken in the event of an alert about a possible intrusion. Sometimes it is prudent to block the attack to protect the information assets at the expense of losing important information and evidence related to the attack. Cost vs. benefits of deploying defensive measures vs. obtaining evidence should be clearly delineated in the policies.

The ISM should determine the appropriate mix between externally managed security service providers to manage the organizations' IDSs and internal staff to achieve timely and knowledgeable reaction to malicious activity. Using only external security intrusion detection and incident response services is almost without exception unwise in that internal staff generally better understand the level of business risk that each incident introduces. Additionally, relying completely on outsourced services generally hinders integration of these functions into the IT mainstream. Although outsourcing may be more cost-effective and may also result in a higher level of technical expertise than might otherwise be available, involving employees in intrusion detection and incident response efforts, at least to some degree, is a wise idea.

5.9.4 Help Desk Processes for Identifying Security Incidents

The ISM should have processes defined for help desk personnel to distinguish a typical help desk request from when a possible security incident is reported. The help desk is extremely likely to receive the first report of a security-related problem. Prompt recognition of an incident in progress and quick referral to appropriate parties is critical to minimizing the damage resulting from such incidents.

By defining appropriate criteria and by improving the awareness of help desk personnel, the ISM will develop another important method to detect a security incident. Proper training will also help to reduce the risk that the help desk will be successfully targeted in a social engineering attack designed to obtain access to accounts, as when a perpetrator pretends to be a user who has been locked out and who requires immediate access to the system.

In addition to identifying the possible security incident, help desk personnel should be aware of the proper procedures to report and escalate the issue. This way, the organization can address the information in a timely manner.

5.9.5 The Notification Process

Having an effective and timely security incident notification process is a critical component of an effective security program. The ISM should understand how obtaining timely and relevant information can help the organization respond quickly and efficiently and will ultimately protect the organization from greater amounts of loss and damage that normally occur when incidents occur. Mechanisms that enable an automated detection system or monitor to send e-mail or phone messages to designated personnel exist. Functions within organizations that are most likely to need information concerning incidents when they occur include:

- Risk management
- Human relations (whenever an attack appears to be initiated by one or more insiders)
- Legal
- Public relations
- Network operations

If the information is taken seriously and responded to in a timely fashion, the overall response of the security organization can be enhanced considerably.

The ISM must guard against issuing too many alerts. Having decision criteria in place to determine the priority of events and criteria for issuing alerts will not only help others to take any alerts that are issued seriously, but will also help ensure that timely and coordinated responses occur to important events.

Notification activities are effective only if knowledgeable personnel understand their responsibilities and perform them in an efficient and timely manner. The ISM, therefore, needs to define the responsibilities and communicate them to key personnel. The ISM should also work with human resources to determine how these responsibilities can be documented in employee's job descriptions.

5.10 DOCUMENTING EVENTS

5.10.1 Establishing Procedures

The ISM must continually focus on preventative, reactive and proactive processes to protect the organization's information resources. However, there are times when an incident may occur and the security staff needs to have documented procedures so that relevant information can be recorded and the data preserved. By preserving these data, the ISM can investigate each event and provide information to a forensics team, if necessary.

Having a good legal framework is important to provide options to the organization. The ISM should develop data preservation procedures with the advice and assistance of legal counsel, the organization's managers and knowledgeable law enforcement officials to assure the procedures provide sufficient guidance to IT and security staff. With the assistance of these specialized resources, the ISM should be able to develop procedures to handle each security event in a manner that is appropriate to meet business objectives.

There are a few basic actions the information systems staff must understand. This includes doing nothing that could change/modify/contaminate potential or actual evidence. Professional forensics personnel can inspect computer systems that may be attacked, but if the organization's personnel contaminate the information, the data may not be admissible in a court of law and/or the forensics staff may be unable to use the data in investigating an incident. Computer forensics, gathering and handling information and physical objects relevant to a security incident in a systematic manner so that they can be used as evidence in a court of law, should usually be performed by a specially trained staff, third-party specialists, security incident response team or law enforcement officials. The initial response by the system administrator should include:

- Retrieving information needed to confirm an incident
- Identifying the scope and size of the affected environment (networks, systems, applications)
- Determining the degree of loss, modification or damage (if any)
- Identifying the possible path or means of attack
- Backing up all possible sources of evidence or relevant information when appropriate. (Note that full backups are better than incremental backups. Still, backups are costly in terms of time to perform them and disruption to users of backed up systems. Backups should be made only after costs vs. benefits have been carefully considered.).

5.10.2 Requirements for Evidence

The ISM should understand that any contamination of evidence following an intrusion could severely harm an organization's ability to prosecute a perpetrator. In addition, the modification of data can inhibit computer forensic activity necessary to identify the perpetrator and all the changes and effects resulting from the attack.

By overlooking these considerations, the organization may also not be able to identify how the attack occurred and how the security program should be changed and enhanced to reduce the risk of a similar successful attack in the future.

