IT Governance Institute®

Leading the IT Governance Community

2nd Edition

CobiT® Security Baseline

An Information Security Survival Kit

Current Security Risks

44 Steps Towards Security

Information Security Survival Kits

IT Governance Institute®

Leading the IT Governance Community

2nd Edition

CobiT Security Baseline

An Information Security Survival Kit

Current Security Risks

44 Steps Towards Security

Information Security Survival Kits

IT Governance Institute®

The IT Governance Institute (ITGI™) (*www.itgi.org*) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities. ITGI offers electronic resources, original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer

ITGI (the 'Owner') and the author have designed and created this publication, titled *COBIT® Security Baseline: An Information Security Survival Kit, 2nd Edition* (the 'Work'), primarily as an educational resource for control professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web sites: *www.itgi.org*

ISBN 978-1-933284-81-1
COBIT® Security Baseline: An Information Security Survival Kit, 2nd Edition
Printed in the United States of America

ACKNOWLEDGEMENTS

IT Governance Institute wishes to recognise:

Editors
Steven De Haes, University of Antwerp Management School, Belgium
Erik Guldentops, CISA, CISM, University of Artwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Kevin Hayes, Learning and Skills Council, UK
John W. Lainhart IV, CISA, CISM, IBM Business Consulting Services, USA
Dirk Steuperaert, CISA, PricewaterhouseCoopers LLP, Belgium

Expert Reviewers
Kent Anderson, CISM, Network Risk Management LLC, USA
Garry Barnes, CISA, CISM, NSW Department of Education and Training, Australia
Michael Bilger, IBM Global Services, USA
William C. Boni, CISM, Motorola, USA
Dirk Bruyndonckx, CISA, CISM, MCA, KPMG LLP, Belgium
Reynaldo de la Fuente, CISA, CISM, Datasec SRL, Uruguay
Arnold Dito, CISA, USA
Heidi Erchinger, CISA, CISSP, System Security Solutions Inc., USA
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Kyeong Hee Oh, CISA, CISM, CISSP, Green Soft, Korea
Jimmy Heschl, CISM, CISA, KPMG, Austria
John A. Kay, CISA, Information Systems Auditor/Consultant, USA
Luc Kordel, CISA, CISM, CISSP, RE, Kordel & Co., Belgium
Mark Lobel CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA
Leslie Macartney, CISA, CISM, UK
Debra Mallette, CISA, Kaiser Permanente, USA
Akira Matsuo, CISA, CPA, KPMG, Japan
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada

ITGI Board of Trustees
Lynn Lawton, CISA, FCA, FIIA, PIIA, KPMG LLP, UK, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President
Frank Yam, CISA, FHKCS, FH KIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee
Tony Hayes, FCPA, Queensland Government, Australia, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Lucio Molina Focazzio, CISA, Colombia
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada
Michael Schirmbrand, Ph. D., CISA, CISM, CPA, KPMG, Austria
Robert E. Stroud, CA Inc., USA
John Thorp, The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and IT Alignment and Governance Research Institute (ITAG), Belgium

COBIT Steering Committee
Robert E. Stroud, CA Inc., USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Rafael Eduardo Fabius, CISA, Republica AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Jimmy Heschl, CISM, CISA, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgium

ITGI Affiliates and Sponsors
ISACA Chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants Inc.
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
CA
Hewlett-Packard
IBM
ITpreneurs Nederlands BV
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

TABLE OF CONTENTS

1. **Introduction** 7
   COBIT as a Foundation for Good Security Practices 7
   Security Is Not a One-time Effort 8
   Document Structure 8

2. **Information Security Defined** 10

3. **Current Risks—Why Information Security Is Important** 12
   Hype or Reality 12

4. **COBIT Security Baseline—44 Steps Towards Security** 14

5. **Information Security Survival Kit 1—Home Users** 23
   Specific Information Security Risks for Home Users 23
   Home Users Survival Kit 23

6. **Information Security Survival Kit 2—Professional Users** 25
   Specific Information Security Risks for Professional Users 25
   Professional Users Dos and Don’ts 25

7. **Information Security Survival Kit 3—Managers** 27
   Specific Information Security Risks for Managers 27
   Managers Checklist 27

8. **Information Security Survival Kit 4—Executives** 30
   Specific Information Security Risks for Executives 30
   Executives Questions and Actions 30

9. **Information Security Survival Kit 5—Senior Executives** 33
   Specific Information Security Risks for Senior Executives 33
   Senior Executives Questions and Actions 33

10. **Information Security Survival Kit 6—Boards of Directors/Trustees** 35
    Specific Information Security Risks for Board Members 35
    Directors and Trustees Questions and Actions 35

11. **Summary of Technical Security Risks** 37
    Intentional Misuse of the Computer 37
    Violation of Rules and Regulations 40
    Accidents 40

12. References....................41
General Information Security and IT Governance Standards and Frameworks....................41
General Information Security Web Sites....................43
Technical Information Security Guidance....................44
Information Security News....................46

Appendix— COBIT and Related Products....................47

1. INTRODUCTION

Information security is a key aspect of IT governance, and it is an important issue for all computer users to understand and address. As computer systems have become more and more commonplace in all walks of life, from home to school and the office, unfortunately, so too have the security risks.

The widespread use of the Internet, handheld and portable computer devices, and mobile and wireless technologies has made access to data and information easy and affordable. On the other hand, these developments have provided new opportunities for IT-related problems to occur, such as theft of data, malicious attacks using viruses, hacking, denial-of-service (DoS) attacks and even new ways to commit organised crime. These risks, as well as the potential for careless mistakes, can all result in serious financial, reputational and other damages.

The technology also provides opportunities to enhance security in ways that were impossible before, such as backups and granularity in restricting access. Recognising the need for better security guidance, this booklet has been developed to provide essential advice and practical tools to help protect computer users from these risks.

COBIT AS A FOUNDATION FOR GOOD SECURITY PRACTICES

This guide is based on *Control Objectives for Information and related Technology* (COBIT®), which is a comprehensive set of resources that contains the information organisations need to adopt an IT governance and control framework. COBIT covers security in addition to other risks that can occur with the use of IT. This guide has been updated and aligned with the new COBIT® 4.1 framework.

This publication focuses on the specific risk of information security in a way that is simple to follow and implement for the home user or the user in small to medium enterprises, as well as for executives and board members of larger organisations. It provides the following elements:

- Useful background reading
- An introduction to information security—what it means and what it covers
- An explanation of why security is important, with examples of the most common things that can go wrong
- Some thought-provoking questions to help determine risks
- The COBIT-based security baseline, providing key controls
- In addition to the mapping against COBIT 4.1, a mapping against the updated ISO/IEC 27002:2005 information security standard
- Information security survival kits providing essential questions and checklists for varying audiences, including home users, professional users, managers, executives and boards of directors
- An appendix containing a summary of technical security risks

There is no such thing as 100 percent security, but by following the advice suggested in this guide and maintaining an awareness of security-related risks and vulnerabilities, a very effective level of security will be achieved. Although this guide is not exhaustive, if all the guidance provided is implemented, security protection will be well above the average found in most organisations.

SECURITY IS NOT A ONE-TIME EFFORT

This guide should be referred to regularly because principles like these need to be continually reinforced. IT environments keep changing, and new security risks can occur at any time.

The amount of effort applied to implementing a safe and secure working environment should be based on the impact a security problem could have at home or at work. However, implementing good security does not necessarily mean large amounts of time or expense. For example, by raising awareness, recognising the risks that can occur and taking sensible precautions when using IT, security can be achieved with little effort.

Implementing technical safeguards can be more complex and expensive; therefore, proven products from reputable suppliers should always be used and, if necessary, experts should be called on for advice. In any case, these are not one-time efforts but require attention on an ongoing basis.

This guide cannot highlight every risk or suggest precisely what level of control is needed, but it will significantly improve the ability to identify what must be done and why.

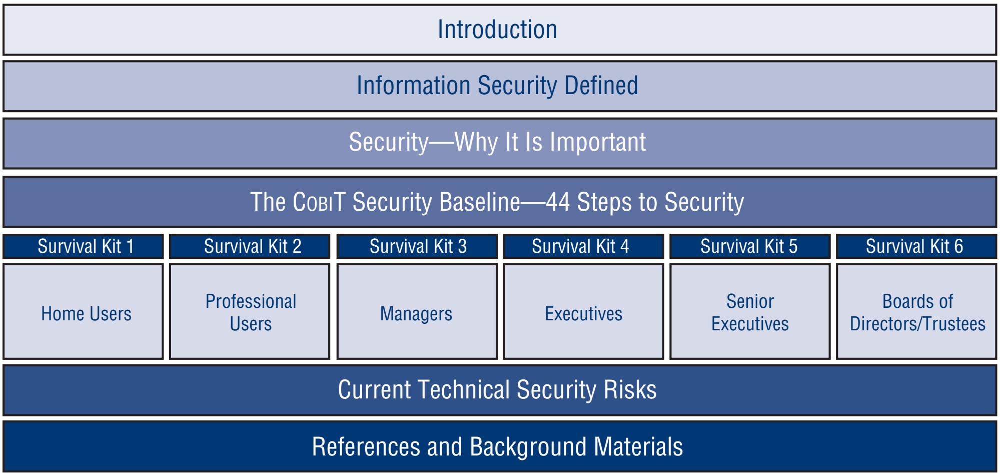
The benefits of good information security are not just a reduction in risk or a reduction in the impact should something go wrong. Good security will improve an enterprise's reputation, build its confidence and increase the trust from others with whom business is conducted, and can even improve efficiency by making it possible to avoid wasted time and effort recovering from a security incident. Having a good security posture can allow an organisation to more successfully embrace new opportunities.

If additional IT issues and/or risks other than security are of concern, *COBIT® Quickstart: Essentials to Quickstart IT Governance, 2nd Edition,* which provides a summary baseline of the key IT control objectives, or the full COBIT set of resources may be useful.

DOCUMENT STRUCTURE

Figure 1 illustrates the structure of this guide and will help readers easily navigate the document.

