CISM Review Questions, Answers & Explanations Manual 2006

Information Systems
Audit and Control
Association®

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

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

Disclosure

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Phone: +1.847.253.1545
Web sites: www.isaca.org

ISBN 1-933284-39-0
CISM Review Questions, Answers & Explanations Manual 2006
Printed in the United States of America

PREFACE

ISACA is pleased to offer this 200 questions, answers and explanations manual. The purpose of this manual is to provide the CISM candidate with sample questions and testing topics to help prepare and study for the CISM examination.

The material for this manual consists of 200 multiple-choice study questions, answers and explanations, which are arranged in the same proportion as the CISM job practice. These questions, answers and explanations are intended to introduce CISM candidates to the types of questions that appear on the CISM examination. They are not actual questions from the exam. Questions are sorted by CISM content areas and a sample test of 200 questions is also provided in the same proportion as the actual CISM examination. Sample questions contained in this manual are provided to assist the understanding of the material in the *CISM Review Manual 2006* and to depict the type of question format typically found on the CISM exam.

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

ISACA wishes you success with the CISM examination. Your commitment to pursuing the leading certification for information security managers is exemplary, and for this reason, we welcome your comments and suggestions on the use and coverage of this manual. At the end, you will find a feedback questionnaire. After the examination is over, please take a moment to complete and mail this questionnaire back to ISACA. Your observations will be invaluable as new questions, answers and explanations are prepared.

TABLE OF CONTENTS

INTRODUCTION

OVERVIEW

This manual consists of 200 multiple-choice questions, answers and explanations. These questions are selected and provided in two formats.

Questions Sorted by Content Area
Questions, answers and explanations are provided (sorted) by CISM content areas. This allows the CISM candidate to study material by content area and refer to specific questions to evaluate comprehension of the topics covered within each content area. These questions are representative of CISM questions, although they are not actual test items. They are intended to provide the CISM candidate with an understanding of the type and structure of question that would typically appear on the examination.

Sample Test
The 200 questions are also provided as a sample test. Candidates are urged to use this sample test and the answer sheet provided to simulate an actual examination. Many candidates use this exam as a pre-test to determine their own specific strengths or weaknesses, or as a final exam. Sample exam answer sheets have been provided for both uses. In addition, a sample exam answer/reference key is included. These sample test questions have been cross-referenced to the questions, answers and explanations by area, so it is convenient to refer to the explanations of the correct answers. This publication is ideal to use in conjunction with the *CISM Review Manual 2006*.

It should be noted that the *CISM Review Questions, Answers & Explanations Manual 2006* has been developed to assist a CISM candidate to study and prepare for the CISM examination. As you use this publication to prepare for the examination, please note that it covers a broad spectrum of information security management issues. Do not assume that reading and working the questions in this manual will fully prepare you for the examination. Since examination questions often relate to practical experiences, a CISM candidate is cautioned to refer to his/her own experiences and to other publications referred to in the *CISM Review Manual 2006*. These additional references are an excellent source of further detailed information and clarification. It is recommended that candidates evaluate the job content areas in which he/she feels weak or requires a further understanding, and study accordingly. Also, please note that this publication has been written using standard American English.

TYPES OF QUESTIONS ON THE CISM EXAM

CISM exam questions are developed with the intent of measuring and testing practical knowledge and the application of general concepts and standards. As previously mentioned, all questions are multiple choice and are designed for one best answer.

The candidate is cautioned to read each question carefully. Many times a CISM examination question will require the candidate to choose the appropriate answer that is **MOST** likely or **BEST**. Or, a candidate may be asked to choose a practice or procedure that would be performed **FIRST** related to the other answers. In every case, the candidate is required to read the question carefully, eliminate known wrong answers and then make the best choice possible. Knowing that these types of questions are asked and how to study to answer them will go a long way toward answering them correctly.

Every CISM question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario or description also may be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. Please note that questions requiring the candidate to choose one to several items from a list are not used on the CISM examination and should not be used as a study source.

Another condition a candidate should consider when preparing for the examination is to recognize that information security is a global profession, and individual perceptions and experiences may not reflect the more global position or circumstance. Since the examination and CISM manuals are written for the international information security community, a candidate will be required to be somewhat flexible when reading a condition that may be contrary to a candidate's experience. It should be noted that CISM examination questions are written by experienced information security managers from around the world. Each question on the exam is reviewed by ISACA's CISM Test Enhancement Committee and CISM Certification Board, which consist of international members. This geographical representation ensures that all test questions are understood equally in every country and language.

These review manuals are living documents. As technology advances, these manuals will be updated to reflect such advances. Any suggestions to enhance the materials covered herein, or reference materials, should be directed to:

Mail: **ISACA**
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Attention: Certification Department
Phone: +1.847.253.1545, ext. 484
Fax: +1.847.253.1443
E-mail: *efernandez@isaca.org*

QUESTIONS, ANSWERS AND EXPLANATIONS BY AREA

T1 INFORMATION SECURITY GOVERNANCE

T1-1 Which of the following should be the **FIRST** step in developing an information security strategy?

A. Perform a technical vulnerabilities assessment.
B. Analyze the current business strategy.
C. Perform a business impact analysis.
D. Assess the current levels of security awareness.

B Prior to assessing technical vulnerabilities or levels of security awareness, an information security manager needs to gain an understanding of the current business strategy and direction. A business impact analysis should be performed prior to developing a business continuity plan, but this would not be an appropriate first step in developing an information security strategy.

T1-2 Senior management commitment and support for information security can **BEST** be obtained through presentations that:

A. use illustrative examples of successful attacks.
B. explain the technical risks to the organization.
C. evaluate the organization against best practices.
D. tie security risks to key business objectives.

D Senior management needs to understand the business justification for investing in security. This can best be accomplished by tying security to key business objectives. Senior management will not be as interested in technical risks or examples of successful attacks. Industry best practices are important to senior management, but not as important as key business objectives.

T1-3 The **MOST** appropriate role for senior management in supporting information security is the:

A. evaluation of vendors offering security products.
B. assessment of risks to the organization.
C. approval of policy statements and funding.
D. monitoring of adherence to regulatory requirements.

C Since senior management is ultimately responsible for information security, they should approve major policy statements and requests to fund the information security practice. Evaluation of vendors, assessment of risks and monitoring compliance with regulatory requirements are day-to-day responsibilities of the information security manager.

T1-4 Which of the following would **BEST** indicate the success of information security governance within an organization?

A. The steering committee approves all security projects.
B. The security policy manual is distributed to all managers.
C. Security procedures are accessible on the company intranet.
D. The corporate network utilizes multiple screened subnets.

A The existence of a steering committee that approves all security projects would be an indication of the existence of a good governance program. The mere availability of policies and procedures does not ensure that they are current. A corporate network may utilize good security practices, but this is not governance.

T1-5 Information security governance is **PRIMARILY** driven by:

A. technology constraints.
B. regulatory requirements.
C. litigation potential.
D. business strategy.

D Governance is directly tied to the strategy and direction of the business. Technology constraints, regulatory requirements and litigation potential are all secondary.

T1-6 Which of the following are mandatory rules and regulations?

A. Policies
B. Procedures
C. Standards
D. Best practices

C Standards are authoritative rules and regulations. Policies are high-level statements of objectives. Procedures are how-to guidance that is meant to instruct. Best practices indicate ideal methods of implementation.

T1-7 Which of the following represents the major focus of privacy regulations?

A. Data mining
B. Penetration testing
C. Supplier data
D. Customer data

D Customer data have been a major focus of recent privacy regulation. Data mining is an accepted tool for *ad hoc* reporting. Penetration testing is not normally associated with privacy issues. Supplier data are not likely to involve privacy issues.

T1-8 Investments in information security technologies should be based on:

A. a vulnerability assessment.
B. a value analysis.
C. the business climate.
D. audit recommendations.

B Investments in security technologies should be based on a value analysis and a sound business case. Demonstrated value should take precedence over the current business climate. Basing decisions on audit recommendations would be reactive in nature. Vulnerability assessments are useful, but they do not determine whether or not the cost is justified.

T1-9 Which of the following should be developed **FIRST**?