To ensure admissibility of evidence, it is advisable to use forensic tools to create a byte-by-byte copy of any evidence that may exist on hard drives and other media. To avoid the potential for alteration or destruction of incident-related data, any testing or data analysis should be conducted using this copy. The original should be given to a designated evidence custodian who should store it in a locked combination safe. The original media must remain unchanged and a record of who has had custody of it, the chain of evidence, must be maintained for the evidence to be admissible in a court of law.

Processes and procedures that address the proper use and handling of electronic evidence also need to be in place. The result will be strengthening the credibility of the evidence as an ongoing part of the organizations' system of records and controls.

5.11 POSTEVENT REVIEWS

5.11.1 Identifying Causes and Corrective Actions

The ISM should manage postevent reviews to learn from each incident and the resulting response and recovery effort and to use the information to improve the organization's response and recovery procedures. The ISM may perform these reviews with the help of third-party specialists if detailed forensic skills are needed.

Security incidents may not always be the result of externally initiated attacks, or even internally initiated attacks, but also can be the result of failures in security controls that have been implemented. For a systematic review of security events, the ISM should appoint an event review team. This team should review any evidence and develop

recommendations to enhance the information security program by identifying root (most fundamental) cause of a specific event and necessary measures to prevent the same/similar events from recurring. The root cause of many break-ins to systems, for example, is often weak or nonexistent vulnerability assessment and patch management efforts.

5.11.2 Postincident Reviews and Follow-up Procedures

Understanding the purpose and structure of postincident reviews and follow-up procedures will enable the ISM to continuously improve the security program. A consistent methodology should be adopted within the information security organization so that when a problem is found, an action plan is developed to reduce/mitigate it. Once the action plan is devised, steps should then be taken to implement the solution. By repeating these basic principles, the information security program will be able to adapt to changes in the organization and the threats it faces. In addition, this reduces the amount of time personnel need to react to security incidents, so they are able to spend more time on proactive activities.

5.12 CHAPTER 5 GLOSSARY

Access path
The logical route an end user takes to access computerized information including networks, systems, authentication and authorized systems, applications and application controls

Access rights
Permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy

Accountability
The ability to map a given activity or event to the responsible party to make the individual accountable for his/her actions

Activation
Action to put into operation a recovery team, alternate facility or service, procedure or contract

Administrative controls
The actions or controls dealing with operational effectiveness, efficiency and adherence to regulations and management policies

Alert situation
The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The organization entering into an alert situation initiates a series of escalation steps.

Alternate facilities
Locations and infrastructures from which the alternate processes are executed, when the main premises are unavailable or destroyed. This includes other buildings, offices or data processing centers.

Alternate process
Automatic or manual processes designed and established to continue critical business processes from point of failure to return to normality

Anonymous File Transfer Protocol (AFTP)
A method of downloading public files using the File Transfer Protocol (FTP). Anonymous FTP is called anonymous because users do not need to identify themselves before accessing files from a particular server. In general, users enter the word "anonymous" when the host prompts for a username. Anything can be entered for the password, such as the user's e-mail address or simply the word guest. In many cases, an anonymous FTP site will not even prompt a user for a name and password.

Antivirus software
Application software deployed at multiple points in an IT architecture designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected

Application controls
Manual or programmed activities intended to ensure the completeness and accuracy of records and the validity of entries made. The objective of application controls, either manual or programmed, is to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from manual and programmed processing.

Audit trail
A series of records either in hard copy or in electronic format that provide a chronological record of user activity and other events that show the details of user and system activity. Audit trails can be used to document when users log in, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred.

Authentication
The verification of the authenticity of a person or system requesting access to a resource to establish their legitimacy before access to the requested resource is granted. During the authentication process, the user enters a name or account number (identification) and password (authentication).

Availability
Ensuring that information systems and data are ready for use when they are needed; often expressed as the percentage of time that a system can be used for productive work

Backup center
This is an alternate facility to continue IT/IS operations when the main DP center is unavailable for a long period. There are several types depending on the time needed to make them operational (e.g., cold, warm, hot, mirror) property (own, hired, cooperative), the mobility (e.g., portable, fixed) and so on.

Bit-stream image
Bit-stream backups, also referred to as mirror image backups, involve the backup of all areas of a computer hard disk drive or another type of storage media. Such backups exactly replicate all sectors on a given storage device. All files and ambient data storage areas are thus copied.

Brute force
Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found

Business impact analysis (BIA)
An exercise that determines the impact of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting system.

Chain of custody
The chain of custody is a legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding, to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. This includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.

CobiT
Control Objectives for Information and related Technology, the international set of IT control objectives published by the IT Governance Institute

Confidentiality
The protection of sensitive or private information from unauthorized disclosure

Control center
The control center hosts the recovery meetings where disaster recovery operations are managed

COSO
A report titled *Internal Controls—An Integrated Framework* sponsored by the Committee of Sponsoring Organizations of the Treadway Commission in 1992. It provides guidance and a comprehensive framework of internal controls for all organizations.

Criticality analysis
An analysis to evaluate resources or business functions to identify their importance to the organization and the impact if a function cannot be completed or a resource is not available

Cybercops
An investigator of computer-crime-related activities

Damage evaluation
The determination of the extent of damage that is necessary to provide for an estimation of the recovery time frame and the potential loss to the organization

Decryption key
A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption

Defense in-depth
The practice of layering defenses to provide added protection. Defense in-depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an organization's computing and information resources.