Figure 1—*COBIT Security Baseline* Structure



Introduction

Information Security Defined

Security—Why It Is Important

The COBIT Security Baseline—44 Steps to Security

Survival Kit 1	Survival Kit 2	Survival Kit 3	Survival Kit 4	Survival Kit 5	Survival Kit 6
Home Users	Professional Users	Managers	Executives	Senior Executives	Boards of Directors/Trustees

Current Technical Security Risks

References and Background Materials

2. Information Security Defined

Security relates to the protection of valuable assets against unavailability, loss, misuse, disclosure or damage. In this context, valuable assets are the information recorded on, processed by, stored in, shared by, transmitted from or retrieved from any medium. The information must be protected against harm from threats leading to different types of impacts, such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents, and intentional damage.

> *Information security provides the management processes, technology and assurance to allow businesses' management to ensure business transactions can be trusted; ensure IT services are usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it.*
>
> —Dr. Paul Dorey, director, Digital Business Security, BP Plc., UK

The objective of information security is protecting the interests of those relying on information and the systems and communications that deliver the information from harm resulting from failures of availability, confidentiality and integrity. The impact of the Internet and the growth of the networked economy have added the need for trust in electronic transactions. For most computer users, the security objective is met when:

- Information systems are available and usable when required, and can appropriately resist attacks and recover from failures (availability)
- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is protected against unauthorised modification or error so that accuracy, completeness and validity are maintained (integrity)
- Business transactions and information exchanges between enterprises, customers, suppliers, partners and regulators can be trusted (authenticity and non-repudiation)

The relative priority and significance of availability, confidentiality, integrity and trust vary according to the value and type of information and the context in which the information is used. For example, integrity of management information is especially important to a business that relies on critical strategy-related decisions, and integrity of an online purchase is very important to the home user.

The amount of protection required depends on how likely a security risk is to occur and how big an impact it would have if it did occur. Protection is achieved by a combination of technical and non-technical safeguards. For the home user, this means installation of reputable security tools, maintenance of up-to-date software, care with backups, and being careful and alert to the hazards of using computers and connecting to the Internet. For large enterprises, protection will be a major task with a layered series of safeguards, such as physical security measures, organisational measures, security procedures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls.

In the ever-changing technological environment, security that is state-of-the-art today may be obsolete tomorrow. Therefore, security protection must keep pace with these changes.

> *Computer security: A computer is secure if you can depend on it and its software to behave as you expect.*
>
> —Dr. Eugene Spafford, professor and executive director, Purdue University Center for Education and Research in Information Assurance and Security (CERIAS), USA

3. CURRENT RISKS—WHY INFORMATION SECURITY IS IMPORTANT

IT has become an integral part of everyday business and private life, and dependency on information systems is constantly growing. New technologies have emerged that allow unprecedented functionality but introduce new risks and environments that are harder to control, e.g., wireless technology, mobile computing and integration of technologies (such as audio/video and mobile computing). Increased dependency on IT means a higher impact when things go wrong. Whether it occurs to a home user relying on home banking or an enterprise relying on online customers, an Internet security breach can have a real and major impact. With the widespread use of networks, individuals are rightly concerned about the privacy of their personal information, and companies need to protect the confidentiality of corporate data, while encouraging electronic business.

Increasing technical complexity leads to new and more complex risks. In chapter 11, Summary of Technical Security Risks, a non-exhaustive and indicative primer on current technical risks that users might face today is provided.

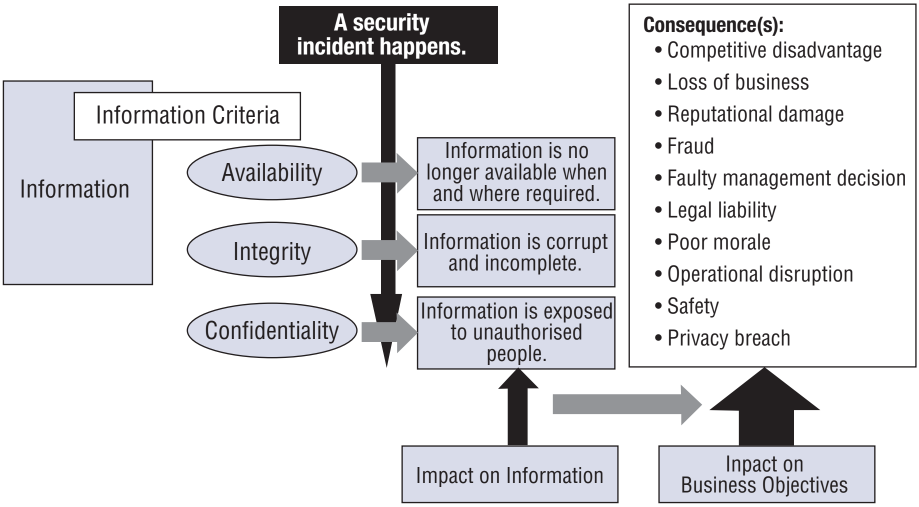
Gaps in security are usually caused by:
- Lack of a comprehensive and maintainable risk and threat management process
- New vulnerabilities resulting from the widespread use of new technologies
- Lack of maintenance to assure all patches are promptly made
- Increased networking and mobile working
- Lack of security awareness
- Insufficient discipline when applying controls
- New and determined efforts of hackers, fraudsters, criminals and even terrorists
- Changing legislative, legal and regulatory security requirements

Because new technology provides the potential for dramatically enhanced business performance, improved and demonstrated information security can add real value to the organisation by contributing to interactions with trading partners, closer customer relationships, improved competitive advantage and protected reputation. It can also enable new and easier ways to process electronic transactions and generate trust.

HYPE OR REALITY

Anyone doubting the significance of information security should take a moment to consider the potential impact of a security incident personally or on the organisation or working environment. **Figure 2** illustrates some of the ramifications if an incident were to occur.

Figure 2—Impact of a Security Incident


A security incident happens.
Information
Information Criteria
Availability
Integrity
Confidentiality
Information is no longer available when and where required.
Information is corrupt and incomplete.
Information is exposed to unauthorised people.
Consequence(s):
• Competitive disadvantage
• Loss of business
• Reputational damage
• Fraud
• Faulty management decision
• Legal liability
• Poor morale
• Operational disruption
• Safety
• Privacy breach
Impact on Information
Inpact on Business Objectives

Competitive disadvantage	How damaging would it be if information were disclosed to a competitor?
Loss of business	Could business revenues or profits be lost if information were disclosed, incorrect or lost?
Reputational damage	If information were disclosed, what damage could there be to customer confidence, public image or shareholder/supplier loyalty?
Fraud	If information were disclosed or altered, could goods or funds be improperly diverted?
Faulty management decision	Could incorrect business decisions be made as a result of errors in or unauthorised changes to information?
Legal liability	Could disclosure of information or tampering with information result in a breach of legal, regulatory or contractual obligations?
Poor morale	If information were disclosed or lost, could there be a damaging effect on staff morale or motivation?
Operational disruption	Could the business be otherwise disrupted by the unavailability of applications or information services?
Safety	Could incorrect records put the user's health or even life at risk?
Privacy breach	Could the user suffer personally through loss of privacy or unauthorised use of his/her identity?

4. COBIT SECURITY BASELINE— 44 STEPS TOWARDS SECURITY

Like securing a house, securing information systems requires a combination of physical/technological and behavioural measures. There is no sense in turning on the house alarm and leaving the back door open. There is also no sense in implementing the latest network security devices if staff members do not know how to operate the devices or know what to do if a breach is detected. Information security is as much about behaviour as it is about technical safeguards.

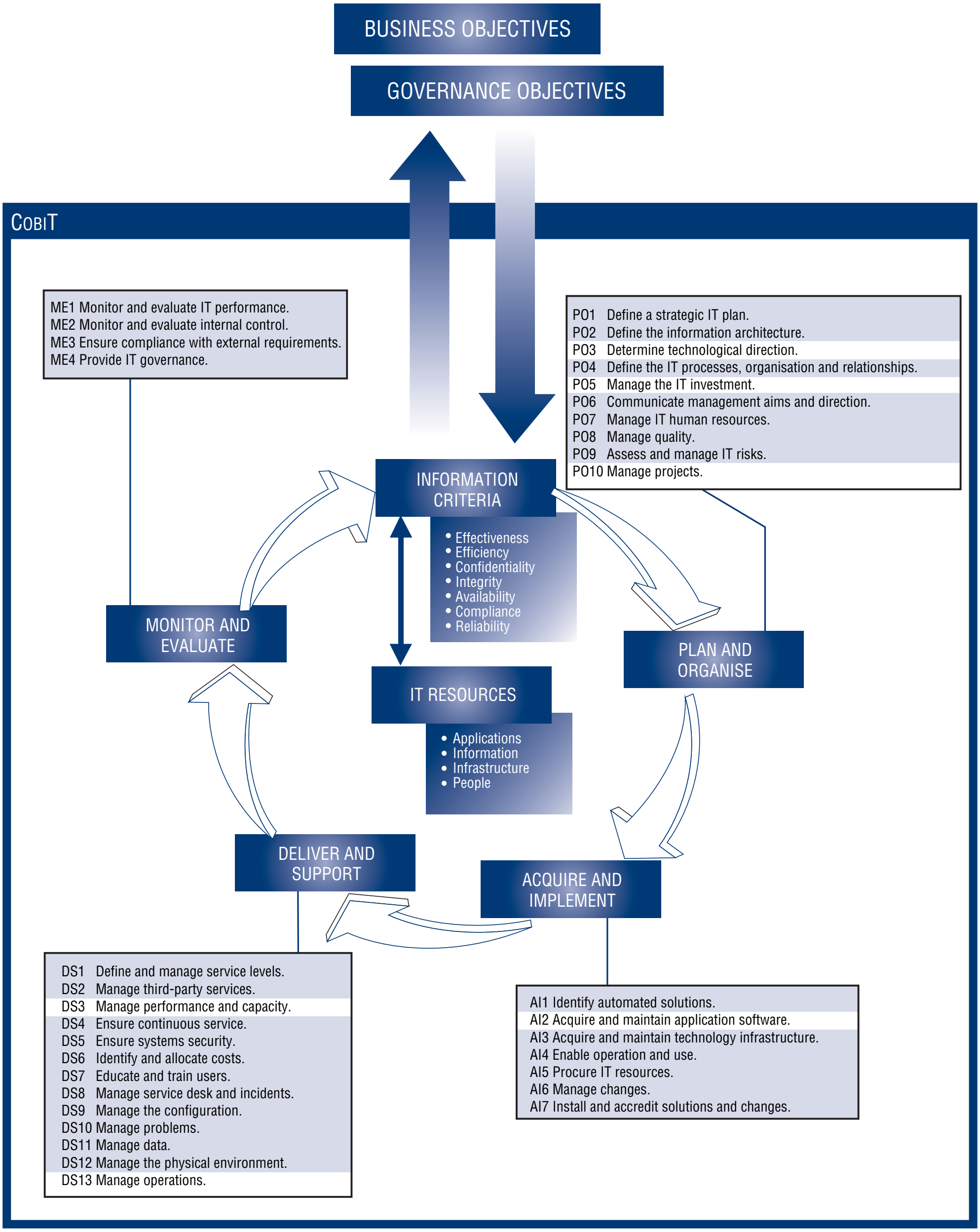
To help an organisation focus on the most essential information security steps, the most important security-related objectives have been extracted from the COBIT framework and are presented in this book. They are shaded in the diagram in **figure 3**. The diagram consists of the COBIT framework process model, which consists of 34 generic IT processes grouped into four domains—Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME).