A. Standards
B. Procedures
C. Policies
D. Guidelines

C Policies are high-level statements of objectives and, therefore, should be developed first. Policies are the foundation for the development of standards, guidelines and procedures.

T1-10 Retention of business records should be based **PRIMARILY** on:

A. business strategy and direction.
B. regulatory and legal requirements.
C. storage capacity and longevity.
D. business case and value analysis.

B Retention of business records is generally driven by legal and regulatory requirements. Business strategy and direction would not normally apply nor would they override legal and regulatory requirements. Storage capacity and longevity are important but secondary issues. Business case and value analysis would be secondary to complying with legal and regulatory requirements.

T1-11 Owners of information should be responsible for its:

A. classification.
B. protection.
C. recoverability.
D. availability.

A Information owners are responsible for the classification of data. Classification determines the degree to which data are protected and restricted. Protection, recoverability and availability should be the responsibility of the custodians of information (information technology).

T1-12 Which of the following is characteristic of centralized information security management?

A. More expensive to administer
B. Better adherence to policies
C. More aligned with business unit needs
D. Faster turnaround of requests

B Centralization of information security management results in greater uniformity and better adherence to security policies. It is generally less expensive to administer due to the economies of scale; however, turnaround can be slower due to the lack of alignment with business units.

T1-13 The likelihood of successfully implementing information security governance will be minimized if there is a lack of:

A. security awareness training.
B. updated security polices.
C. a computer incident management team.
D. senior management support.

D Without senior management support, it would be difficult to obtain the necessary funding and aid required to implement information security governance. Although the other choices are important issues, they are secondary to obtaining senior management support.

T1-14 Which of the following individuals would be in the **BEST** position to sponsor the creation of an information security steering group?

A. Chief security officer
B. Chief operating officer
C. Chief internal auditor
D. Chief legal counsel

B The chief operating officer is more highly placed within the organization and has the most knowledge of business operations and objectives. The chief internal auditor and chief legal counsel are appropriate members of such a steering group; however, sponsoring the creation of the steering committee should be initiated by someone versed in the strategy and direction of the business. Since the chief security officer is looking to this group for direction, he/she is probably not in the best position to oversee formation of this group.

T1-15 The **MOST** important component(s) of a privacy policy is/are:

A. notifications.
B. warranties.
C. liabilities.
D. geographic coverage.

A Privacy policies must contain notifications and opt-out provisions. They do not necessarily address warranties, liabilities or geographic coverage.

T1-16 The cost of implementing a security control should not exceed the:

A. annualized loss expectancy.
B. cost of an incident.
C. expected benefits.
D. opportunity costs.

C The cost of implementing security controls should not exceed the overall expected benefits nor should the cost to protect an asset exceed the worth of the asset. Annualized loss expectancy represents the losses that are expected to happen during a single calendar year, and a security mechanism may cost more than this amount (or the cost of a single incident) and still be considered cost-effective. Opportunity costs relate to revenue lost by forgoing the acquisition of an item or the making of a business decision.

T1-17 What will **BEST** tie information security to business objectives?

A. Value analysis
B. Security metrics
C. Deliverables list
D. Process improvement model

A Value analysis can be used to illustrate the value proposition of how information security supports the achievement of business objectives. Security metrics measure improvement within the security practice but do not tie it to business objectives. Similarly, listing deliverables and creating process improvement models does not tie information security to business objectives.

T1-18 When a security standard conflicts with a business objective, the situation should be resolved by:

A. changing the security standard.
B. enforcing the security standard.
C. performing a risk analysis.
D. allowing an exception to the standard.

C Conflicts of this type should be based on a risk analysis of the costs and benefits of allowing or disallowing an exception to the standard.

T1-19 Minimum standards for securing the technical infrastructure should be defined in the security:

A. strategy.
B. guidelines.
C. model.
D. architecture.

D Minimum standards for securing the technical infrastructure should be defined in a security architecture document. This document defines how components are secured and the security services that should be in place. A strategy is a broad, high-level document. A guideline is advisory in nature. A security model shows the relationships between components.

T1-20 Which of the following would normally **NOT** be covered in an insurance policy for computer equipment coverage?

A. Equipment leased to another company by the insured
B. Equipment leased to the insured by another company
C. Equipment under the direct control of the insured
D. Equipment purchased on an installment plan

A For coverage to apply, the insured must have direct control of the equipment. If the insured leases computer equipment to another company, then that company is responsible for obtaining insurance coverage. Computer equipment can be insured if purchased or leased under an installment plan.

T1-21 The **MOST** inappropriate reporting base for the information security management function would be to report to the:

A. director of financial management.
B. risk management director.
C. business division manager.
D. infrastructure director.

D Placing security management under the infrastructure director would present a conflict of interest, since the goals and objectives of the infrastructure manager could be in opposition to those of the information security manager. Risk management would, on the other hand, be a good fit, while placement under the director of financial management or a business division manager would ensure that security is properly aligned with business strategy and direction.

T1-22 Which of the following is **MOST** appropriate for inclusion in an information security strategy?

A. Business controls designated as key controls
B. Security processes, methods, tools and techniques
C. Firewall rule sets, network defaults and IDS settings
D. Budget estimates to acquire specific security tools

B A set of security objectives, processes, methods, tools and techniques together constitute a security strategy. Although IT and business governance are intertwined, business controls will not normally be found in a security strategy. Budgets will generally not be included in an information security strategy. Also, until an information security strategy is formulated and implemented, specific tools will not be identified and specific cost estimates will not be available. Firewall rule sets, network defaults and IDS settings are technical details subject to periodic change and not appropriate content for a strategy document.

T1-23 Senior management commitment and support for information security will be diminished if the information security manager:

A. emphasizes organizational risk above technology risk.
B. establishes a set of organizationwide metrics.
C. emphasizes security needs above organizational needs.
D. explains that each organizational unit must take responsibility.

C Senior management needs to understand that information security exists to help the organization meet its objectives. If the information security manager sets information security needs above organizational needs, this will result in a negative reaction from senior management. Organizational or business risk should always take precedence. Involving each organizational unit in information security and establishing metrics to measure success will be viewed favorably by senior management.

T1-24 For the information security manager, which of the following roles will represent a conflict of interest?

A. Evaluation of third parties requesting connectivity
B. Assessment of the adequacy of disaster recovery plans
C. Final approval of information security policies
D. Monitoring adherence to physical security controls

C Since management is ultimately responsible for information security, it should approve information security policy statements. The information security manager should not have final approval. Evaluation of third parties requesting access, assessment of disaster recovery plans and monitoring of compliance with physical security controls are acceptable practices and do not present any conflict of interests.

T1-25 Which of the following is **MOST** indicative of the failure of information security governance within an organization?

A. The information security department has had difficulty filling vacancies.
B. The information security policy manual is only available in electronic form.
C. The information security oversight committee only meets quarterly.
D. The data center manager has final sign-off responsibility on all security projects.

D A steering committee should be in place to approve all security projects. The fact that the final sign-off for all security projects is the data center manager indicates that a steering committee is not being used and that information security is relegated to a subordinate place in the organization. This tends to indicate a failure of information security governance. For an oversight or steering committee to meet quarterly is not inappropriate. Similarly, having the security policy manual only available electronically may be desirable due to the size of the organization and frequency of updates. Due to the shortage of good qualified information security professionals, difficulty in filling vacancies is not uncommon.

T1-26 Information security priorities may occasionally override:

A. technical requirements.
B. regulatory requirements.
C. privacy requirements.
D. business requirements.

A Information security priorities may occasionally override technical specifications, which then must be rewritten to conform to minimum security standards. Regulatory and privacy requirements are government-mandated and, therefore, not subject to override. The needs of the business should always take precedence in deciding information security priorities.

T1-27 When an organization hires a new information security manager, which of the following goals should this individual pursue first?

A. Develop a security architecture.
B. Build senior management support.
C. Assemble an experienced staff.
D. Interview peer organizations.

B New information security managers should seek to build rapport and establish lines of communication with senior management to enlist their support. Interviewing peer organizations is beneficial to better understand industry best practices, but it is secondary to obtaining senior management support. Similarly, developing a security architecture and assembling an experienced staff are objectives that can be obtained later.