Degauss
The application of variable levels of alternating current (AC) for the purpose of demagnetizing magnetic recording media. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, leaving a very low residue of magnetic induction on the media. Degauss loosely means to erase.

Digital certificate
The electronic equivalent of an ID card that is established under the X.509 standard, which is used to provide sender authenticity, message integrity and nonrepudiation

Digital code signing
The process of digitally signing computer code so its integrity remains intact

Disaster declaration
The communication to appropriate internal and external parties that the disaster recovery plan is being put into operation following a disaster situation

Disaster recovery plan
A set of human, physical, technical and procedural resources orientated to recover, within the minimum time and cost, an activity interrupted by an emergency or disaster

Disaster notification fee
The fee the recovery site vendor charges when the customer notifies them that a disaster has occurred and the recovery site is required. The fee is implemented to discourage false disaster notifications.

Disaster recovery plan desk checking
Disaster recovery plan desk checking is typically a read-through of a disaster recovery plan without any real actions taking place. It generally involves a reading of the plan, discussion of the action items and definition of any gaps that might be identified.

Disaster recovery plan walk-through
Disaster recovery plan walk-through is generally a more robust test of the recovery plan requiring that some recovery activities take place and are tested. A disaster scenario is often given and the recovery teams talks through the steps they would need to take to recover. They should test as many aspects of the plan as possible.

Discretionary access control (DAC)
A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Disk mirroring
The practice of duplicating data in separate volumes on two hard disks to make storage more fault tolerant. Mirroring provides data protection in the case of disk failure because data are constantly updated to both disks.

DMZ
The buffer zone between the Internet and the private network that is engineered using firewalls and other devices to prevent access by external parties to internal systems. The acronym is based on the military term "demilitarized zone" that is used to describe the buffer zone established between North and South Korea.

Domain name service (DNS)
A network service based on a hierarchical database system distributed across the Internet that translates the web address to IP addresses and vice versa

Dual control
A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource

External storage
The location which contains the backup copies to be used in case of disaster

Fall-through logic
Predicting which way a program will branch when an application is presented. It is an optimized code based on a branch prediction.

Firewall
A system or combination of systems that enforces a boundary between two or more networks typically forming a barrier between a secure and an open environment such as the Internet

Forensic examination
The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise

Honeypot
A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems

Hot site
A fully operational offsite data processing facility equipped with hardware and system software to be used in the event of a disaster

Hypertext Transfer Protocol (HTTP)
A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML, XML or other pages to the client browsers.

Impact analysis
An impact analysis is a study to determine the most critical services or applications for the organization. In an impact analysis threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.

Information security governance
The leadership, organizational structures and processes that safeguard information

Information security program
The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis

Integrity
The accuracy, completeness and validity of information in accordance with business values and expectations

Internet service provider (ISP)
A third party that provides individuals and organizations access to the Internet and a variety of other Internet-related services

Interruption window
The time the company can wait from the point of failure to the restoration of the minimum and critical services or applications. After this time, the progressive losses caused by the interruption are excessive for the organization.

Intrusion detection system (IDS)
An IDS inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack

IP Security (IPSec)
A protocol that supports two encryption modes: transport and tunnel. Transport mode encrypts the data portion (payload) of each packet but leaves the header untouched. Tunnel mode is more secure, since it encrypts the header and payload. On the receiving side, an IPSec-compliant device decrypts each packet.

ISO/IEC 17799
Originally released as part of the British Standard for Information Security in 1999 as the Code of Practice for Information Security Management, which in October 2000 was elevated by the International Organization for Standardization to an international code of practice for information security management. This standard defines information confidentiality, integrity and availability controls in a comprehensive information security management system.

Mail relay server
An e-mail server that relays messages so that neither the sender nor the recipient is a local user

Mandatory access control (MAC)
A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf

Maximum tolerable outages (MTO)
Maximum time the organization can support processing in alternate mode

Message Authentication Code
An American National Standards Institute (ANSI) standard checksum that is computed using the DES

Mirrored site
An alternate site that contains the same information as the original. Mirror sites are set up for backup and disaster recovery as well as to balance the traffic load for numerous download requests. Such download mirrors are often placed in different locations throughout the Internet.

Mobile site
The use of a mobile/temporary facility to serve as a business resumption location. They can usually be delivered to any site and can house information technology and staff.

Monitoring policy
Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted

Nonrepudiation
Assurance that a party cannot later deny originating data. It is the provision of proof of the integrity and origin of the data and can be verified by a third party. A digital signature can provide nonrepudiation.

Nonintrusive monitoring
The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities

Offline files
Computer file storage media not physically connected to the computer; typically tapes or tape cartridges used for backup purposes

Open Shortest Path First (OSPF)
A routing protocol that has been developed for IP networks. It is based on the shortest path first or link state algorithm.