The tables in **figures 4** through **7** provide key control objectives and suggested minimum control steps, cross-referenced to the COBIT processes and COBIT control objectives. In total, the tables contain 44 steps toward better information security. **Figures 4** through **7** also note related control objectives in ISO/IEC 27002:2005. The references to the ISO 27002 standard show that the baseline aligns with the standard and also provides links to further guidance.

The cross-referencing to COBIT provides links to more detailed generic guidance on each of the 44 key control objectives that can be tailored for IT security. In addition, *COBIT Control Practices, 2nd Edition* provides further implementation advice.

In addition to the specific COBIT control objectives, the process control (PC) objectives merit special notice. They are defined on page 14 of the COBIT 4.1 framework, and outline good practices that apply to all IT-related processes, including those that are security-related. It is worthwhile to consider how the PCs can best be achieved in any particular user environment.

Figure 3—COBIT Control Objectives



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

Figure 4—Plan and Organise

Control Objective	Control Step	ISO/IEC 27002:2005	COBIT 4.1
Define the security strategy and the information architecture.			
Identify information and services critical to the enterprise and consider their security requirements.	1. Based on the business impact for critical business processes, identify: • Critical data—Data that must not be misused or lost • Services that need to be available • Transactions that must be trusted (to be authenticated and have integrity) Consider the security requirements: • Do confidential data need to be protected against disclosure? • Who is authorised to access and modify data? • Are data retention and backup procedures required? • What are the availability requirements? • What are the authorisation and verification requirements for electronic transactions? Develop a business case for important security investments. Define appropriate technology standards for security-related hardware and software.	4.1, 4.2, 5.1, 7.2	**PO1:** 1.2, 1.4, 1.6 **PO2:** 2.2, 2.3 **PO3:** 3.4 **PO4:** 4.9 **DS5:** 5.1, 5.2
Define the IT organisation and relationships.			
Define and communicate information security responsibilities.	2. Define specific responsibilities for the management of information security and: • Ensure that responsibilities are assigned, communicated and properly understood. • Evaluate the risk of concentrating too many security roles and responsibilities in one person. • Provide the resources required to exercise responsibilities effectively.	6.1, 10.1	**PO4:** 4.8, 4.10, 4.11, 4.15 **PO7:** 7.3 PC4
Communicate management aims and direction.			
Define and communicate management aims and directions with respect to information security.	3. Consistently define, communicate and regularly discuss the basic rules for meeting security requirements and responding to security incidents. Establish minimum requirements and communicate these on a regular basis, reminding employees of security risks and their personal responsibilities. Establish staff awareness of the requirement for the timely reporting of suspected security incidents. Make sure that security directions are in line with the business objectives.	5.1, 6.1, 10.8, 11.3, 13.2	**PO6:** 6.2, 6.3, 6.4, 6.5 **DS5:** 5.2

Figure 4—Plan and Organise (*cont.*)

Control Objective	Control Step	ISO/IEC 27002:2005	COBIT 4.1
Manage IT human resources.			
Ensure that security functions are staffed properly with people who possess the necessary skills to fulfil the role.	4. When hiring, verify skills using reference and background checks.	8.1	**PO7:** 7.6
	5. Obtain through hiring or training the skills needed to support the enterprise security requirements. Verify annually whether skills and qualifications are up to date, and act accordingly.	8.1	**PO7:** 7.1, 7.2
	6. Ensure that no key security task is dependent upon a single resource.	10.1	**PO4:** 4.13 **PO7:** 7.5
	7. Define information security-related performance measures for employees.	8.2	**PO7:** 7.7
Assess and manage IT risks.			
Discover, prioritise, and either contain or accept relevant information security risks.	8. Regularly discuss with key staff (from business and IT management) where and when security problems can adversely impact business objectives and how to protect against them.	4.1	**PO2:** 2.3 **PO9:** 9.1, 9.2, 9.3, 9.4
	9. Prepare a risk management action plan to address all risks according to business risk.	4.2	**PO9:** 9.5, 9.6
	10. Establish staff understanding of the need for responsiveness and consider cost-effective means to manage the identified security risks through security controls (e.g., backup, access control, virus protection, firewalls) and insurance coverage.	4.1, 4.2, 6.1, 8.2	**PO7:** 7.4 **PO9:** 9.5 **AI1:** 1.1, 1.2

Figure 5—Acquire and Implement

Control Objective	Control Step	ISO/IEC 27002:2005	COBIT 4.1
Identify automated solutions.			
Consider security when identifying, automated solutions.	11. When acquiring automated and third-party solutions, ensure that a full security evaluation is completed.	12.1, 12.2, 12.5	**AI1:** 1.1, 1.2, 1.3 **AI5:** 5.2, 5.3, 5.5
	12. Ensure that the solutions are functional and that operational security requirements are specified and compatible with current or planned systems. Determine the trustworthiness of the selected security technology/service through references, external advice, contractual arrangements, etc.	12.1, 12.5	**AI1:** 1.1, 1.2 **AI2:** 2.2, 2.4 **AI4:** 4.1, 4.4 **AI5:** 5.3, 5.4
Acquire and maintain application and technology infrastructure.			
Consider security when acquiring and maintaining the technology infrastructure.	13. Challenge suppliers and developers to ensure that the application and technology infrastructure properly support security requirements in a consistent manner.	9.2, 12.1, 12.4	**PO8:** 8.3 **AI2:** 2.3, 2.4, 2.5, 2.6, 2.8 **AI3:** 3.1, 3.4
	14. Document which additional security measures are needed to protect the technology infrastructure itself.	11.4, 11.5	**AI3:** 3.2
	15. Identify and monitor sources for keeping up to date with security patches, and implement those appropriate for the enterprise infrastructure.	12.6	**AI3:** 3.3 **AI6:** 6.1 **DS5:** 5.9
Enable operation and use.			
Consider security when enabling operational use.	16. Ensure that staff members know how to integrate security in day-to-day procedures. Document procedures and train staff members on security matters.	8.2, 10.1	**AI4:** 4.1, 4.2, 4.3, 4.4 **AI7:** 7.1
Manage changes.			
Ensure that all changes, including patches, support enterprise objectives and are carried out in a secure manner. Ensure that day-to-day business processes are not impacted.	17. Evaluate all changes, including patches, to establish the impact on the integrity, exposure or loss of sensitive data, availability of critical services, and validity of important transactions. Based on this impact, perform adequate testing prior to making the change.	10.1, 10.3, 12.5	**AI2:** 2.8 **AI3:** 3.4 **AI6:** 6.1, 6.2 **AI7:** 7.2, 7.4, 7.6
	18. Record and authorise all changes, including patches and emergency changes (although authorisation of emergency changes may occur after the change is applied).	12.5	**AI6:** 6.2, 6.3, 6.4, 6.5

Figure 5—Acquire and Implement (*cont.*)

Control Objective	Control Step	ISO/IEC 27002:2005	COBIT 4.1
Install and accredit solutions and changes.			
Ensure that all new systems and changes are accepted only after sufficient testing of security functions.	19. Test the system (or major change) against functional and operational security requirements in a fully representative environment. Testing should include how the security functions integrate with existing systems. Do not test on the live production system or use personally identifiable information. Make sure that not only are test systems separated from operational systems, but also that the underlying data are separated. Be aware that test environments often have less security.	10.3, 12.5	**PO8:** 8.3 **AI3:** 3.4 **AI7:** 7.2, 7.4, 7.6, 7.8
	20. Perform final security acceptance by evaluating all test results against business goals and security requirements, involving key staff members who will use, run and maintain the system.	10.3, 12.5	**AI7:** 7.7, 7.8, 7.9

Figure 6—Deliver and Support

Control Objective	Control Step	ISO/IEC 27002:2005	COBIT 4.1
Define and manage service levels.			
Define and manage security aspects of service levels.	21. Ensure that management establishes security requirements and regularly reviews compliance of internal service level agreements and contracts with third-party service providers.	6.2, 10.2, 15.2	**AI5:** 5.2 **DS1:** 1.3, 1.5, 1.6 **DS2:** 2.4
Manage third-party services.			
Manage security aspects of third-party services.	22. Assess the professional capability of third parties, and ensure that they provide a contact person who possesses the authority to act upon enterprise security requirements and concerns.	6.2, 10.2	**AI5:** 5.3 **DS2:** 2.3, 2.4
	23. Consider the enterprise's dependence on third-party suppliers for security requirements, and mitigate continuity, confidentiality and intellectual property risk by implementing such measures as escrow, legal liabilities, penalties and rewards.	6.2	**DS2:** 2.3
	24. Consider including in agreements the right to audit and perform SysTrust, SAS 70, ISA402 or other third-party reviews.	15.2	**ME2:** 2.6