T1-28 It is **MOST** important that an information security architecture be aligned with which of the following?

A. Industry best practices
B. Information technology plans
C. Information security best practices
D. Business objectives and goals

D An information security architecture should always be properly aligned with business goals and objectives. Alignment with IT plans or industry and security best practices are secondary by comparison.

T1-29 Which of the following are **MOST** likely to be discretionary?

A. Policies
B. Procedures
C. Guidelines
D. Standards

C Policies define security goals and expectations for an organization. These are defined in more specific terms within standards and procedures. Standards establish what is to be done while procedures describe how it is to be done. Guidelines provide recommendations that business management must consider in developing practices within their areas of control, and as such, they are discretionary.

T1-30 The chief information security officer (CISO) generally chairs which of the following?

A. The executive steering committee
B. The information technology management committee
C. The enterprise security governance board
D. The service delivery/operations management team

C The CISO generally chairs the enterprise security governance board. The IT management board is chaired by the chief information officer (CIO), the service delivery/operations team by the chief technology officer (CTO) and the executive steering committee by the CIO or chief operating officer (COO).

T1-31 Security technologies should be selected **PRIMARILY** on the basis of their:

A. ability to mitigate audit findings.
B. evaluations in trade publications.
C. use of new and emerging technologies.
D. benefits in comparison to their costs.

D Investments in security technologies should be based on their overall value in relation to their cost. If the value can be demonstrated, this should take precedence over whether they use new or exotic technologies, how they are evaluated in trade publications or if they can resolve certain audit findings.

T1-32 Which of the following are seldom changed in response to technological changes?

A. Standards
B. Procedures
C. Policies
D. Guidelines

C Policies are high-level statements of objectives. Because of their high-level nature and statement of broad operating principles, they are less subject to periodic change.

T1-33 The **MOST** important factor in planning for the long-term retention of electronically stored business records is to take into account potential changes in:

A. storage capacity and shelf life.
B. regulatory and legal requirements.
C. business strategy and direction.
D. application systems and media.

D Long-term retention of business records may be severely impacted by changes in application systems and media. For example, devices that can read 5.25" diskettes or reel-to-reel tapes are rapidly becoming extinct. Similarly, data stored in nonstandard formats that can only be read and interpreted by previously decommissioned applications may be difficult, if not impossible, to recover. Business strategy and direction do not generally apply nor do legal and regulatory requirements. Storage capacity and shelf life are important but are secondary issues.

T1-34 Custodians of information are generally responsible for its:

A. classification.
B. accuracy.
C. recoverability.
D. completeness.

C Information custodians are responsible for the recoverability of information. Classification, accuracy and completeness are generally the responsibility of the information owners.

T1-35 Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

A. More uniformity in quality of service
B. Better adherence to policies
C. More aligned to business unit needs
D. Less total cost of ownership (TCO)

C Decentralization of information security management generally results in better alignment to business unit needs. It is generally more expensive to administer due to the lack of economies of scale. Uniformity in quality of service tends to vary from unit to unit.

T1-36 Which of the following is **MOST** indicative of senior management support of an information security function?

A. Security awareness training is offered.
B. Security polices are reviewed annually.
C. A computer incident management team exists.
D. The security manager reports directly to the chief executive officer (CEO).

D Having the security manager report directly to the CEO provides the best indication that senior management support is strong. Regular access to the CEO gives the information security manager unencumbered access to senior management and strong leverage in making a case for information security. Although the offering of security awareness training, the annual review of security policies and the existence of a computer incident management team are all positive elements, they are secondary in relation to the reporting relationship.

T1-37 Who should be the formal sponsor for the design and implementation of a new security infrastructure in a large global enterprise?

A. Chief security officer (CSO)
B. Chief operating officer (COO)
C. Chief privacy officer (CPO)
D. Chief legal counsel (CLC)

B The COO is more highly placed within the organization and most knowledgeable of business operations and objectives. The CPO and CLC may appear as good choices, but they have the same influence within the organization as the COO. Although the CSO is knowledgeable of what is needed, the sponsor for this task should be someone with far-reaching influence across the organization.

T1-38 The need for privacy policies is **PRIMARILY** driven by which of the following?

A. Customer demands
B. Competitive advantage
C. Threat of lawsuits
D. Regulatory requirements

D Privacy policies are largely driven by laws and regulations imposed by government. Customer demands, threat of lawsuits and any competitive advantage are all secondary issues.

T1-39 The **PRIMARY** goal of information security governance should be to create value through the:

A. review of internal control mechanisms.
B. proactive involvement in business decision making.
C. total elimination of risk factors.
D. instillation of trust among stakeholders.

D The development of trust in the integrity of information among stakeholders should be the primary goal of information security governance. Review of internal control mechanisms relates more to auditing, while the total elimination of risk factors is not practical or possible. Proactive involvement in business decision making implies that security needs dictate business needs, when in fact just the opposite is true.

T1-40 The use of and relationships among security technologies are **BEST** defined through which of the following?

A. Security metrics
B. Network topology
C. Security architecture
D. Process improvement models

C A security architecture explains the use and relationships of security mechanisms. Security metrics measure improvement within the security practice but do not explain the use and relationships of security technologies. Process improvement models and network topology diagrams do not describe the use and relationships of these technologies.

T1-41 A business unit desires to deploy a new technology in a manner that places it in violation of existing information security standards. After discussions with the business unit, they insist on proceeding with the deployment to take advantage of highly desirable market conditions. What immediate action should the information security manager take?

A. Enforce the existing security standard.
B. Change the standard to permit the deployment.
C. Perform a risk analysis to quantify the risk.
D. Permit a 90-day window to see if a problem occurs.

C Resolving conflicts of this type should be based on a sound risk analysis of the costs and benefits of allowing or disallowing an exception to the standard. A blanket decision should never be given without conducting such an analysis.

T1-42 Acceptable levels of information security risk should be determined by:

A. legal counsel.
B. security management.
C. external auditors.
D. senior management.

D Senior management has ultimate responsibility for determining what levels of risk the organization is willing to assume. Legal counsel, the external auditors and even security management are not in a position to make such a decision.

T2 RISK MANAGEMENT

T2-1 Risk mitigation would normally include:

A. assessment.
B. acceptance.
C. evaluation.
D. monitoring.

B Acceptance of a risk is an alternative to be considered in the risk mitigation process. Assessment and evaluation are components of the risk analysis process. Monitoring is a separate process.

T2-2 A risk management program should reduce risk to:

A. zero.
B. an acceptable level.
C. an annualized rate of less than 5 percent of revenue.
D. breakeven with the cost of the program.

B Risk should be reduced to an acceptable level based on the risk preference of the organization. Reducing risk to zero is impractical and could be cost-prohibitive. To tie risk to a percentage of revenue or to the cost of administering the risk program would be inadvisable, since there would be no direct correlation.

T2-3 The **MOST** important reason for conducting the same risk assessment more than once is because:

A. mistakes are often made in the initial reviews.
B. security risks are subject to frequent change.
C. different reviewers will analyze risk factors differently.
D. it shows management that the security staff is adding value.

B Risks are constantly changing. A previously conducted risk assessment will not have measured risks that have been introduced since the last assessment. Although an assessment can never be perfect and will invariably contain some errors, this is not the most important reason for periodic reassessment. Similarly, the fact that different reviewers will analyze risk factors differently is not sufficient. Finally, risk assessments should not be performed merely to justify the existence of the security function.

T2-4 Which of the following **BEST** indicates a successful risk management practice?

A. Overall risk is quantified.
B. Inherent risk is eliminated.
C. Residual risk is minimized.
D. Control risk is tied to business units.

C A successful risk management practice minimizes the residual risk to the organization. In choice A, the fact that overall risk has been quantified does not necessarily indicate the existence of a successful risk management practice. B is incorrect since it is virtually impossible to eliminate inherent risk. In the case of D, although the tying of control risks to business may improve accountability, this is not as desirable as minimizing residual risk.

T2-5 Which of the following would generally have the **MOST** significant negative impact on an organization?