Packet filtering
Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules

Passive response
A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action

Password cracker
A tool that tests the strength of user passwords searching for passwords that are easy to guess by repeatedly trying words from specially crafted dictionaries and often also by generating thousands (and in some cases even millions) of permutations of characters, numbers and symbols

Penetration testing
A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers

Ports
An interface point between a CPU and a peripheral device. A port can also be a convention that allows remote services to connect to a host in an orderly manner.

Proxy Server
A server that acts on behalf of a user. Typically proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps perform additional authentication, and then complete a connection to a remote destination on behalf of the user.

Reciprocal agreement
Emergency processing agreements between two or more organizations with similar equipment or applications. Typically participants promise to provide processing time to each other when an emergency arises.

Recovery action
Execution of a response or task according to a written procedure

Recovery point objective (RPO)
A measurement of the point prior to an outage to which data are to be restored

Recovery time objective (RTO)
The amount of time allowed for the recovery of a business function or resource after a disaster occurs

Redundant Array of Inexpensive Disks (RAID)
A technology that provides performance improvements and fault-tolerant capabilities, via hardware of software solutions, by writing to a series of multiple disks to improve performance and save large files simultaneously

Redundant site
A recovery strategy involving the duplication of key information technology components including data or other key business processes where by fast recovery can take place

Resilience
The ability of a system or network to recover automatically from any disruption usually within minimal recognizable effect

Risk assessment
A process used to identify and evaluate risks and their potential impact on an organization in quantitative or qualitative terms

Risk avoidance
The process for systematically avoiding risk

Risk mitigation
The reduction of risk through the use of countermeasures and controls

Risk transfer
The process of assigning risk to another organization, usually through the purchase of an insurance policy

Service delivery objectives (SDOs)
Level of services to be reached during the alternate process mode until the normal situation is restored. This is directly related with the business needs.

Sniffing
An attack in which data traversing a network are captured and monitored without authorization. This is similar to the more traditional wire tap but is done without legal authority. Sniffing is commonly used to capture passwords and other interesting and sensitive information that traverses the network.

Social engineering
An attack based on deceiving users or administrators at the target site. Social-engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user in an attempt to gain illicit access to systems. A person who illegally enters computer systems by persuading authorized person to reveal IDs, passwords and other confidential information.

Split knowledge
A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items; a condition under which two or more entities separately have key components which individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module

Spoofing
Faking the sending address of a network transmission

Threat analysis
An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against information assets and information technology. The threat analysis usually also defines the level of threat and the likelihood of that threat to materialize.

Two-factor authentication
The use of two independent mechanisms for authentication for example requiring a smart card and a password

Virus signature files
The file of virus patterns that are compared with existing files to determine if they are infected with a virus or worm

Virtual private network (VPN)
A secure private network that uses the public telecommunications infrastructure to transmit data. In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.

Warm site
A warm site is similar to a hot site; however, it is not fully equipped with all necessary hardware needed for recovery.

Web hosting
The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites. Most hosting is "shared" which means that web sites of multiple companies are on the same server in order to share costs.

Web Server
Using the client-server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.

Worm
A self-replicating program that does not attach itself to programs, but rather spreads independently of users' actions. Worms are in effect programmed network attacks.

5.13 CHAPTER 5 SAMPLE QUESTIONS

CISM exam questions are developed with the intent of measuring and testing practical knowledge in information security management. All questions are multiple choice and are designed for one best answer. Every CISM question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement.

In some instances, a scenario or a description problem may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. Many times a CISM examination question will require the candidate to choose the **MOST** likely or **BEST** answer.

In every case the candidate is required to read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked and how to study to gain knowledge of what will be tested will go a long way toward answering them correctly.

The sample questions contained below are designed to depict the type of question format on the CISM examination.

1. The primary goal of a post incident review is to:

   A. gather evidence for subsequent legal action.
   B. identify individuals who failed to take appropriate action.
   C. make a determination as to the identity of the attacker.
   D. identify ways to improve the response process.

2. What are the characteristics of an appropriate strategy for recovering critical resources?

   A. It covers all possible disruptions and damage to all of an organization's IT resources.
   B. It results in the lowest possible recovery time for virtually all incidents that occur.
   C. It provides a cost for a satisfactory recovery time that is sensible considering the impact and probability of occurrence that is specified in the business impact analysis.
   D. All of the above

3. The process of creating and maintaining a disaster recovery/business continuity plan should include which of the following?

   A. Creating a business impact analysis of the consequences of the disruption of critical business processes
   B. Identifying and prioritizing computing and other resources needed to support critical business processes during a disruption
   C. Conducting a test of the plan
   D. All of the above

4. The initial approach to disaster recovery should be to evaluate which of the following?

   A. Replacing faulty and obsolete IT equipment
   B. Built-in resilience of IT systems
   C. Restoring lost and damaged IT systems and facilities
   D. Creating additional security countermeasures if a disaster should occur

5. Which of the following statements about an incident response capability is correct?

A. A well-defined and well-managed incident response capability should have a proactive influence on an information security program.
B. An incident response capability's primary focus should be on security breaches, necessitating that it be independent of disaster recovery operations.
C. An incident response capability should have the authority to do whatever it deems appropriate when it is involved in responding to an incident.
D. The responsibility for creating a business continuity plan belongs primarily to an incident response capability.