Figure 6—Deliver and Support (*cont.*)

Control Objective	Control Step	ISO/IEC 27002:2005	COBIT 4.1
Ensure continuous service.			
Ensure that the enterprise is capable of carrying on its day-to-day automated business activities with minimal interruption from a security incident.	25. Identify critical business functions and information and the resources (e.g., applications, third-party services, supplies, data files) that are critical to support them. Provide for availability of these resources to maintain continuous service in the event of a security incident.	4.1, 4.2, 10.3, 13.2, 14.1	**PO2:** 2.3 **PO9:** 9.3, 9.4 **DS4:** 4.1, 4.3 **DS5:** 5.6 **DS10:** 10.1, 10.2, 10.3 **DS12:** 12.5
	26. Establish basic principles for safeguarding and reconstructing IT services, including identifying alternative processing arrangements and determining how to obtain supplies and services in an emergency, how to return to normal processing after the security incident, and how to communicate with customers and suppliers.	14.1	**DS4:** 4.2, 4.4, 4.8
	27. Together with key employees, define what needs to be backed up and stored offsite to support recovery of the business (e.g., critical data files, documentation, other IT resources) and secure it appropriately. At regular intervals, ensure that the backup resources are usable and complete.	7.2, 10.5, 14.1	**DS4:** 4.5, 4.9 **DS11:** 11.5, 11.6
	28. Control access and access privileges to services based on the individual's business requirement to view, add, change or delete information and transactions. Control access rights of service providers, suppliers and customers.	11.1, 11.2	**DS5:** 5.3, 5.4
	29. Ensure that responsibility is identified, documented and allocated to manage all user accounts and security tokens (e.g., passwords, cards, devices). Periodically review/confirm the actions and authority of those managing user accounts.	10.1, 11.2	**DS5:** 5.4, 5.7, 5.8 **DS13:** 13.4
	30. Log important security violations (e.g., unauthorised system and network access, virus, misuse, illegal software). Ensure that they are reported immediately and acted upon in a timely manner.	10.10, 13.1, 15.1	**DS5:** 5.5, 5.6, 5.9 **DS10:** 10.1
	31. To ensure that counterparties can be trusted and transactions are authentic and non-repudiable when using electronic transaction systems, ensure that the security instructions with trading partners are adequate and compliant with contractual obligations.	6.2, 10.8, 10.9, 12.3	**DS5:** 5.11 AC6
	32. Enforce the use of virus protection software and anti-spyware throughout the enterprise's infrastructure, and maintain up-to-date virus definitions.	10.4	**DS5:** 5.9

Figure 6—Deliver and Support (*cont.*)

Control Objective	Control Step	ISO/IEC 27002:2005	COBIT 4.1
Ensure continuous service (*cont.*).			
	33. Define a policy for what information can come into and go out of the organisation, and configure the network security systems accordingly. Consider how to protect physically transportable storage devices. Monitor exceptions and follow up on significant incidents.	9.2, 10.8, 10.9, 11.4, 12.4	**DS5:** 5.2, 5.10, 5.11 **DS12:** 12.3
Manage the configuration.			
Ensure that all onfiguration items are appropriately secured and security risks minimised by ensuring the enterprise's awareness of its IT-related assets and licences.	34. Ensure that there is a regularly updated and complete inventory of the IT hardware and software configuration.	7.1	**DS9:** 9.1, 9.2, 9.3
	35. Regularly review whether all installed software is authorised and licenced properly. Use only legal software.	7.1, 15.2	**DS9:** 9.3
Manage data.			
Ensure that all data remain complete, accurate and valid during input, processing, storage and distribution.	36. Subject data to a variety of controls to check for integrity (accuracy, completeness and validity) during input, processing, storage and distribution. Control transactions to ensure their authenticity and that they cannot be repudiated.	10.8, 11.6, 12.2	**DS5:** 5.11 **DS11:** 11.6 **AC1, AC2, AC3, AC4, AC5, AC6**
	37. Distribute sensitive output only to authorised individuals.	10.8	**DS11:** 11.6 **AC5, AC6**
	38. Define retention periods, archival requirements and storage terms for input and output documents, data, and software. Ensure that they comply with user and legal requirements.	7.2, 10.7, 15.2	**DS11:** 11.2, 11.4
	39. While in storage, check continuing integrity, accessibility and readability of the data.	9.2, 10.7	**DS4:** 4.9 **DS11:** 11.2
Manage the physical environment.			
Protect all IT equipment from damage.	40. Physically secure the IT facilities and assets (e.g.,data rooms), especially those most at risk to a security threat.	9.1, 9.2	**DS12:** 12.1, 12.2, 12.3, 12.4, 12.5
	41. Physically protect computer equipment, including mobile and storage devices, from damage, theft and accidental loss.	9.1, 9.2 12.3, 12.5	**DS12:** 12.2,

Figure 7—Monitor and Evaluate

Control Objective	Control Step	ISO/IEC 27002:2005	COBIT 4.1
Monitor and evaluate IT performance—assess internal control adequacy.			
Regularly monitor the performance of information security.	42. Have key staff members regularly: • Assess adequacy of security controls compared to defined requirements and in light of current vulnerabilities • Reassess what security exceptions need to be monitored on an ongoing basis • Evaluate how well the security mechanisms are operating and check for weaknesses by using such measures as intrusion detection, penetration and stress testing, and testing of contingency plans • Document all violations and exceptions and ensure that they are acted upon in accordance with the security policy • Monitor compliance of security key controls	4.1, 10.10, 15.2	**ME1:** 1.2, 1.4, 1.5, 1.6 **ME2:** 2.1, 2.4
Obtain independent assurance.			
Gain confidence and trust in security through reliable and independent sources.	43. Obtain competent external resources to review the information security control mechanisms, and assess compliance with laws, regulations and contractual obligations relative to information security. Leverage their knowledge and experience for internal use.	15.3	**ME2:** 2.5 **ME4:** 4.7
Ensure regulatory compliance.			
Ensure that information security functions comply with applicable laws, regulations and other external requirements.	44. Identify tasks and activities required to comply with security obligations including privacy; intellectual property rights; and other legal, regulatory, contractual and insurance requirements. Educate staff members on being responsive to their security obligations.	15.1	**PO3:** 3.3 **ME3:** 3.1, 3.2, 3.3, 3.4

5. INFORMATION SECURITY SURVIVAL KIT 1—HOME USERS

SPECIFIC INFORMATION SECURITY RISKS FOR HOME USERS

The following examples show how home users can be exposed to information security risks:

- Being unaware of the dangers of using the Internet
- Introducing faulty or unreliable software with security weaknesses
- Using of old and out-of-date operating systems, security software and/or application software, such as browser and e-mail software, increasing the probability of system crashes and lost data
- Being exposed to pornography and other undesirable media
- Allowing uncontrolled use by children, friends, etc.
- Using home computers for business activities, thereby exposing corporate information to new hazards
- Being exposed to information and identity theft through viruses, spyware, spam, phishing and other attacks

HOME USERS SURVIVAL KIT

Home users can range from those with virtually no technical knowledge to those who may be more advanced but not necessarily aware of all the security issues. Two lists of basic precautions have been provided to guide this wide range of individuals (**figures 8** and **9**).

Figure 8—Security Precautions for Nontechnical Home Users

☑ Obtain guidance from qualified and reputable advisors (certified technicians) from time to time to ensure that the computer installation has no significant security flaws.

☑ If you depend on computers to do business, sign up for onsite support and ensure the availability of an on-call facility should anything go wrong.

☑ Obtain reputable security software. Protection packages can be obtained from all PC software dealers that include all the main functions necessary, e.g., antivirus, spyware, firewall and content filtering. If needed, use a specialist to ensure proper installation.

☑ Sign up for automatic updates and maintenance on the security software to ensure that the protection is current and up to date.

☑ Do not open unknown e-mail attachments, and be aware that e-mail addresses can be faked. Let the security software check all e-mails and follow the advice given by the tool.

☑ Install only official, up-to-date operating systems, security software and applications; avoid installing anything that is not needed.

☑ Turn off the computer or disconnect it from the network when it is not in use.

☑ Make regular backups of data on removable media and store them away from the computer.

Figure 8—Security Precautions for Nontechnical Home Users (*cont.*)

☑ If you use the Internet for business or personal reasons, such as shopping, use only reputable suppliers and web sites. Do not provide more personal or company information than is truly needed.

☑ Avoid storing any sensitive data on a laptop or personal digital assistant (PDA), including cell phones and Blackberries, and be careful not to leave the devices in places where they can be stolen. If available, use encryption software.

☑ If you are working from home, consult the company's system support personnel to ensure that enterprise security rules are followed.

☑ To be comfortable about children's interaction with the Internet, consider putting the family computer in open view, using site and content filters and consulting parental advice sites.

☑ Talk with children about some of the hazards that may affect them when using the Internet, and about acceptable use of the Internet.

☑ If you have real concerns about children's use of the computer, ask for specialist advice.

☑ If you suspect something has gone wrong or the machine is behaving in an unexpected way, call a specialist advisor to check the system. Remember that 'pulling the plug' can and will stop any attack. Wait for the specialist advisor before plugging it back in.

The home user with more technical experience should use all the basic precautions listed in **figure 8**, as well as the precautions in **figure 9**.

Figure 9—Security Precautions for Technically Competent Home Users

☑ If you need to open an unknown e-mail attachment, save it and scan it with antivirus software—and possibly disconnect from the network—before opening.

☑ Do not run programs of unknown origin, however appealing they may be. If you are considering sending them on to others, be aware that they may contain malicious software. Use freeware with caution.

☑ Make a boot disk/CD-ROM/DVD to recover from security breaches and other failures if the computer is damaged or compromised.

☑ Do not receive, use or pass on illegal software or viruses, and remember that you can be held accountable for inappropriately passing on sensitive, proprietary or personal information. Use familiar, recommended or trusted sites for e-shopping, and provide personal details only when truly needed.