A. Theft of computer software
B. Interruption of utility services
C. Loss of customer confidence
D. Internal fraud resulting in monetary loss

C Although the theft of software, interruption of utility services and internal frauds are all significant, the loss of customer confidence is the most damaging and could cause the business to fail.

T2-6 Which of the following should management use to determine the amount of resources to devote to mitigating exposures?

A. Risk analysis results
B. Audit report findings
C. Penetration test results
D. A fixed percentage of the IT budget

A Risk analysis results are the most useful and complete source of information for determining the amount of resources to devote to mitigating exposures. Audit report findings may not address all risks and will not address annual loss frequency. Penetration test results will provide only a very limited view of exposures while a fixed percentage of the IT budget would be arbitrary and not tied to the exposures faced by the organization.

T2-7 Which of the following will **BEST** protect an organization from internal security attacks?

A. Static IP addressing
B. Internal address translation
C. Prospective employee background checks
D. Employees certifying that they have read policies

C Because past performance is a strong predictor of future performance, background checks of prospective employees would best prevent attacks from originating within an organization. Static IP addressing would do little to prevent an attack from within. Internal address translation using nonroutable addresses is useful against external attacks but not against internal attacks. Employees who certify that they have read security policies are desirable, but this will not guarantee that the employees will behave honestly.

T2-8 The value of a physical asset should be based on:

A. original cost.
B. net cash flow.
C. net present value.
D. replacement cost.

D The value of a physical asset should be based on its replacement cost, as this is the amount that would be needed to replace the asset if it were to become damaged or destroyed. Original cost may be significantly different than the current cost of replacing the asset. Net cash flow and net present value do not accurately reflect the true value of the asset.

T2-9 In a business impact analysis, the value of an information system should be based on the overall:

A. cost to design.
B. cost to re-create.
C. cost if unavailable.
D. value to competitors.

C The value of an information system should be based on the cost that would be incurred if the system were to become unavailable. The cost to design or re-create the system is not as relevant since a business impact analysis measures the impact that would occur if an information system were to become unavailable. Similarly, the value to competitors would not be as relevant.

T2-10 Acceptable risk is achieved when:

A. residual risk is minimized.
B. transferred risk is minimized.
C. control risk equals acceptable risk.
D. residual risk equals transferred risk.

A Residual risk is the risk that remains after putting into place an effective risk management program; therefore, acceptable risk will be achieved when this amount is minimized. Transferred risk is risk that has been assumed by a third party. Accordingly, choices B and D are incorrect since transferred risk does not necessarily indicate whether risk is at an acceptable level.

T2-11 The value of information assets is **BEST** determined by:

A. individual business managers.
B. business systems developers.
C. information security management.
D. peer companies' industry averages.

A Individual business managers will be in the best position to determine the value of information assets, since they are most knowledgeable of the asset's impact on the business. Business systems developers and information security managers would not be as knowledgeable of the impact on the business. Peer companies' industry averages would not necessarily provide detailed enough information or be as relevant to the unique aspects of the business.

T2-12 It would be **MOST** difficult to accurately estimate the likelihood of which of the following threats?

A. Flood
B. Earthquake
C. Explosion
D. Windstorm

C Flood, earthquake and windstorm are all naturally occurring disasters that have been tracked statistically over many years and average rates of occurrence are available for specific localities. An explosion is more unpredictable and any averages will not take into account issues and trends such as terrorism.

T2-13 Qualitative risk analysis is **MOST** appropriate when assessment data:

A. spans multiple industries.
B. contains percentage estimates.
C. is more than seven years old.
D. contains subjective information.

D Since it is difficult, if not impossible, to analyze subjective data using quantitative methods, qualitative risk analysis is the most appropriate. Percentage estimates would be characteristic of quantitative risk analysis. The age of the information or the fact that it spans multiple industries would not be as relevant.

T2-14 Which of the following will **BEST** identify areas of risk that have been addressed?

A. Gap analysis
B. Regression analysis
C. Correlation analysis
D. Business impact analysis

A A gap analysis is useful in addressing the differences between the current state and an ideal future state. Regression analysis is used to test changes to program modules, while correlation analysis tests the relationship between variables. A business impact analysis addresses the financial impact of the unavailability of a system.

T2-15 During which phase of development is it **MOST** appropriate to begin assessing the risk of a new application system?

A. Feasibility
B. Design
C. Development
D. Testing

A Risk should be addressed as early in the development of a new application system as possible. Identified risks, in some cases, could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes will become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

T2-16 The **BEST** way to integrate risk management into life cycle processes is through:

A. policy development.
B. change management.
C. awareness training.
D. regular monitoring.

B Change management is a process in which new risks can be introduced into business processes and systems. For this reason, risk management should be an integral component of the change management process. Policy development, awareness training and regular monitoring, although all worthwhile activities, are not as critical as change management.

T2-17 Which of the following would be **MOST** useful in developing a series of recovery time objectives (RTOs)?

A. Gap analysis
B. Regression analysis
C. Correlation analysis
D. Business impact analysis

D RTOs are a primary deliverable of a business impact analysis. RTOs relate to the financial impact of a system not being available. A gap analysis is useful in addressing the differences between the current state and an ideal future state. Regression analysis is used to test changes to program modules, while correlation analysis tests the relationship between variables.

T2-18 The recovery time objective is reached at which of the following milestones?

A. Disaster declaration
B. Recovery of the backups
C. Restoration of the system
D. Return to normal processing

C The recovery time objective is based on the amount of time required to restore a system. Disaster declaration would be at the beginning of this period. Recovery of the backups would be shortly after the beginning of this period. Return to normal processing would be significantly later than the recovery time objective.

T2-19 Which of the following **BEST** describes the level of risk that an organization is willing to accept?

A. Control risk
B. Monetary value
C. Risk exposure
D. Risk preference

D Risk preference is the appetite for risk or the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring.

T2-20 When a significant security flaw is found in a new system that is about to be moved into production, it should be reported to:

A. senior management in a quarterly report.
B. users who may be impacted by the flaw.
C. senior management in an immediate report.
D. customers who may be impacted by the flaw.

C As the system is about to be moved into production, it is important that senior management be appraised of the flaw as soon as possible. To wait until the issuance of a quarterly report may be too late. This information should not be reported to users or customers, as this could create an unnecessary loss of confidence.

T2-21 The decision on whether new risks should fall under periodic or event-driven reporting should be based on:

A. severity and duration.
B. visibility and duration.
C. likelihood and duration.
D. absolute monetary value.

D Absolute monetary value is the best measure, as it most accurately quantifies the net risk to the organization. Severity and duration and visibility and duration are not as relevant, if the likelihood is remote. Likelihood and duration is not as relevant, since it omits the severity.

T2-22 Risk acceptance is a component of which of the following?

A. Assessment
B. Mitigation
C. Evaluation
D. Monitoring

B Risk acceptance is one of the alternatives to be considered in the risk mitigation process. Assessment and evaluation are components of the risk analysis process. Risk acceptance is not a component of monitoring.

T2-23 Risk management programs are designed to reduce risk to:

A. a level that is too small to be measurable.
B. the point at which the expense exceeds the benefit.
C. a level that the organization is willing to accept.
D. a rate of return that equals the current cost of capital.

C Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive. To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the expense equals or exceeds the benefit.

T2-24 A risk assessment should be conducted:

A. once for each business process and subprocess.
B. every three to five years for critical business processes.
C. by external parties to maintain objectivity.
D. annually or whenever there is a significant change.

D Risks are constantly changing. A risk assessment conducted several years previously will not measure new risks that have been introduced since the last assessment. Therefore, conducting a risk assessment only once is insufficient. Similarly, every three to five years for critical processes is insufficient. It is not necessary that risk assessments be performed by external parties.

T2-25 A risk management program should **MOST** importantly seek to:

A. quantify overall risk.
B. minimize residual risk.
C. eliminate inherent risk.
D. maximize the sum of all annualized loss expectencies (ALEs).

B A risk management program should minimize the amount of risk that cannot be otherwise eliminated or transferred. This is the residual risk to the organization. Quantifying overall risk is important but not as critical as the end result. Eliminating inherent risk is virtually impossible. Maximizing the sum of all ALEs is actually the opposite of what is desirable.