6. If an organization needs insurance against dishonest or fraudulent behavior by its own employees, which of the follow types of coverage would it need to obtain?

A. Fidelity
B. Business interruption
C. Valuable papers and records
D. Business continuity

7. When a business continuity plan is tested, it is **BEST** to record results in terms of which of the following?

A. Verbal descriptions
B. Metrics such as time, amount and accuracy
C. The complexity of the test
D. How closely the test results resemble the results that would be obtained in live production environments

8. If an intruder or malicious program has gained superuser (e.g., root) access to a system, it is **BEST** to do which of the following?

A. Keep the system administrator(s) from accessing the system until it can be shown that they were not the attackers.
B. Carefully inspect the system and intrusion detection output to identify all changes and then undo them.
C. Rebuild the system.
D. Change all passwords, then resume normal operations.

9. Which of the following statements concerning the use of outsourced intrusion detection services is true?

A. Even if outsourcing intrusion detection services, ensure that some company employees are involved in intrusion detection.
B. Outsourced intrusion detection services generally cost more than having one's own employees involved in intrusion detection.
C. Expertise available from intrusion detection service providers is generally less than is available from within a company.
D. Most intrusion detection service providers will not provide only intrusion detection services—they will require a contract with them for incident response services.

10. If a forensics copy of a hard drive is needed, the copied data will be most defensible from a legal standpoint if what type of copy is made?

A. A compressed copy of all contents of the hard drive
B. A copy that includes all files and directories
C. A byte-by-byte copy of all data
D. An encrypted copy of all contents of the hard drive

5.14 CHAPTER 5 ANSWERS TO SAMPLE QUESTIONS

1. **D** The goal of a postincident review is to identify ways in which the incident response process can be improved. It should not be focused on finding and punishing those individuals who did not take appropriate action or learning the identity of the attacker. Evidence should have already been gathered earlier in the process.

2. **C** A recovery strategy must be based on business impact—specifically, by minimizing rather than completely eliminating it, the latter of which is impossible.

3. **D** All of the answers here—performing a business impact analysis, identifying and prioritizing resources needed, and testing the plan—are critical components of creating and maintaining a disaster recovery/business continuity plan.

4. **B** Resilience of systems should be the ISM's initial focus. Keeping systems resilient rather than having to change to a different mode of operations is the most straightforward and often the most cost-effective approach.

5. **A** An effective incident response capability should proactively influence an information security program because it should produce "lessons learned" from incidents that change practices within an information security program. If, for example, an incident response team must constantly deal with incidents due to failure to patch vulnerabilities in systems, this team should provide feedback to the ISM that more attention needs to be paid to the vulnerability eradication effort.

6. **A** Fidelity coverage means insurance coverage against loss from dishonesty or fraud by employees.

7. **B** Metrics provide an objective means of recording data (e.g., in contrast to verbal descriptions), and they are also most conducive to subsequent analysis. Perhaps most important of all, however, is that metrics provide the best way to communicate results to management and others who need to learn about the results of testing.

8. **C** If someone or a malicious program gains superuser privileges on a system without authorization, the organization never really knows what the perpetrator or program has done to the system. The only way to assure the integrity of the system is to wipe the system clean (usually after making a complete data backup for the purpose of further analysis and also to prevent the destruction of data that may not exist elsewhere) and start over again by reinstalling the operating system and applications. Note that alternative D would be defensible if the system was rebuilt first, but the way this alternative is worded makes it wrong because it omits any mention of the need to rebuild the system. To be correct, alternative D would have to be worded "rebuild the system and then change all passwords."

9. **A** An organization should not completely outsource intrusion detection efforts. Internal employees need to be involved, at least to some degree, to prevent intrusion detection from becoming an isolated activity within the IT arena. Additionally, internal employees are much more likely to understand business risks connected with incidents and attacks that are detected.

10. C There is no alternative to making a byte-by-byte copy, if one wants forensics evidence that is "air tight." Only a byte-by-byte copy will result in capturing all data on a hard drive. Copying all files and folders will, in contrast, miss certain data, such as data between the end of a file and the end of the disk sector ("slack space").

5.15 CHAPTER 5 REFERENCES

Barbin, Douglas; John Patzakis; "Computer Forensics Emerges as an Integral Component of an Enterprise Information Assurance Program," ***Information Systems Control Journal*****, vol. 3, 2002, p. 25-27**

Brassil, Regina; "The Changing Realities of Recovery. How Onsite and Mobile Options Revolutionized the Business Continuity Industry," ***Information Systems Control Journal*****, vol. 2, 2003, p. 30-32**

Business Impact Analysis: Business Unit/Cost Center Questionnaire, *www.auditnet.org/docs/BIAQuestionnaire.doc*

Caldwell, Matthew; "The Importance of Event Correlation for Effective Security Management," ***Information Systems Control Journal*****, vol. 6, 2002, p. 36-38**

CERT Coordination Center, "Defending Yourself: The Role of Intrusion Detection Systems," *www.cert.org/archive/pdf/IEEE_IDS.pdf*