☑ If you recieve what you suspect to be a spoofed e-mail from someone with malicious intent, contact the service provider's support personnel immediately.

☑ If you are working from home and suspect security problems on the computer, consult the enterprise system support personnel to ensure that the enterprise's security rules are followed. If you are using a laptop or PDA that contains sensitive data, consider installing security software and encrypting the data to provide added protection.

☑ Configure wireless networks properly and ensure that access is managed correctly.

6. INFORMATION SECURITY SURVIVAL KIT 2—PROFESSIONAL USERS

SPECIFIC INFORMATION SECURITY RISKS FOR PROFESSIONAL USERS

The following examples show how professional users can be exposed to information security risks:
- Being unaware of corporate security policies and procedures, and personal responsibilities
- Inadequately appreciating the value of corporate information
- Sharing access with colleagues or friends
- Mixing business computing with home computing
- Using laptops, handheld devices and other computer media when out of the office

PROFESSIONAL USERS DOS AND DON'TS

Figures 10 and **11** list the dos and don'ts for professional users.

Figure 10—Dos for Professional Users

DO:

☑ Understand personal responsibility with regard to information security and maintain knowledge of corporate policies on software usage, network/Internet usage of antivirus software, and anti-spyware usage.

☑ Keep informed about the established security rules, apply them and, if unclear, seek guidance. Since this is a changing environment, keep continually informed.

☑ Be aware of the types of security incidents that can and do occur.

☑ Report security incidents and concerns about:
- Access violations
- Inadequate backups
- System unavailability
- Poorly controlled or error-prone electronic transactions
- Equipment issues, such as unknown origin, broken equipment, etc.

☑ Make regular backups of critical data and periodically test the backups to ensure that data can be restored

☑ Change passwords immediately upon receipt and then regularly in accordance with policy. Ensure that the chosen password is difficult to guess and meets established best practices for length, complexity, unacceptable names, etc.

☑ Lock rooms and check the desktop when leaving important data or equipment behind.

☑ Remember that anything written in an e-mail may be held against the writer or his/her enterprise and that this evidence can be kept forever

☑ Dispose of sensitive information effectively—shred, wipe disks, destroy media, etc.

☑ Return all company materials, including data files, upon termination of employment.

Figure 11—Don’ts for Professional Users

Do not:

☒ Use enterprise computing resources for unapproved purposes (e.g., intellectual property protection violations, illegal content)

☒ Leave the system unattended and accessible for extended periods of time

☒ Tell anyone your password or share any other authentication token with anyone (except properly authorised group passwords)

☒ Disclose sensitive data to anyone who is not authorised to receive them or who does not need to know them

☒ Load or use pirated software or unqualified shareware onto any enterprise computer

☒ Bypass established network connection rules

☒ Bypass or uninstall virus checking software, virus recovery software, anti-spyware or other security enabling software

☒ Ignore security incidents

☒ Neglect sensitive information in your care (on portable media, e.g., CDs, DVDs, flash/pen media, PDAs, laptops)

☒ Introduce and/or remove computing equipment without authorisation

7. INFORMATION SECURITY SURVIVAL KIT 3—MANAGERS

SPECIFIC INFORMATION SECURITY RISKS FOR MANAGERS

The following examples show how managers can be exposed to information security risks:

- Failing to recognise the significance and impact of security breaches
- Being unaware of security risks
- Failing to give direction
- Failing to monitor activities of staff
- Failing to identify incidents and/or notice security weaknesses
- Relying on technical security alone and neglecting the risks arising from people and process issues

MANAGERS CHECKLIST

Figure 12 contains an extensive (yet non-comprehensive) list of the most important conditions managers should check to avoid risks and satisfy minimum security objectives. Review this in conjunction with implementing the security baseline in chapter 4.

Figure 12—Conditions to Check

☑ Ensure that responsibilities relating to information security and the security dos and don'ts are clearly defined.

☑ Ensure that staff members have sufficient resources and skills to exercise their security responsibilities.

☑ Ensure that security is considered in job performance appraisals and results in appropriate rewards and disciplinary measures.

☑ Ensure awareness of the need to protect information.

☑ Provide training to operate information systems securely.

☑ Respond to suspected and actual security incidents.

☑ Ensure that security is an integral part of the systems development life cycle (SDLC) process and explicitly addressed during each phase of the process.

☑ Ensure that staff members with sensitive roles have been vetted.

☑ Ensure that the organisation is not dependent on one individual for any key security task (i.e., appropriate segregation of duties). Consider cross-training as a way to further ensure this.

☑ Ensure that privacy and intellectual property rights, as well as other legal, regulatory, contractual and insurance requirements, have been identified with respect to security and processes in your area of responsibility.

☑ Ensure that applicable security measures have been identified and implemented (e.g., effective backup, basic access control, virus detection and protection, firewalls, intrusion detection, insurance coverage).

☑ Ensure that a suitable technical environment is in place to support security measures.

Figure 12—Conditions to Check (*cont.*)

☑ Ensure that staff members know how security measures operate and have integrated them in day-to-day procedures.

☑ Ensure that key users have safely and regularly tested security measures in a representative environment.

☑ Establish rules for assessing and authorising changes and for evaluating their security impact.

☑ Ensure that security aspects have been considered in all service level agreements (SLAs) and the security competence of the service providers has been assessed.

☑ Ensure that risks of dependency on security service providers have been assessed and mitigated.

☑ Ensure that on-call support, backup, resilience and continuity have been established for IT services supporting critical business functions.

☑ Ensure that users know what to do in case critical IT services are unavailable.

☑ Ensure that appropriate access control and connectivity rules for internal and external users have been implemented, based on business needs and risks.

☑ Ensure that security administration has been enabled and resourced with procedures and service levels to identify users and assign, activate, maintain and eventually remove access rights.

☑ Ensure that incident management procedures are defined and in effect to ensure that relevant security incidents (access control violations, viruses, illegal use of software, hacking, etc.) are identified, monitored, analysed and acted upon.

☑ Ensure that the security baseline and vulnerabilities have been constantly assessed through monitoring system weaknesses, such as intrusion detection, penetration and stress testing, and testing of contingency plans.

☑ Ensure that there is a measurable and management-transparent security strategy based on benchmarking, maturity models, gap analysis, and continuous performance monitoring and reporting.

☑ Ensure that security guidance and contractual obligations for e-commerce and electronic payments exist and are frequently reviewed for appropriateness, new threats and risks.

☑ Ensure that an up-to-date list of hardware and software critical for important IT services is maintained, including the disaster backup site.

☑ Ensure that archiving and backup procedures for critical information have been defined and implemented.

☑ Ensure that important computing equipment is safe from theft, damage or loss, e.g., put cables on laptops, lock computer rooms and know the location of media devices.

☑ Ensure that applying a high level of control has hardened all security and critical server and communications platforms.

☑ Ensure that operating system versions have been continuously kept up to date.

☑ Ensure that physical and environmental protections (e.g., for heat, dust or electricity) are in place.

☑ Ensure that adequate security has been implemented for wireless communications systems and is monitored continuously.

☑ Where appropriate, ensure that competent external resources have reviewed the information security control mechanisms and assessed compliance with laws, regulations and contractual obligations relative to information security. Leverage their knowledge and experience, and act upon their suggestions.

☑ Ensure that clear, pragmatic enterprise and technology continuity programmes have been established and are periodically tested and kept up to date.

Figure 12—Conditions to Check (*cont.*)

☑ Ensure that critical business processes and supporting infrastructures are periodically reassessed and made resilient to failure, especially targeting single points of failure.

☑ Ensure that the usage of computers is monitored for compliance with established rules of appropriate usage.

☑ Ensure that the organisation has been kept informed of new threats (e.g., viruses) and has been included in regular risk assessments.

☑ Ensure that mobile computing devices have been included in the security strategy and have been protected. For example:

- Laptops, PDAs (including cell phones and Blackberries), etc., are protected from theft and physical damage, and stored data are protected from disclosure
- Portable media (e.g., optical, memory) are protected

8. Information Security Survival Kit 4—Executives

SPECIFIC INFORMATION SECURITY RISKS FOR EXECUTIVES

The following examples show how executives can be exposed to information security risks:
- Failing to appreciate which risks are most significant
- Failing to communicate the right security culture and control framework
- Failing to delegate responsibilities for risk management at all levels
- Failing to detect where security weaknesses exist within the organisation
- Failing to monitor risk management activities to ensure compliance with policy
- Failing to implement ongoing information security risk management practices

EXECUTIVES QUESTIONS AND ACTIONS

This survival kit, as well as the survival kits for senior executives (CEOs) and boards of directors, contains two tables (**figures 13** and **14**):
- A questionnaire—Questions that should be asked that may help executives understand whether they are on the right track with regard to information security governance
- An action list—Specific actions to be taken collectively by executives

Figure 13—Questions to Ask

☑ When was the last risk assessment completed on the criticality of information security assets? Are risk assessments that involve business users undertaken as needed?

☑ Does the risk assessment consider the impact on the entity's ability to operate if the critical information is unavailable, corrupted, inappropriately compromised or lost? Does it cover the consequences of a security incident in terms of lost revenues, customers and investor confidence? Does it determine what the consequences would be if the infrastructure became inoperable? Does it speak to the interrelationships between the critical components of the infrastructure?

☑ Does the risk assessment consider what information assets are subject to laws and regulations? Does it result in adequate procedures to assure compliance with these laws and regulations?

☑ Is the information security risk assessment a regular agenda item at IT management meetings, and does management follow through with improvement initiatives?

☑ What are other people doing, and how is the enterprise placed in relation to them? What is industry best practice, and how does the enterprise compare?

Figure 13—Questions to Ask (*cont.*)

☑ When was the latest policy statement issued on information security? Does this policy statement adequately cover:
- The critical information security assets
- The importance placed on information security by the board and management (tone at the top)
- The identified risks
- The control mechanisms established to address these risks
- The monitoring and feedback procedures
- The frequency with which this policy is reviewed

☑ When was the last performance review made of the person responsible for information security (i.e., the information security officer)? Is the process to keep management informed on security issues by the information security officer adequate? Does the process encourage knowledgeable contributions and actions, or does it 'shoot the messenger'?