T2-26 Which of the following risks would **BEST** be assessed using qualitative risk assessment techniques?

A. The theft of purchased software
B. A power outage lasting 24 hours
C. A permanent decline in customer confidence
D. The loss of e-mail for 72 hours due to a virus attack

C A permanent decline in customer confidence does not lend itself well to measurement by quantitative techniques. Qualitative techniques are more effective in evaluating things like customer loyalty and goodwill. Theft of software, power outages and temporary loss of e-mail can more easily be quantified into monetary amounts that can be assessed with quantitative techniques.

T2-27 Which of the following will **BEST** prevent externally generated security attacks?

A. Static IP addressing
B. Network address translation
C. Background checks for temporary employees
D. Writing all computer logs to removable media

B Network address translation will be helpful by having internal addresses that are nonroutable. Background checks of temporary employees will be more likely to prevent an attack launched from within the enterprise. Static IP addressing will do little to prevent an attack. Writing all computer logs to removable media will not help in preventing an attack.

T2-28 In performing a risk assessment on the impact of losing a database server, the value of the server should be calculated using the:

A. original cost to acquire the server.
B. value of the data stored on the server.
C. annualized loss expectancy (ALE) for the server.
D. new cost to obtain a replacement server.

D The value of the server should be based on its cost to replace. The original cost may be significantly different from the current cost and therefore not as relevant. The value of the data is not at issue, since this can be restored for backup media. The ALE for all risks related to the server does not represent the server's value.

T2-29 A business impact analysis (BIA) is the **BEST** tool for calculating:

A. total cost of ownership.
B. priority of restoration.
C. annualized loss expectancy (ALE).
D. residual risk to the organization.

B A BIA is the best tool for calculating the priority of restoration for applications. It is not used to determine total cost of ownership, ALE or residual risk to the organization.

T2-30 When residual risk is minimized:

A. acceptable risk is achieved.
B. transferred risk is minimized.
C. control risk is reduced to zero.
D. residual risk equals transferred risk.

A Since residual risk is the risk that remains after putting into place an effective risk management program, acceptable risk will be achieved when this amount is minimized. Transferred risk is risk that has been assumed by a third party. Accordingly, choices B and D are incorrect, since transferred risk does not necessarily indicate whether risk is at an acceptable level. Minimizing residual risk will not reduce control risk to zero.

T2-31 Which of the following threats would generally be the **EASIEST** to accurately estimate its likelihood?

A. Terrorism
B. Chemical spill
C. Explosion
D. Windstorm

D Windstorms are all naturally occurring disasters that have been tracked statistically over many years and average rates of occurrence are available for specific localities. Terrorism, chemical spills and explosions are more unpredictable and difficult to estimate for specific locations.

T2-32 Quantitative risk analysis is **MOST** appropriate when assessment data:

A. include customer perceptions.
B. contain percentage estimates.
C. are lacking in specific details.
D. contain subjective information.

B Percentage estimates are more characteristic of quantitative risk analysis. Customer perceptions, lack of specific details or subjective information lend themselves more to qualitative risk analysis.

T2-33 Which of the following would be the **MOST** appropriate application of gap analysis?

A. Evaluating a business impact analysis (BIA)
B. Developing a balanced business scorecard
C. Demonstrating the relationship between variables
D. Measuring current state vs. desired future state

D A gap analysis is most useful in addressing the differences between the current state and an ideal future state. It is not as appropriate for evaluating a BIA, developing a balanced business scorecard or demonstrating the relationship between variables.

T2-34 Identification and prioritization of risk enables project managers to:

A. establish implementation milestones.
B. reduce the overall amount of testing.
C. direct attention on areas of greatest impact.
D. accelerate completion of the feasibility study.

C Identification and prioritization of risk allows project managers to focus more attention on areas of greater importance and impact. It will not reduce the overall amount of testing, facilitate establishing implementation milestones or allow a feasibility study to be completed any sooner.

T2-35 A risk analysis should:

A. limit the scope to a benchmark of similar companies.
B. assume an equal degree of protection for all assets.
C. address the potential size and likelihood of loss.
D. give more weight to the likelihood vs. the size of the loss.

C A risk analysis should take into account the potential size and likelihood of a loss. It should not be limited to a group of companies of similar size. It should not assume an equal degree of protection for all assets, since assets may have different risk factors. Also, the likelihood of the loss should not receive greater emphasis than the size of the loss, as both are used to calculate annualized loss expectancy.

T2-36 The recovery point objective (RPO) is at which of the following milestones?

A. Disaster declaration date
B. Offsite media creation date
C. Restoration of the system
D. Return to normal processing

B The RPO is the point in time of system recovery; this is the creation date of the tapes sent offsite that were subsequently used to restore the system. Disaster declaration is subsequent to this point in time. Restoration of the system occurs at a later date, as does the return to normal processing.

T2-37 When a minor security flaw is found in a new system that is about to be moved into production, this should be reported to:

A. senior management in a quarterly report.
B. users who may be impacted by the flaw.
C. senior management in an immediate report.
D. customers who may be impacted by the flaw.

A Since the system flaw is minor, it is not necessary to immediately report the situation to senior management. It is not necessary to notify customers or users, since this may undermine their confidence in the system.

T2-38 Which of the following **BEST** describes the probability that a successful attack will occur?

A. The value of the target and level of protection is high.
B. The motivation and ability of the attacker is high.
C. The value of the target is high and protection is low.
D. The motivation of the attacker and value of the target is high.

C When the value of the target is high and the protection is low, the possibility of a successful attack is substantially increased. When the level of protection is high, the probability of a successful attack is reduced. A highly motivated and talented attacker increases the probability but not to the degree afforded by choice C.

T2-39 Information security risk is increased the **MOST** when:

A. procedures are not enforced.
B. change management is lacking.
C. systems are developed in-house.
D. systems are complex and distributed.

B The lack of change management is a severe omission and will greatly increase information security risk. Since procedures are generally nonauthoritative, their lack of enforcement is not a primary concern. Systems that are developed in-house and complex distributed systems are becoming commonplace and do not represent an increase in security risk as much as poor change management.

T2-40 Which of the following **BEST** describes the scope of risk analysis?

A. Key financial systems
B. Organizational activities
C. Key systems and infrastructure
D. Systems subject to regulatory compliance

B Risk analysis should include all organizational activities. It should not be limited to subsets of systems or just systems and infrastructure.

T2-41 Ultimately, management's decision on the level of acceptable risk is a:

A. subjective decision.
B. qualitative decision.
C. probability decision.
D. quantitative decision.

A The decision by management on the level of acceptable risk is subjective, since it includes a mix of qualitative and quantitative factors that ultimately must be weighed using management's best judgment.

T2-42 The determination as to whether a risk has been reduced to an acceptable level should be determined by:

A. organizational requirements.
B. information systems requirements.
C. information security requirements.
D. international standards of best practice.

A Organizational requirements should determine when a risk has been reduced to an acceptable level. Information systems and information security should not make the ultimate determination. Since each organization is unique, international standards of best practice do not represent the best solution.

T3 INFORMATION SECURITY PROGRAM(ME) MANAGEMENT

T3-1 Who is in the **BEST** position to champion the development and ensure the success of an information security program?

A. Internal audit
B. External audit
C. Senior management
D. Infrastructure management

C Senior management is in the best position to champion the establishment of, and continued support for, an information security program. Internal and external audit are both good advocates for this, but they are secondary to the influence of senior management. Infrastructure management would have a lesser degree of influence.

T3-2 Which of the following **BEST** ensures that information transmitted over the Internet will remain confidential?

A. Encryption
B. Steganography
C. Biometric authentication
D. Two-factor authentication

A Encryption ensures that transmitted information cannot be easily intercepted and read. Steganography is the technique of hiding messages within other files. Biometric and two-factor authentication would not by themselves prevent a message from being intercepted and read.

T3-3 The effectiveness of virus detection software is **MOST** dependent on which of the following?

A. Number of product upgrades
B. Number of available patches
C. License agreement warranties
D. Update frequency of DAT files (odat)

D New viruses are introduced almost every day. The effectiveness of virus detection software depends on frequent updates of virus signatures that are stored on DAT files. Patches and product upgrades are related to the periodic updating of the program code, which would not be as time-critical. License agreement warranties would not be as critical.