ComputerWorld, Security Knowledge Center, *www.computerworld.com/securitytopics/security/resources/0,11188,KEY73_RLI704,00.htm*

Contingency Planning and Management, CPM Group, *www.contingencyplanning.com*

Disaster Recovery Journal, *www.drj.com*

Doughty, Ken; "Business Continuity: A Business Survival Strategy," ***Information Systems Control Journal*****, vol. 1, 2002, p. 28-36**

Deloitte & Touche, ***e-Commerce Security—Business Continuity Planning*****, Information Systems Audit and Control Foundation, USA, 2002**

Endorf, Carl; Eugene Schultz; Jim Mellander; ***Intrusion Detection and Prevention*****, McGraw-Hill, USA, 2004**

Federal Computer Incident Response Center, *www.fedcirc.gov* (Describes an incident response approach and is a repository for other incident response information)

Federal Emergency Management Agency, *www.fema.org*

Federal Emergency Management Agency, Global Emergency Management System, *www.fema.gov/gems/index.jsp*

Frasier, B. (Ed.); *Site Security Handbook*, RFC 2196, *www.ietf.org/*

Grance, T.; K. Kent; B. Kim; *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, NIST Publication 800-61, 2003, *http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf*

Hiles, Andrew; Peter Barnes (Eds.); *Definitive Handbook of Business Continuity Management*, Wiley, USA, 2001

Information Security and Forensics Society, *www.isfs.org.hk* (Includes guidance and standardized security and forensics techniques)

International Association of Computer Investigative Specialists, *www.cops.org/forensic_examination_procedures.htm#Forensic%20Examination%20Procedures* (Provides a description of forensic procedures)

Note: Publications in bold are available in the ISACA Bookstore, ***www.isaca.org/pubs1.htm*****.**

International Association of Emergency Managers, *www.iaem.com* (Provides information on emergency management techniques and roles)

International Organization on Computer Evidence, *www.ioce.org*

Mandia, K.; C. Prosise; M. Pepe; *Incident Response and Computer Forensics 2nd Edition*, McGraw-Hill, USA, 2003

Maconachy, William V.; Corey Schou; James Frost; John Springer; "Building an Educational Response to Terrorism: A Multifaceted Problem, A Multidimensional Response," *Information Systems Control Journal*, vol. 6, 2004, p. 42-47

McCallam, D.H; P.G. Luzwick; *Maintaining Operational Continuity During Attacks on the Information Environment*, *Information Security Bulletin*, vol. 7, issue 5, 2002, p. 17-28

Meyers, Kenneth N.; *Manager's Guide to Contingency Planning for Disaster: Protecting Vital Facilities and Critical Operations 2nd Edition*, Wiley, USA, 1999

Musaji, Yusufali F.; "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans," *Information Systems Control Journal*, vol. 1, 2002, p. 49-55

National Institute of Standards and Technology (NIST), "Establishing a Security Incident Response Capability," USA, *http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf* (A guide for establishing an incident response center)

Northcutt, S.; *Network Intrusion Detection: An Analyst's Handbook*, New Riders, USA, 1999

Proctor, P.; *The Practical Intrusion Detection Handbook*, Prentice Hall, USA, 2000

Purdue University, Intrusion Detection, *www.cerias.purdue.edu/coast/intrusion-detection/welcome.html*

Ross, Steven J.; "Lessons From Tragedy," *Information Systems Control Journal*, vol. 1, 2002, p. 11-12

Schultz, E.; R.M. Shumway; *Incident Response: A Strategic Guide for Handling Security Incidents in Systems and Networks*, New Riders, USA, 2001

Schultz, Eugene; E. Spafford; "Intrusion Detection: How to Utilise a Still Immature Technology," in H. Tipton and M. Krause, *Information Security Management Handbook, 4th Edition*, USA, Auerbach, 2000

Search Security, *http://searchsecurity.techtarget.com/bwlRelatedInfo/0,290917,sid14_tax285163,00.html* (Search engine for information security-related articles)

Stephenson, Peter; *Investigating Computer-Related Crime*, CRC Press, USA, 2000

Survice Engineering Company, *www.survice.com*

Zawada, Brian; Jared Schwartz; " Business Continuity Management Standards—A Side-by-side Comparison," *Information Systems Control Journal*, vol. 2, 2003, p. 26-28

Note: Publications in bold are available in the ISACA Bookstore, *www.isaca.org/pubs1.htm*.

General Information

Requirements for Certification

To earn the CISM designation, information security professionals are required to:

1. Successfully pass the CISM exam
2. Adhere to the Information Systems Audit and Control Association Code of Professional Ethics and agree to comply with a continuing education policy
3. Submit verified evidence of five (5) years of work experience in the field of information security. Three (3) of the five (5) years of work experience must be gained performing the role of an information security manager. In addition, this work experience must be broad and gained in three of the five "job practice" areas.