☑ What safeguards have been established over systems connected to the Internet to protect the entity from loss, damage and/or disclosure affecting critical assets and systems (such as through malicious software, intrusions and denial-of-service attacks)? Are the systems being actively monitored, and is management kept informed of the results?

☑ What information security awareness training has been established, and does it appear adequate considering the assessed risks? Does it reach all parties involved in IT? Is it given periodically to all staff members?

☑ What safeguards have been established over the physical security of computer assets, and do they appear adequate?

☑ When was the last time an information security audit was performed? Does management track its own progress on recommendations?

☑ Is there a security programme (i.e., staff, budget, tangible resources) in place that covers all of the above questions? Is there clear accountability about who carries it out, and has the function's location within the management hierarchy been identified?

☑ Are regular analyses performed on the number and type of incidents affecting the organisation? Are improvements implemented to reduce the likelihood and/or consequence of future incidents?

Figure 14—Action List

☑ Set up and execute a risk management programme that identifies threats, analyses vulnerabilities, assesses criticality and uses industry best practices for due care.

☑ Define and implement a security framework that consists of standards, measures, practices and procedures. Develop clear policies and detailed guidelines, supported by a repetitive and assertive communications plan that reaches every employee.

☑ Ensure that a measurable and management-transparent security strategy is created based on benchmarking, maturity models, gap analysis and continuous performance reporting.

☑ Ensure that the information security strategy pragmatically measures risks and seeks to cost-effectively mitigate risk at an acceptable level with minimal business disruptions.

☑ Review the security strategy and update it at least annually or more frequently when significant business changes require. Take into consideration interrelationships between physical and information security.

☑ Conduct a periodic executive risk brainstorming session, prepared by security and audit professionals (internal and external), resulting in actionable conclusions that are followed up on until closure. Invite the security officer.

Figure 14—Action List (*cont.*)

☑ Develop what-if scenarios on information security and risk, leveraging the knowledge of specialists.

☑ Regularly assess vulnerabilities through monitoring system weaknesses using security alert service bulletins and vendor bulletins, intrusion and stress testing, and testing of contingency plans. Ensure that a business continuity plan exists and has been regularly tested.

☑ Ensure that critical business processes and supporting infrastructures are resilient to failure and are periodically reviewed and reassessed. Especially target single points of failure.

☑ Establish security baselines and rigorously monitor compliance.

☑ Run security responsiveness programmes, security audits and assessments, including frequent penetration and continuity tests.

☑ Ensure that security incidents are investigated and resolved in a timely manner, with root causes identified and weaknesses corrected. Apply forensic methods, such as systems control, co-ordination with law enforcement, and data collection and analysis.

☑ Ensure that information security fits in the organisation's risk, IT governance or corporate governance framework:
- Effective security is not only a technology problem; it is also a business issue.
- Related risk management must address the corporate culture, management's security consciousness and actions.

☑ Make available a record of information, services and transactions that are critical to the enterprise.

☑ Define a high-level approach to:
- Who may access and modify data
- What data retention and backup are needed
- How to maintain service availability
- How to authorise and verify electronic transactions

☑ Base authorisations on business rules and match the authentication method to the business risk.

☑ Ensure that information security is part of the overall business life cycle.

9. INFORMATION SECURITY SURVIVAL KIT 5—SENIOR EXECUTIVES

SPECIFIC INFORMATION SECURITY RISKS FOR SENIOR EXECUTIVES

The following examples show how senior executives can be exposed to information security risks:

- Failing to appreciate what risks are most significant
- Failing to mandate the right security culture and control framework and set the right security example
- Failing to embed responsibilities for risk management into the management team
- Failing to detect where the most critical security weaknesses exist within the organisation
- Failing to monitor risk management investments and/or be able to measure benefits realised
- Failing to direct risk management and be in a position to know what residual risk remains

SENIOR EXECUTIVES QUESTIONS AND ACTIONS

Figures 15 and **16** list questions to ask and actions to take for senior executives.

Figure 15—Questions to Ask

☑ How is the board kept informed of information security issues? When was the last briefing made to the board on security risks and the status of security improvements?

☑ Is the enterprise clear on its position relative to information security risks? Does it tend toward risk avoidance or risk taking, and is this consistent with the enterprise's overall approach to risk?

☑ How much is being spent on information security? On what? How were the expenditures justified? What projects were undertaken to improve security last year? Have sufficient resources been allocated?

☑ How many staff members had security training last year, and in what subjects? How many of the management team members received security training?

☑ How does the organisation detect security incidents? How are they escalated, and what does management do about them? Is management prepared to recover from a major security incident? Are proper safeguards in place to ensure correct handling of forensic data if required?

☑ Is management confident that security is adequately addressed in the organisation? Can members of management readily produce verifiable data to prove it? Has the organisation ever had its network security checked by a third party?

☑ Is management aware of the latest information security issues and good practice(s)?

☑ What is industry good practice, and how does the enterprise compare?

☑ Are information security issues considered when developing business and IT strategy?

Figure 15—Questions to Ask (*cont.*)

☑ Can the entity continue to operate properly if critical information is unavailable, corrupted, inappropriately compromised or lost? What would be the consequences of a security incident in terms of lost revenues, customers and investor confidence? What would be the consequences if the infrastructure became inoperable?

☑ Which information assets are subject to laws and regulations? What has management instituted to assure compliance with the laws and regulations?

☑ Does the information security policy address the concerns of the board and management on information security (tone at the top), cover identified risks, establish an appropriate infrastructure to manage and control the risks, and establish appropriate monitoring and feedback procedures? Is it periodically reviewed and reassessed (at least annually)?

☑ Is there a security programme in place that covers all of the above questions? Is there clear accountability about who carries it out?

Figure 16—Action List

☑ Establish a security organisation and function that assists management in the development of policies and assists the enterprise in carrying them out.

☑ Assign responsibility, accountability and authority for all security-related functions to appropriate individuals in the organisation.

☑ Establish clear, pragmatic enterprise and technology continuity programmes, which are then continually tested and kept up to date.

☑ Conduct information security audits based on a clear process and accountabilities, with management tracking the closure of recommendations.

☑ Include security in job performance appraisals, and apply appropriate rewards and disciplinary measures.

☑ Develop and introduce clear and regular reporting on the organisation's information security status to the board of directors based on the established policies, guidelines and applicable standards. Report on compliance with these policies, important weaknesses and remedial actions, and important security projects.

☑ Ensure effective co-ordination amongst all of the organisation's security and risk management functions.

10. INFORMATION SECURITY SURVIVAL KIT 6—BOARD OF DIRECTORS/TRUSTEES

SPECIFIC INFORMATION SECURITY RISKS FOR BOARD MEMBERS

The following examples show how boards of directors/trustees can be exposed to information security risks:

- Being unaware of risk exposures
- Being unaware of legal and regulatory requirements
- Failing to understand the impact of security failures on the business and the potential effect on stakeholders, share prices, competition, etc.
- Being unable to monitor management's performance in managing security risks
- Failing to set the tone at the top with regard to the importance of security
- Failing to judge the value of security investment proposals

DIRECTORS AND TRUSTEES QUESTIONS AND ACTIONS

Figures 17 and **18** list questions to ask and actions to take.

Figure 17—Questions to Ask

☑ When was the last time management got involved in security-related decisions? How often does management get involved in progressing security solutions?

☑ Does management know who is responsible for security? Does the responsible individual know? Does everyone else know?

☑ Does anyone know how many information and communications technology (ICT) assets the company owns? Would anybody know if some went missing?

☑ Has management identified all information (customer data, strategic plans, research results, etc.) that would cause embarrassment or competitive disadvantage if it was leaked?

☑ How many incidents did the organisation experience in the last year? What was the cause and effect? Is an analysis undertaken to reduce the likelihood and/or consequence of future incidents?

☑ Does anyone know how many people are using the organisation's systems? Does anyone know what those people are allowed to do, or what they are doing on these systems?

☑ Is security considered an afterthought or a prerequisite during business strategy and planning activities?

☑ What would be the consequences of a serious security incident in terms of lost revenues, lost customers and investor confidence?

☑ Has management set up an independent audit of information security? Does management track its own progress on recommendations?

Figure 18—Action List

☑ Set direction:
- Define cultural values related to risk awareness.
- Drive policy and strategy.
- Define a global risk profile.
- Set priorities.

☑ Assign responsibilities to management.

☑ Insist that management make security investments and security improvements measurable, and monitor and report on programme effectiveness.

☑ Ensure that the board and/or audit committee clearly understand their roles in information security and how they will work with management and auditors.

☑ Ensure that internal and external auditors agree with the board and/or audit committee and management on how information security should be covered in the audit.

☑ Require a report of security progress and issues for the board and/or audit committee.

☑ Develop crisis management practices, involving executive management and the board of directors, from agreed-upon thresholds onward.

11. Summary of Technical Security Risks

Figures 19 through **21** contain a summary of technical security risks.

INTENTIONAL MISUSE OF THE COMPUTER

Figure 19—Computer Misuse Security Risks

Trojan horse programs

Trojan horse programs are a common way for intruders to trick the user (a process sometimes referred to as social engineering) into installing 'back door' programs, which can allow intruders to easily access the user's computer without his/her knowledge, change the system configurations or infect the computer with a computer virus.

Back door and remote administration programs

On computers using a Windows operating system, intruders commonly use three tools—BackOrifice, Netbus and SubSeven—to gain remote access to the computer. Once installed, these back door or remote administration programs allow other people to access and control the computer. The CERT[1] vulnerability note about BackOrifice should be reviewed. Other computer platforms may be vulnerable, and the user needs to monitor vulnerability reports and maintain the system.

Denial-of-service attacks

A denial-of-service (DoS) attack causes the computer to crash or to become so busy processing data that the legitimate user is unable to use it. In most cases, the latest patches will prevent the attack.