T3-4 The greatest reduction in overhead costs for security administration would be provided by:

A. mandatory access control.
B. role-based access control.
C. decentralized access control.
D. discretionary access control.

B Role-based access control allows users to be grouped into job-related categories, which significantly eases the required administrative overhead. Mandatory and discretionary access control would both require a greater degree of administrative overhead. Decentralized access control generally requires a greater number of staff to administer.

T3-5 Out-of-band communications are **MOST** appropriate when transmitting:

A. password changes.
B. encrypted files.
C. large data files.
D. nonstandard protocols.

A Sending the password over the same medium may cause a system breach to be perpetuated; therefore, password changes should be communicated to the user using some other form of communication. Encrypted files, large data files and the use of nonstandard protocols do not require the use of out-of-band communications.

T3-6 Which of the following devices should be placed within a DMZ?

A. Router
B. Firewall
C. Mail relay
D. Authentication server

C A mail relay should normally be placed within a DMZ to shield the internal network. An authentication server, due to its sensitivity, should always be placed on the internal network, never on a DMZ that is subject to compromise. Both routers and firewalls may bridge a DMZ to another network, but do not technically reside within the DMZ network segment.

T3-7 An intrusion detection system (IDS) should be placed:

A. outside the firewall.
B. on the firewall server.
C. on a screened subnet.
D. on the external router.

C An IDS should be placed on a screened subnet, which is a DMZ. Placing it on the Internet side of the firewall would leave it defenseless. The same would be true of placing it on the external router, if such a thing were feasible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the IDS on the same physical device.

T3-8 The **BEST** reason for an organization to have two discrete firewalls connected directly to the Internet and the same DMZ would be to:

A. provide defense in-depth.
B. separate test and production.
C. permit traffic load balancing.
D. prevent a denial-of-service attack.

C Having two entry points each guarded by a separate firewall would be desirable to permit traffic load balancing. As they both connect to the Internet and to the same DMZ, such an arrangement would not be practical for separating test from production or preventing a denial-of-service attack.

T3-9 An extranet server should be placed:

A. outside the firewall.
B. on the firewall server.
C. on a screened subnet.
D. on the external router.

C An extranet server should be placed on a screened subnet, which is a DMZ. Placing it on the Internet side of the firewall would leave it defenseless. The same would be true of placing it on the external router, although this would not be possible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the extranet on the same physical device.

T3-10 Accountability by business process owners can **BEST** be obtained through:

A. periodic reminder memorandums.
B. strict enforcement of policies.
C. policies signed by IT management.
D. education and awareness meetings.

D Business process owners should be educated on the importance of accountability. This can best be accomplished through education and awareness meetings. Periodic reminder memos will not be as effective. Strict enforcement of policies will not always take into account the needs of the business. Policies signed by IT management will be less effective than those signed by the senior management of the organization.

T3-11 The main advantage of involving the owner of a business process in the evaluation and management of information security risks is their understanding of the:

A. infrastructure risks.
B. industry best practices.
C. security mechanisms.
D. specific business risks.

D Business process owners are the most knowledgeable concerning specific business risks. They are not as knowledgeable concerning infrastructure risks and security mechanisms, and they may not be aware of industry best practices.

T3-12 Of the following, the **BEST** metric for evaluating the effectiveness of security awareness training is the number of:

A. password resets.
B. reported incidents.
C. individuals trained.
D. access rule violations.

B Reported incidents will provide an indicator of the awareness level of staff. More reported incidents could indicate that the staff is paying more attention to security. Password resets and access rule violations may or may not have anything to do with awareness levels. The number of individuals trained may not correlate to whether they are more aware or merely went through the process and came out unchanged.

T3-13 When implementing a new system using a purchased software package, the time and duration of which of the following system life cycle phases will likely be reduced the **MOST**?

A. Feasibility
B. Development
C. Testing
D. Postimplementation review

B With the exception of customization and interface requirements, a purchased package minimizes the development needs. Feasibility, testing and postimplementation review must be performed as before.

T3-14 Which of the following is the **BEST** method for ensuring that security procedures and guidelines are read and understood?

A. Periodic focus group meetings
B. Periodic reminder memos to management
C. Using computer-based training presentations (CBTs) with quizzes
D. Employees signing an acknowledgement of receipt

C Using CBTs with end of section reviews provides feedback on how well users understand what has been presented. Reminder memos will have little impact, and focus groups may or may not provide meaningful detail. Although a signed employee acknowledgement is good, it does not indicate whether the material has been read and/or understood.

T3-15 When contracting with an outsourcer to provide security administration the most important contractual element is the:

A. right-to-terminate clause.
B. limitations of liability.
C. service level agreements.
D. hold-harmless agreements.

C Service level agreements provide metrics to which outsourcing firms can be held accountable. This is more important than a limitation on the outsourcing firm's liability, a right-to-terminate clause or a hold-harmless agreement, which involves liabilities to third parties.

T3-16 Which of the following is the **BEST** metric for evaluating the effectiveness of an intrusion detection mechanism?

A. Number of attacks detected
B. Number of successful attacks
C. Ratio of false-positives to false-negatives
D. Ratio of successful to unsuccessful attacks

C The ratio of false-positives to false-negatives will indicate whether an intrusion detection system (IDS) is properly tuned to minimize the number of false alarms while at the same time minimizing the number of omissions. The number of attacks detected, successful attacks or the ratio of successful to unsuccessful attacks would not indicate whether the IDS is properly configured.

T3-17 Which of the following is the **MOST** effective in preventing weaknesses from being introduced during the life cycle of a system?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

B Change management controls the process of introducing changes to systems. This is often the point at which a weakness will be introduced. Patch management involves the correction of software weaknesses. Security baselines provide minimum recommended settings, while acquisition management controls the purchasing process.

T3-18 Which of the following tools is **MOST** appropriate for determining how long a security project will take to implement?

A. Gantt chart
B. Waterfall chart
C. Critical path method
D. Balanced scorecard method

C The critical path method is most effective for determining how long a project will take. A waterfall chart is used to understand the flow of one process into another. A Gantt chart facilitates the proper estimation and allocation of resources. The balanced scorecard method is used as an aid to corporate governance in measuring the attainment of goals.

T3-19 The biometric access control method that has the **BEST** acceptance in terms of user attitudes is:

A. facial recognition.
B. iris scanning.
C. retina scanning.
D. fingerprint scanning.

D Fingerprint scanning has the best acceptance in terms of user attitudes. Users are more resistant to having devices scan their eyes because of fear that their eyes may be damaged in the process. Facial recognition is somewhat more sensitive than fingerprinting due to privacy issues and because certain cultures are resistant to photographing or imaging the face.

T3-20 Which of the following is the **MOST** effective in preventing attacks that exploit weaknesses in operating systems?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

A Patch management corrects discovered weaknesses by applying a correction (a patch) to the original program code. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings, while acquisition management controls the purchasing process.

T3-21 When a system change violates an existing security standard, the conflict should be resolved:

A. using a cost-benefit analysis.
B. in favor of the security standard.
C. in favor of the new system change.
D. using best practices for that industry.

A Decisions regarding security should always weigh the potential costs of a control against the expected benefit to be derived. Each situation is unique; therefore, it is not advisable to always decide in favor of a standard or in favor of the request from the business unit. Similarly, industry practices cannot always be applied to the unique situations of the business.

T3-22 Which of the following is in the **BEST** position to approve plans to implement the information security governance framework?

A. Internal audit
B. Legal counsel
C. Senior management
D. Infrastructure management

C Senior management is in the best position to approve plans to implement an information security governance framework. Internal audit and legal counsel are good advocates, but they are secondary to the authority and influence of senior management. Infrastructure management will not be in the best position, since it focuses more on the technologies rather than the business.

T3-23 Which of the following is the **MOST** effective solution for preventing internal users from modifying sensitive and classified information?

A. Screened subnets
B. System access logs
C. Role-based access controls
D. Intrusion detection system

C Role-based access controls help ensure that users only have access to files and systems appropriate for their job role. Screened subnets are DMZs and are more oriented toward attacks by external users. Similarly, an intrusion detection is not as effective in preventing unauthorized data access by internal users.