   Substitutions for work performed in the role of an information security manager are not allowed. However, a maximum of two (2) years for general work experience in the field of information security may be substituted as follows:

   - Two years of general work experience may be substituted for currently holding one of the following broad security-related certifications or a post-graduate degree:
     —Certified Information Systems Auditor (CISA) in good standing
     —Certified Information Systems Security Professional (CISSP) in good standing
     —Post-graduate degree in information security or a related field (for example, business administration, information systems, information assurance)

   OR

   - A maximum of one year of work experience may be substituted for one of the following:
     —One full year of information systems management experience
     —Currently holding a skill-based security certification [e.g., SANS Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security+, Disaster Recovery Institute Certified Business Continuity Professional (CBCP)]

   Experience must have been gained within the 10-year period preceding the application for certification or within five (5) years from the date of initially passing the exam. Application for certification must be submitted within five (5) years from the passing date of the CISM exam. All experience must be verified independently with employers.

It is important to note that a CISM candidate may choose to take the CISM exam prior to meeting the experience requirements.

Description of the Examination

The CISM Certification Board oversees the development of the examination and ensures the currency of its content. The exam consists of 200 multiple-choice questions that cover the CISM job practice areas. The exam covers five information security management areas created from the CISM job practice analysis and reflects the work performed by information security managers. The job practice was developed and validated using prominent industry leaders, subject matter experts and industry practitioners.

Registration for the CISM Examination

The 2006 CISM examination will be administered on Saturday, 10 June 2006, unless specified otherwise in the CISM Bulletin of Information. To register for the examination, a candidate must complete and submit the registration form in the Bulletin of Information. The registration form can be obtained from ISACA at the following address:
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA
Attention: CISM Examination Registrar
Telephone: +1.847. 253.1545
Fax: +1.847. 253.1443
E-mail: *certification@isaca.org*

Additionally, an online form is available at the ISACA web site, *www.isaca.org*.

The CISM examination fee must accompany the registration form. The *Candidate's Guide to the CISM Examination* will be sent upon receipt and recording of your registration form.

Administration of the Examination

ISACA has contracted with an internationally recognized testing agency. This not-for-profit corporation engages in the development and administration of credentialing examinations for certification and licensing purposes. It assists ISACA in the construction, administration and scoring of the CISM and CISA examinations.

Sitting for the Examination

Be prompt. Registration will begin at the time indicated on your admission ticket at each center. All candidates must be registered and in the test center when the chief examiner begins reading the oral instructions. No candidate will be admitted to the test center once the chief examiner begins reading the oral instructions, approximately 30 minutes before the examination begins.

Remember to bring your admission ticket and an acceptable form of identification with a photo passport, photo ID or driver's license or other identification with a signature and such descriptive information as height, weight and eye color (such as a nonphoto driver's license).

Observe the following conventions when completing the examination:

- You are not allowed to bring study materials into the examination site.
- Bring several No. 2 lead pencils. Do not assume someone will provide you with a pencil for answering the examination.
- The chief examiner or designate at each test center will read aloud the instructions for entering information on your answer sheet. It is imperative that you include your examination identification number as it appears on your admission ticket and any other requested information. Failure to do so may result in a delay or errors.
- Read the provided instructions carefully before attempting to answer questions. Skipping over these directions or reading them too quickly could result in you missing important information and possibly losing credit points.
- It is imperative that you mark the appropriate area when indicating your response on the answer sheet. When correcting a previously answered question, fully erase a wrong answer before writing in the new one.
- Remember to answer all questions since there is no penalty for wrong answers. Grading is based solely on the number of questions answered correctly. Do not leave any question blank.
- Identify key words or phrases in the question (**MOST, BEST, FIRST...**) before selecting and recording your answer.

Budgeting Your Time

The following are time-management tips for the exam:

- Try to arrive at the examination testing site at least 30 minutes before the examination instructions are read. This will give you time to locate a seat and get acclimated.
- The examination is administered over a four-hour period. This allows for a little over one minute per question. Therefore, it is advisable that candidates pace themselves to complete the entire exam. Candidates must complete an average of 50 questions per hour.
- Candidates are urged to record their answers on their answer sheet. No additional time will be allowed after the examination time has elapsed to transfer or record answers should candidates mark their answers in the question booklet.

Rules and Procedures

- You will be asked to sign the answer sheet to protect the security of the examination and maintain the validity of the scores.
- Upon the discretion of the CISM Certification Board, any candidate can be disqualified who is discovered engaging in any kind of misconduct, such as giving or receiving help; using notes, papers or other aids; attempting to take the examination for someone else; or removing test materials or notes from the testing room. The testing agency will provide the board with records regarding such irregularities. The board will review reported incidents, and all board decisions are final.
- You cannot take the exam question booklet with you after completion of the exam.

CISM Exam Results

Approximately 10 weeks after the exam date, score reports will be mailed to candidates. To ensure the confidentiality of scores, exam results will not be repeated by telephone, fax or e-mail. CISM candidates will receive a report indicating their exam score. Candidates can request an e-mail pass/fail-only result by marking the appropriate box on the CISM examination registration form. This score is a scaled score with candidates receiving a score of 75 or more passing the exam. These individuals can then apply for CISM certification. A candidate receiving a score of 74 or less must retake the exam.