Being an intermediary for another attack

Intruders frequently use compromised computers as launching pads for attacking other systems. The use of distributed denial-of-service (DDoS) tools is an example of this. The intruders will install an 'agent' (frequently through a Trojan horse program) that runs on the compromised computer, awaiting further instructions. Then, when many agents are running on different computers, a single 'handler' can instruct all of them to launch a DoS attack on another system. Thus, the end target of the attack is not the original user's computer, but someone else's; the original user's computer is just a convenient tool in a larger attack.

Unprotected Windows networking shares

Intruders can exploit unprotected Windows networking shares in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but also is a threat to other sites on the Internet.

Mobile code (Java/JavaScript/ActiveX)

There have been reports of problems with 'mobile code' (e.g., Java, JavaScript and ActiveX). These programming languages let web developers write code that is executed by the organisation's web browser. Although such code is generally useful to the organisation, intruders also use it to gather information (such as which web sites the user visits) or run malicious code on the computer. It is possible to disable Java, JavaScript and ActiveX in the web browser, but the user should be aware that this may limit legitimate browser functionality. Also, the user should be aware of the risks involved in the use of mobile code within e-mail programs. Many e-mail programs use the same code as web browsers to display HTML. Thus, vulnerabilities that affect Java, JavaScript and ActiveX are often applicable to e-mail and web pages.

[1] See Chapter 12, References, for more information.

Figure 19—Computer Misuse Security Risks (*cont.*)

Cross-site scripting

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form or a database inquiry. Later, when the web site responds, the malicious script is transferred to the browser. This can potentially expose the web browser to malicious scripts by:

- Following links in web pages, e-mail messages or newsgroup postings without knowing where they link
- Using interactive forms on an untrustworthy site
- Viewing online discussion groups, forums or other dynamically generated pages where users can post text containing HTML tags

E-mail spoofing

E-mail spoofing is when an e-mail message appears to have originated from one source when it actually was 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 a password). Spoofed e-mail can range from harmless pranks to social engineering ploys. Examples of the latter 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 account if they do not comply
- E-mail claiming to be from a person in authority requesting users to send a copy of a password file or other sensitive information

E-mail-borne viruses

Viruses and other types of malicious code are often spread as attachments to e-mail messages. Before opening any attachments, the user should be aware of the source of the attachment. It is not enough that the e-mail originated from a recognised address. For example, the Melissa virus spread precisely because it originated from a familiar address. Also, malicious code might be distributed in amusing or enticing programs. Many recent viruses use these social engineering techniques to spread. Examples include W32/Sircam and W32/Goner.

Hidden file extensions

Windows operating systems contain an option to hide file extensions for known file types. The option is enabled by default, but a user may choose to disable this option to have file extensions displayed by Windows. Multiple e-mail-borne viruses are known to exploit hidden file extensions. The first major attack that took advantage of a hidden file extension was the VBS/LoveLetter worm that contained an e-mail attachment named LOVE-LETTER-FOR-YOU.TXT.vbs. Other examples include Downloader (MySis.avi.exe or QuickFlick.mpg.exe), VBS/CoolNote (COOL_NOTEPAD_ DEMO.TXT.vbs) and VBS/OnTheFly (AnnaKournikova.jpg.vbs). The files attached to the e-mail messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types, when in fact the file is a malicious script or executable (.vbs or .exe).

Chat clients

Internet chat applications, such as instant messaging applications and Internet relay chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialogue, web URLs and, in many cases, files of any type. Because many chat clients allow for the exchange of executable code, they present risks similar to those of e-mail clients. As with e-mail clients, the chat clients' ability to execute downloaded files should be limited. As always, the user should be wary of exchanging files with unknown parties.

Figure 19—Computer Misuse Security Risks (*cont.*)

Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. These data may include usernames, passwords and proprietary information that travels over the network in cleartext. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access. Relative to DSL and traditional dial-up users, cable modem users have a higher risk of exposure to packet sniffers, since entire neighborhoods of cable modem users are effectively part of the same local area network (LAN). A packet sniffer installed on any cable modem user's computer in a neighborhood may be able to capture data transmitted by any other cable modem in the same neighborhood.

Identity theft

An imposter obtains key pieces of information, such as someone's US Social Security number, driver's license number or any other personal data, and uses it for personal gain.

Tunneling

Tunneling is the transfer of data within a private or corporate network through a public network, e.g., employees working at home, using a VPN connection to connect to the corporate network over the Internet. If not properly set up, someone could get access to the home PC via the Internet and get unauthorised access to the corporate network via the VPN.

Zombies

Automatic programs search for systems that are connected to the Internet but are unprotected, take them over without the owner's knowledge, and use them for malicious purposes.

Spyware

Innocent-looking software (e.g., P2p-agent software used in popular peer-to-peer communications software) can include or hide software that collects information about the system and the user, and can send this information to third parties without the legitimate user knowing.

Spamming

The process of sending unsolicited or unwanted e-mails (generally in very large numbers) to unsuspecting recipients

Phishing

A form of social engineering, generally conducted via e-mail. The target is tricked into releasing confidential information (account numbers, passwords, trade data, etc.) by answering a false request from a company or agency.

Inappropriate or accidental data disclosure

A disclosure where the data themselves are not affected, but are revealed (inadvertently or maliciously) to an unauthorised party

Physical theft

Physical theft of a computer, of course, results in loss of confidentiality and availability, and (assuming the computer is ever recovered) makes the integrity of the data stored on the disk suspect. Regular system backups (with the backups stored somewhere away from the computer) allow for recovery of the data, but backups alone cannot address confidentiality. Cryptographic tools are available that can encrypt data stored on a computer's hard disk.

VIOLATION OF RULES AND REGULATIONS

Figure 20—Violations of Rules and Regulations

Intellectual property

Compliance with all software licence agreements should be ensured. In addition, intellectual property law will protect other forms of media, and care should be taken to respect these rights.

Decent use of the Internet

The Internet allows access to unlimited information, including sources that are considered indecent or sometimes outright illegal. Such use of the Internet is discouraged in both a working environment and a private home.

Industrial espionage

Data and information that are not well protected or that are inappropriately or accidentally disclosed may allow competitors to spy upon the user's information.

Rules and regulations

The use of information systems is, depending on the country, state or industry, subject to a number of rules and regulations. These need to be known and obeyed. Domains covered by such rules include privacy, retention of information, minimal system protection requirements and attestation requirements.

ACCIDENTS

Figure 21—Accidents

Disk failure

Availability is one of the three key elements of information. Although all stored data can become unavailable—if the media they are stored on is physically damaged, destroyed or lost—data stored on hard disks are at higher risk due to the mechanical nature of the device. Hard disk crashes are a common cause of data loss on personal computers.

Power failure and surges

Power problems (e.g., surges, blackouts and brownouts) can cause physical damage to a computer, inducing a hard disk crash or otherwise harming the electronic components of the computer. Common mitigation methods include using surge suppressors and uninterruptible power supplies (UPS).

Software problems

One of the most common problems when using computers is software, i.e., software not performing in a stable or predictable manner or not performing up to expectations or specifications. End users carry little responsibility here, but manufacturers and developers do.

12. REFERENCES

More information on the subject of information security can be obtained in the following references.

GENERAL INFORMATION SECURITY AND IT GOVERNANCE STANDARDS AND FRAMEWORKS

American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants, 'Trust Services—WebTrust and SysTrust', USA and Canada, 2000

Business Industry Advisory Council/International Chamber of Commerce, 'Information Security Assurance for Executives: An International Business Commentary on the 2002 OECD Guidelines for the Security of Networks and Information Systems: Towards a Culture of Security', France, 22 April 2003

Business Roundtable, 'Building Security in the Digital Resource: An Executive Resource', USA, November 2002

Business Roundtable, 'Information Security Addendum to Principles of Corporate Governance', USA, announced April 2003

Government Accountability Office, *Federal Information System Controls Audit Manual*, USA, January 1999

Glaessner, Thomas; Tom Kellermann; Valerie McNevin; 'Electronic Security: Risk Mitigation in Financial IT Transactions', The World Bank, June 2002

Heinman, Don; 'Public Sector Information Security: A Call to Action for Public-sector CIOs', IBM Endowment for the Business of Government, USA, October 2002

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

Information Systems Security Association (ISSA), 'The Generally Accepted Information Security Principles (GAISP)', USA, in preparation

Institute of Internal Auditors, 'Information Security Governance: What Directors Need to Know', USA, 2001

Institute of Internal Auditors, National Association of Corporate Directors, American Institute for Certified Public Accountants, ISACA, 'Information Security Management and Assurance: A Call to Action for Corporate Governance,' USA, 2000

International Chamber of Commerce, *ICC Handbook on Information Security Policy for Small to Medium Enterprises*, France, 11 April 2003

International Federation of Accountants, 'International Information Technology Guidelines—Managing Security of Information', Information Technology Committee, USA, January 1998

International Information Security Foundation, 'Generally Accepted System Security Principles', USA, Fall 2000

International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), *Code of Practice for Information Security*, ISO/IEC 17799, Switzerland, 5 May 2003

International Organisation for Standardisation (ISO), British Standards Institute*, Information Technology—Guidelines for the Management of Information Security—Part 5: Management Guidance on Network Security*, ISO TR 13335-5, UK, 2001

Internet Security Alliance, *Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices*, *1st Edition*, USA, July 2002

IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003

IT Governance Institute, COBIT *Quickstart*, USA, September 2003

IT Governance Institute, COBIT 4.1, USA, 2007

IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, *2nd Edition*, USA, 2006

IT Governance Institute, *IT Control Objectives for Sarbanes Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting*, *2nd Edition,* USA, 2006

IT Governance Institute, *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*, USA, September 2007

National Association of Corporate Directors, 'Information Security Oversight: Essential Board Practices,' USA, December 2001

National Cyber Security Partnership, *Information Security Governance: A Call to Action, Corporate Governance Task Force Report*, April 2004

National Institute of Standards and Technology (NIST), *Automated Information Security Program Review Areas*, USA, 27 July 2002

NIST, *Building an Information Technology Security Awareness and Training Program,* SP 800-50, USA, 2003