T3-24 Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

A. Biometric authentication
B. Embedded steganographic techniques
C. Two-factor authentication
D. Embedded digital signature

D Digital signatures ensure that transmitted information can be attributed to the named sender. This provides nonrepudiation. Steganographic techniques are used to hide messages or data within other files. Biometric and two-factor authentication are not generally used to provide nonrepudiation.

T3-25 What is an appropriate frequency for updating antivirus signature files for antivirus software on production servers?

A. Daily
B. Monthly
C. Concurrently with O/S patch updates
D. During scheduled weekly change control updates

A New viruses are being introduced almost daily. The effectiveness of virus detection software depends on frequent updates to its virus signatures that are stored on antivirus signature files. Patches may occur less frequently. Weekly or monthly updates are too seldom and may potentially allow new viruses to infect the system.

T3-26 Which of the following devices should be placed within a DMZ?

A. Switch
B. Web server
C. Database server
D. File/print server

B A web server should normally be placed within a DMZ to shield the internal network. Database and file/print servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ, which is subject to compromise. Switches may bridge a DMZ to another network but do not technically reside within the DMZ network segment.

T3-27 A firewall should be placed on a(n):

A. web server.
B. intrusion detection system (IDS) server.
C. screened subnet.
D. domain boundary.

D A firewall should be placed on a (security) domain boundary. Placing it on a web server or screened subnet (DMZ) does not provide any protection. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to have the firewall and the IDS on the same physical device.

T3-28 An intranet server should generally be placed on the:

A. internal network.
B. firewall server.
C. external router.
D. primary domain controller.

A An intranet server should be placed on the internal network. Placing it on an external router leaves it defenseless. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to store the intranet server on the same physical device as the firewall. Similarly, primary domain controllers do not normally share the physical device as the intranet server.

T3-29 Access to a sensitive intranet application by mobile users can **BEST** be accomplished through:

A. data encryption.
B. digital signatures.
C. strong passwords.
D. two-factor authentication.

D Two-factor authentication through the use of strong passwords combined with security tokens provides the highest level of security. Data encryption, digital signatures and strong passwords do not provide the same level of protection.

T3-30 In cases where application-level security controlled by business process owners is found to be poorly managed, improvement can **BEST** be obtained through:

A. periodic reminder memorandums.
B. circulation of best practices.
C. policies signed by IT management.
D. education sessions and periodic reviews.

D Business process owners need to be educated on the importance of accountability. This needs to be followed up with periodic reviews to reinforce accountability. Periodic reminder memos and circulation of best practices is not as effective, and policies signed by IT management are not as effective as those signed by the organization's senior management.

T3-31 Security awareness training should lead to a(n):

A. decrease in password resets.
B. increase in reported incidents.
C. decrease in security policy changes.
D. increase in access rule violations.

B Reported incidents will provide an indicator as to the awareness level of staff. More incidents being reported could indicate that staff is paying more attention to security. Password resets and access rule violations may or may not have anything to do with awareness levels. A decrease in changes to security policies may or may not correlate to security awareness training.

T3-32 When attempting to implement a new enterprise resource planning (ERP) system using a purchased solution, which of the following will take the **LONGEST** to complete?

A. Feasibility study and product selection
B. Loading of program and database libraries
C. Product customization and integration
D. User acceptance testing and sign-off

C Customization of ERP systems and integrating them into the existing infrastructure and lattice work of legacy systems can be quite extensive. Feasibility and product selection, loading of program and database libraries, and user acceptance testing are less time-consuming to complete.

T3-33 Which of the following is the **BEST** method for setting up a new user's initial password for system access?

A. E-mail the password to the user.
B. Have the manager deliver the password.
C. Set the initial password to a null value.
D. Set the initial password equal to the user ID.

B The best choice is for the manager of the new user to deliver the initial password. E-mailing the password will not work since the individual cannot log on to retrieve their password. Setting the password to a null value or equal to the user ID creates a security weakness.

T3-34 An information security program should be sponsored by:

A. infrastructure management.
B. the corporate legal department.
C. key business process owners.
D. quality assurance management.

C The information security program should ideally be sponsored by business managers, as represented by key business process owners. Infrastructure management is not sufficiently independent and lacks the necessary knowledge regarding specific business requirements. Corporate legal counsel and quality assurance similarly are not in as good a position to fully understand how an information security program needs to meet the needs of the business.

T3-35 Which of the following is the **MOST** important item to include when developing web-hosting agreements with third-party providers?

A. Termination conditions
B. Liability limits
C. Service levels
D. Privacy restrictions

C Service levels are key to holding third parties accountable for adequate delivery of services. This is more important than termination conditions, privacy restrictions or liability limitations.

T3-36 The **BEST** metric for evaluating the effectiveness of a firewall is the:

A. number of attacks blocked.
B. number of packets dropped.
C. average throughput rate.
D. number of firewall rules.

A The number of attacks blocked indicates whether a firewall is performing as intended. The number of packets dropped does not necessarily indicate the level of effectiveness. The number of firewall rules and the average throughput rate are not as effective measurements.

T3-37 Which of the following ensures that newly identified security weaknesses are mitigated in a timely fashion?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

A Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings, while acquisition management controls the purchasing process.

T3-38 The **MAIN** advantage of implementing automated password synchronization is that it:

A. reduces overall administrative workload.
B. increases security between multitier systems.
C. allows passwords to be changed less frequently.
D. reduces the need for two-factor authentication.

A Automated password synchronization reduces the overall administrative workload of resetting passwords. It does not increase security between multitier system, allow passwords to be changed less frequently or reduce the need for two-factor authentication.

T3-39 Which of the following tools is **MOST** appropriate for judging whether information security governance objectives are being met?

A. SWOT analysis
B. Waterfall chart
C. Gap analysis
D. Balanced scorecard

D The balanced scorecard is most effective for evaluating the degree to which information security objectives are being met. A SWOT analysis addresses strengths, weaknesses, opportunities and threats. Although useful, a SWOT analysis is not as effective a tool. Similarly, a gap analysis, while useful for identifying the difference between the current state and the desired future state, is not the most appropriate tool. A waterfall chart is used to understand the flow of one process into another.

T3-40 Which of the following is **MOST** effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

A. Patch management
B. Change management
C. Security metrics
D. Version control

B Change management controls the process of introducing changes to systems. Failure to have good change management may introduce new weaknesses into otherwise secure systems. Patch management corrects discovered weaknesses by applying a correction to the original program code. Security metrics provide a means for measuring effectiveness, while version control is a subset of change management.

T3-41 When an O/S patch that will enhance system security cannot be applied because it will adversely impact the ability of a critical application to operate on that platform, which of the following should occur?

A. The O/S patch should be applied and the application then rewritten to conform to the upgraded O/S.
B. A mitigating control should be identified that will compensate for not installing the O/S patch.
C. The O/S patch should be altered to allow the application to run in a privileged state.
D. The application should be switched to run on a test platform, while the production platform is tuned to allow the patch and application to coexist.

B Since the O/S patch will adversely impact a critical application, a mitigating control should be identified that will provide an equivalent level of security. Since the application is critical, the patch should not be applied without regard for the application. Business requirements must be considered. Altering the O/S patch to allow the application to run in a privileged state may create new security weaknesses. Finally, running a production application on a test platform is not an acceptable alternative, since it will mean running a critical production application on a platform not subject to the same level of security controls.

T3-42 Which of the following is **MOST** important in ensuring the success of an information security program?

A. Security awareness training
B. Achievable goals and objectives
C. Sufficient senior management support
D. Adequate start-up budget and staffing

C Sufficient senior management support is the most important factor for the success of an information security program. Security awareness training, although important, is secondary. Achievable goals and objectives as well as having adequate budgeting and staffing are important factors, but they will not ensure success if senior management support is not present.

T4 INFORMATION SECURITY MANAGEMENT

T4-1 The **BEST** way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

A. perform penetration testing.
B. establish security baselines.
C. implement vendor default settings.
D. link policies to an independent standard.