Candidates will receive a score report containing a subscore for each job area. Successful candidates will receive, along with a score report, an application for CISM certification. Unsuccessful candidates will receive, along with a score report, a copy of the new Bulletin of Information. The subscores can be useful in identifying those areas in which the candidate may need further study before retaking the examination. Unsuccessful candidates should note that taking either a simple or weighted average of the subscores does not derive the total scaled score.

Evaluation

To improve the usefulness of future manuals, please take a moment to evaluate the *CISM Review Manual 2006*. Such feedback is invaluable to our efforts to fully serve the profession and future CISM examination candidates.

Please complete this evaluation and return or fax to:

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Attention: CISM Certification
Fax: +1.847.253.1443

1. The *CISM Review Manual 2006* was (check one):

___ very helpful in preparing me for the exam.	___ helpful in preparing me for the exam.	___ not very helpful in preparing me for the exam.

2. The *CISM Review Manual 2006* was (check one):

___ too detailed in preparing me for the exam.	___ detailed enough in preparing me for the exam.	___ not detailed enough in preparing me for the exam.

3. The references to other publications and web sites were (check one):

___ very helpful in preparing me for the exam.	___ helpful in preparing me for the exam.	___ not very helpful in preparing me for the exam.

4. The design of the *CISM Review Manual 2006* made it (check one):

___ very easy to read	___ readable	___ hard to read

Please also note any specific comments and/or suggestions you may have concerning errors and omissions, enhancements, references and format. If you wish, please include your name, address and phone number so we may follow up with you. Thank you for your support and assistance.

Other Comments/Suggestions

Notes

Prepare for the **June/December 2006** *CISM Exam*

Order Now—2006 CISM® Review Materials for Exam Preparation and Professional Development

To pass the CISM exam a candidate should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers study aids and review courses to exam candidates (see *www.isaca.org/cismexam* for more details).

CISM Review Manual 2006

Information Systems Audit and Control Association

The *CISM Review Manual 2006* is a reference guide designed to assist individuals in preparing for the Certified Information Security Manager® (CISM®) examination and for individuals wanting to learn more about the role and responsibilities of an information security manager. The 2006 edition is significantly enhanced with changes of structure for a more comprehensive flow, updates to the content reflecting regulatory and technical changes and expanded coverage of critical areas. The manual features detailed descriptions of the tasks performed by information security managers, and the knowledge necessary to manage, design and oversee an enterprise's information security program. These task and knowledge statements were developed by the CISM Certification Board, validated by subject matter experts and serve as the blueprint for the CISM examination content and emphasis.

Information provided includes an explanation of each task and related knowledge statement, applicable information security management principles, practices and strategies. Detailed references of where to find additional guidance materials is also provided. This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and review courses.

This manual has been developed and organized to assist in the study of the following job practice areas:
- Information security governance
- Risk management
- Information security program(me) management
- Information security management
- Response management

The *CISM Review Manual 2006* also provides definitions and practical examples to facilitate the learning process.

CM-6 English Edition

CISM Questions, Answers & Explanations Manual 2006

Information Systems Audit and Control Association

This manual consists of 200 multiple-choice study questions arranged in the same proportion as the CISM job analysis. Many of these items appeared in the 2004 and 2005 editions of the *CISM Review Questions, Answers & Explanations Manual*, but have been rewritten to recognize a change in practice, be more representative of the exam item format, and/or provide further clarity or explanation of the suggested correct answer. These questions are not actual exam items, and are intended to provide the CISM candidate with an understanding of the type and structure of questions and subject matter that has previously appeared on the examination.

These questions are provided in two formats.
- **Questions sorted by content area**—Questions, answers and explanations are provided (sorted) by CISM job content area. This allows the CISM candidate to study material by content area and refer to specific questions, as well as evaluate their comprehension of the topics covered within each content area.
- **Sample test**—The two hundred questions are scrambled to represent a CISM-length examination. Candidates are urged to use this sample test and the answer sheet provided to simulate an examination. Many candidates use this exam as a pretest to determine their strengths or weaknesses and/or as a final exam. Sample exam answer sheets have been provided for both uses. In addition, a sample exam answer/reference key is included. All sample test questions have been cross-referenced to the questions sorted by content area, making it convenient to refer back to the explanations of the correct answers.

This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement*.

CQA-6 English Edition

CISM Questions, Answers & Explanations Manual 2006 Supplement

Information Systems Audit and Control Association

This manual consists of 100 multiple-choice study questions arranged in the same proportion as the CISM job practice analysis. The questions include the answers and detailed explanations for the candidates to use in preparation for the CISM exam. Unlike some review manuals that use questions from other certification exams, these questions were prepared especially for use in studying for the CISM exam. These questions are intended to provide the CISM candidate with an understanding of the type and structure of questions that have typically appeared on the examination and are not actual test items.

This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and the *CISM Review Questions, Answers & Explanations Manual 2006*.

CQA-6ES English Edition

To order the CISM review materials for the June/December 2006 CISM exam, visit our web site at *www.isaca.org/cismbooks*.

2005 CISM Review Materials are available in Japanese and Spanish.

See *www.isaca.org/nonenglishbooks*.