NIST, *Federal Information Processing Standards* (FIPS), USA, 1999

NIST, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, SP 800-14, USA, 1996

NIST, *Guide for Assessing the Security Controls in Federal Information Systems*, SP 800-53A, USA, 2006

NIST, *Guide for Developing Security Plans for Information Technology Systems*, SP 800-18, USA, 1998

NIST, *Guide for Mapping Types of Information and Information Systems to Security Categories*, SP 800-60 Draft, USA, 2004

NIST, *Guide for the Security Certification and Accreditation of Federal Information Systems*, SP 800-37, USA, 2004

NIST, *An Introduction to Computer Security*, SP 800-12, USA, 1995

NIST, *Recommended Security Controls for Federal Information Systems*, SP 800-53 Draft, USA, 2003

NIST, *Recommended Security Controls for Federal Information Systems*, SP 800-53, USA, 2006

NIST, *Risk Management Guide for Information Technology Systems*, SP 800-30, USA, 2002

NIST, *Security Considerations in the Information System Development Life Cycle*, SP 800-64, USA, 2003

NIST, *Security Metrics Guide for Information Technology Systems*, SP 800-55, USA, 2003

NIST, *Security Self-assessment Guide for Information Technology Systems*, SP 800-26, USA, 2001

Office of Government Commerce, *Information Technology Infrastructure Library* (ITIL), UK, 2001

Organisation of Economic Co-operation and Development, 'OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security', France, adopted 25 July 2002

The Technology Network (TechNet), 'TechNet Corporate Information Security Evaluation for CEOs', USA, *www.technet.org/cybersecurity*

US Congress, 'Federal Information Security Management Act of 2002 (FISMA)', USA, 2002

GENERAL INFORMATION SECURITY WEB SITES

Center for Secure Information Systems, *csis.gmu.edu*

Computer Security Institute, *www.gocsi.com*

Computer Security Resource Center, *csrc.ncsl.nist.gov*

Information Technology Security Evaluation Facility (ITSEF), *www.commoncriteria.nl*

Institute of Electrical and Electronics Engineers Inc., *www.ieee.org*

Internet Engineering Task Force, *www.ietf.org*

Internet Society, *www.isoc.org/internet/issues/security*

ISACA, *www.isaca.org*

IT Governance Institute, *www.itgi.org*

Security of Telecommunication and Information Systems, *www.cordis.lu/infosec/src/crit.htm*

Systems Security Engineering—Capability Maturity Model, *www.sse-cmm.org*

The Open Group, *www.opengroup.org/security*

US Department of Homeland Security, *www.nipc.gov*

TECHNICAL INFORMATION SECURITY GUIDANCE

ActiOnline, *www.antionline.com*

Anonymizer, *www.anonymizer.com*

Anti-Phishing Working Group. *www.antiphishing.org*

Astalavista Group, *www.astalavista.com*

Attrition.org, *www.attrition.org*

AuditNet, *www.auditnet.org*

Australian Computer Emergency Response Team, *www.auscert.org.au*

Beyond-Security's SecuriTeam, *www.securiteam.com*

The Biometric Consortium, *www.biometrics.org*

Bitdefender, *www.bitdefender.com/html/free_tools.php*

Bundesamt für Sicherheit in der Informationstechnik., *www.bsi.bund.de/english/documents.htm*

The Center for Education and Research in Information Assurance and Security, *www.cerias.purdue.edu/tools_and_resources/hotlist*

Center for Information Technology, National Institutes of Health, *www.alw.nih.gov/Security/security-docs.html*

Center for Internet Security, *www.cisecurity.org*

The Complete, Unofficial TEMPEST Information Page, *www.eskimo.com/%7Ejoelm/tempest.html*

CERT, *www.cert.org*

The Communications Security Establishment and the National Cryptologic Program, *www.cse.dnd.ca*

Computer Security Resource Center, *csrc.ncsl.nist.gov*

Computer Security Resource Center for NIST, *csrc.nist.gov/*

Cult of the Dead Cow, *www.cultdeadcow.com*

Cyber Criminals Most Wanted, *www.ccmostwanted.com*

Disaster-Resource.com, *www.disaster-resource.com*

eBCVG.com, *www.ebcvg.com*

Eindhoven University of Technology, FTP Archive of the Mathematics and Computing Science Dept., *ftp.win.tue.nl*

Firewall.cx, *www.firewall.cx*

Generally Accepted System Security Principles (GASSP), The International Information Security Foundation (I2SF), *web.mit.edu/security/www/gassp1.html*

Google Security Categories, *directory.google.com/Top/Computers/Security*

hackerthreads.org, *www.hackerthreads.org/phpbb*

HackerWhacker, *www.hackerwhacker.com*

High-Tech Crime Network, *www.htcn.org*

The Honeynet Project, *project.honeynet.org*

Information Security Forum, *www.securityforum.org*

The Information Warfare Site, *iwar.org.uk*

Institute for Security and Open Methodologies, *www.isecom.org*

Internet Security Glossary, *ftp://ftp.isi.edu/in-notes/rfc2828.txt*

ISACA, *www.isaca.org*

IT Governance Institute, *www.itgi.org*

Linux Security, *www.linuxsecurity.com*

Microsoft Security, *www.microsoft.com/security*

Microsoft Security Center, *www.nwnetworks.com/iesc.html*

Redbooks, *www.redbooks.ibm.com*

The Risks Digest, *http://catless.ncl.ac.uk/Risks*

SANS (SysAdmin, Audit, Network, Security) Institute, *www.sans.org*

Security D2D.com, *www.securityd2d.com*

Security Tracker, *securitytracker.com*

Softlinkers, *www.softlinkers.org*

SunSolve, *http://sunsolve.sun.com*

A Survey of Selected Computer Policies From Institutions of Higher Education, *www.brown.edu/Research/Unix_Admin/cuisp*

TechNet, *http://technet.org*

Uberhacker II, *www.happyhacker.org*

US Computer Crime and Intellectual Property Section of the Criminal Devision, Department of Justice, *www.cybercrime.gov*

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

US Department of Energy Computer Incident Advisory Capability, *ciac.llnl.gov/ciac/index.html*

US Department of Energy Computer Incident Advisory Capability, Hoaxbusters, *http://hoaxbusters.ciac.org*

US Defense Information Systems Agency, Information Assurance Support Environment, *http://iase.disa.mil*

US Federal Computer Incident Response Center (FedCIRC), *www.fedcirc.gov*

US National Institute of Standards and Technology (NIST) ICAT Metabase of Computer Vulnerabilities, *http://icat.nist.gov/icat.cfm*

US National Security Agency Security Recommendation Guides, *nsa1.www.conxion.com/index.html*

US National Security Institute, *www.nsi.org*

W3C (World Wide Web Security) Security Domain, *www.w3.org/Security*

Wardriving.com, *www.wardriving.com*

Wilders.org, *www.wilders.org*

WindowSecurity, *www.windowsecurity.com*

WindowSecurity, Network Security Library, *www.secinf.net*

Zone h, *www.zone-h.org*

INFORMATION SECURITY NEWS

Compsec online, www.compseconline.com

Computerworld, www.computerworld.com/securitytopics/security

Disaster Recovery Journal, www.drj.com

Information Security, infosecuritymag.techtarget.com

InfoSec News, www.c4i.org/isn.html

SC Magazine, www.infosecnews.com

SearchSecurity.com, TechTarget, searchsecurity.techtarget.com

SecurityFocus, www.securityfocus.com

SecurityNews.net, www.securitynews.net

Security magazine, www.securitymagazine.com

TechWeb, www.techweb.com/tech/security

Windows & .Net magazine, www.secadministrator.com

APPENDIX—COBIT AND RELATED PRODUCTS

The COBIT framework, in versions 4.0 and higher, includes all of the following:
- Framework—Explains how COBIT organises IT governance, management and control objectives, and good practices by IT domains and processes, and links them to business requirements
- Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
- Control objectives—Provide generic best practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- Maturity models—Provide profiles of IT processes describing possible current and future states

In the years since its inception, COBIT's core content has continued to evolve, and the number of COBIT-based derivative works has increased. Following are the publications currently derived from COBIT:
- *Board Briefing on IT Governance, 2nd Edition*—Designed to help executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- COBIT Online—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, benchmarking, and a discussion facility for sharing experiences and questions.
- *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the *IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition*.
- *IT Assurance Guide: Using COBIT*—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
- *IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition*—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and a supporting tool kit
- *COBIT Quickstart, 2nd Edition*—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
- COBIT *Security Baseline: An Information Security Survival Kit, 2nd Edition*—Focuses on essential steps for implementing information security within the enterprise

- COBIT Mappings—Currently posted at *www.isaca.org/downloads*:
  - *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*
  - *COBIT Mapping: Overview of International IT Guidance, 2nd Edition*
  - *COBIT Mapping: Mapping of CMMI® for Development V1.2 With COBIT 4.0*
  - *COBIT Mapping: Mapping of ISO/IEC 17799:2000 With COBIT, 2nd Edition*
  - *COBIT Mapping: Mapping of ISO/IEC 17799:2005 With COBIT*
  - *COBIT Mapping: Mapping of ITIL With COBIT 4.0*
  - *COBIT Mapping: Mapping of PMBOK® With COBIT 4.0*
  - *COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0*
  - *COBIT Mapping: Mapping of SEI's CMM for Software With COBIT 4.0*
  - *COBIT Mapping: Mapping of TOGAF 8.1 With COBIT 4.0*

- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*—Presents information security in business terms and contains tools and techniques to help uncover security-related problems

Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:
- *Enterprise Value: Governance of IT Investments—The Val IT Framework*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as do COBIT's control objectives.
- *Enterprise Value: Governance of IT Investments—The Business Case*, which focuses on one key element of the investment management process
- *Enterprise Value: Governance of IT Investments—The ING Case Study*, which describes how a global financial services company manages a portfolio of IT investments in the context of the Val IT framework

For the most complete and up-to-date information on COBIT; Val IT; and related products, case studies, training opportunities, newsletters and other framework-specific information, visit *www.isaca.org/cobit* and *www.isaca.org/valit*.

IT GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*