B Security baselines will provide the best assurance that each platform meets minimum criteria. Penetration testing will not be as effective and can only be performed periodically. Vendor default settings will not necessarily meet the criteria set by the security policies and linking policies to an independent standard will not provide assurance that the platforms meet these levels of security.

T4-2 A web-based business application that utilizes public keys and two-factor authentication is being migrated from test to production. Which of the following is the **MOST** important sign-off for this migration?

A. User management
B. Network management
C. Operations management
D. Database management

A As owners of the system, user management sign-off is the most important. If a system does not meet the needs of the business, then it has not met its primary objective. The needs of network, operations and database management are secondary to the needs of the business.

T4-3 The **BEST** way to ensure that information security policies are followed is to:

A. distribute printed copies to all employees.
B. perform periodic reviews for compliance.
C. tie policies to a recognized international standard.
D. establish a telephone number to report policy abuses.

B The best way to ensure that information security policies are followed is to periodically review levels of compliance. Distributing printed copies, advertising an abuse hotline or linking policies to an international standard will not motivate individuals as much as the consequences of being found in noncompliance.

T4-4 The **MOST** appropriate individual to determine the level of information security needed for a specific business application is the:

A. system developer.
B. infrastructure manager.
C. system custodian.
D. system data owner.

D Data owners are generally the most knowledgeable of the security needs of the business application for which they are responsible. The systems developer, infrastructure manager and system custodian will have specific knowledge on limited areas but will not have full knowledge of the business issues which affect the level of security required.

T4-5 Which of the following will **MOST** reduce the likelihood of an unauthorized individual gaining access to computing resources by pretending to be an authorized individual needing to have their password reset?

A. Performing reviews of password resets
B. Conducting security awareness programs
C. Increasing the frequency of password changes
D. Implementing automatic password syntax checking

B Social engineering can best be mitigated through periodic security awareness training for staff members who may be the target of such an attempt. Changing the frequency of password changes, strengthening passwords and checking the number of password resets may be desirable, but they will not be as effective in reducing the likelihood of a social engineering attack.

T4-6 Which of the following is the **MOST** likely to change an organization's culture to one that is more security conscious?

A. Security policies and procedures
B. Periodic penetration testing
C. Security steering committees
D. Security awareness campaigns

D Security awareness campaigns will be more effective at changing organizational culture than periodic penetration testing or the creation of steering committees and security policies and procedures.

T4-7 The **BEST** way to ensure that an external service provider complies with organizational security policies is to:

A. explicitly refer to the provider in the security policies.
B. have the provider acknowledge in writing reading all policies.
C. refer to policies in the service level agreement.
D. perform periodic reviews of the service provider.

D Periodic reviews will be the most effective way of obtaining compliance from the external service provider. References in policies and service level agreements and requesting written acknowledgement will not be as effective, since they will not trigger the detection of noncompliance.

T4-8 When an emergency security patch is received via electronic mail, the patch should **FIRST** be:

A. loaded onto an isolated test machine.
B. decompiled to check for malicious code.
C. validated to ensure its authenticity.
D. copied onto write-once media to prevent tampering.

C It is important to first validate that the patch is authentic. Only then should it be copied onto write-once media, decompiled to check for malicious code or loaded onto an isolated test machine.

T4-9 Which of the following activities is **MOST** likely to lead to the introduction of weaknesses in security software?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

B Security software will generally have a well-controlled process for applying patches, backing up files and upgrading hardware. The greatest risk occurs when access rules are changed, since they are susceptible to being opened up too much, which can result in the creation of a security exposure.

T4-10 Which of the following is the **BEST** indicator that security awareness training has been effective?

A. Password resets have declined.
B. More incidents are being reported.
C. A majority of employees have received training.
D. Feedback forms from training are favorable.

B More incidents being reported could be an indicator that the staff is paying more attention to security. Password resets and feedback forms may or may not have anything to do with awareness levels. The number of individuals trained may not correlate to whether they are more aware or merely went through the process and came out unchanged.

T4-11 Which of the following metrics would be the **MOST** useful in measuring how well information security is monitoring violation logs? The number of:

A. penetration attempts investigated.
B. violation log reports reviewed.
C. violation log entries reviewed.
D. hours charged to the review process.

A The most useful metric is one that measures the degree to which complete follow-through has taken place. The reviewing of reports, entries on reports and the number of hours charged to the process are not indicative of whether investigative action was taken.

T4-12 Which of the following change management activities would be an indicator that normal operational procedures are being overridden? A high percentage of:

A. similar change requests.
B. change request postponements.
C. cancelled change requests.
D. emergency change requests.

D A high percentage of emergency change requests could be caused by changes that are being introduced at the last minute to bypass normal change management procedures. Similar requests, postponements and cancelled requests all are indicative of a properly functioning change management process.

T4-13 Which of the following is the **MOST** important sign-off for migrating an order processing system from a test environment to a production environment?

A. User management
B. Security management
C. Operations management
D. Database management

A As owners of the system, user management approval would be the most important. Although the sign-offs of security, operations and database management may be appropriate, they are secondary to ensuring the new system meets the requirements of the business.

T4-14 Prior to having a third party perform an attack and penetration test against an organization, the **MOST** important action is to ensure that:

A. the third party provides a demonstration on a test system.
B. goals and objectives are clearly defined.
C. the technical staff has been briefed on what to expect.
D. special backups of production servers are taken.

B The most important action is to clearly define the goals and objectives of the test. Assuming that adequate backup procedures are in place, special backups should not be necessary. Technical staff should not be briefed nor should there be a demo as this will reduce the spontaneity of the test.

T4-15 When a departmental system continues to remain out of compliance with the information security policy's password strength requirements, the **BEST** action to undertake is to:

A. submit the issue to an external arbitration group.
B. conduct an impact analysis to quantify the risks.
C. isolate the system from the rest of the network.
D. grant a special waiver that is subject to annual renewal.

B An impact analysis is warranted to determine whether a special waiver should be granted and to demonstrate to the department the danger of deviating from the established policy. Isolating the system would not support the needs of the business, and submitting the issue to arbitration would not be practical. Any waiver should be granted only after performing an impact analysis.

T4-16 Which of the following, if absent, would be the **MOST** detrimental to the promotion of good security management practices?

A. Security metrics
B. Security baselines
C. Management support
D. Periodic training

C Without management support, all other efforts will be undermined. Metrics, baselines and training are all important, but they depend on management support for their success.

T4-17 Which of the following environments would be the **MOST** likely to deviate from organizational security policies?

A. Locally managed file server
B. Enterprise data warehouse
C. Load-balanced, web server cluster
D. Centrally managed data switch

A A locally managed file server will be the least likely to conform to organizational security policies, because it is generally subject to less oversight and monitoring. Centrally managed data switches, web server clusters and data warehouses are subject to close scrutiny, good change control practices and monitoring.

T4-18 Nonrepudiation can **BEST** be assured by using:

A. delivery path tracing.
B. reverse lookup translation.
C. out-of-band channels.
D. digital signatures.

D Effective nonrepudiation requires the use of digital signatures. Reverse lookup translation involves converting IP addresses to usernames. Delivery path tracing will show the route taken but not confirm the identity of the sender. Out-of-band channels are useful when, for confidentiality, it is necessary to break a message into two parts that are sent by different means.

T4-19 Of the following, the **BEST** method for ensuring that temporary employees do not receive excessive access rights is:

A. mandatory access controls.
B. discretionary access controls.
C. lattice-based access controls.
D. role-based access controls.

D Role-based access controls will grant temporary employee access based on the job function to be performed. This provides a better means of ensuring that the access is not more or less than what is required. Discretionary- mandatory- and lattice-based access controls are all security models, but they do not address the issue of temporary employees as well as role-based access controls.

T4-20 Which of the following areas is **MOST** susceptible to the introduction of security weaknesses?

A. Database management
B. Tape backup management
C. Configuration management
D. Incident response management

C Configuration management provides the greatest likelihood of security weaknesses through misconfiguration and failure to update O/S code correctly and on a timely basis.

T4-21 Security policies should be aligned **MOST** closely to:

A. industry best practices.
B. the needs of the organization.
C. globally accepted best practices.
D. local laws and regulations.

B The needs of the organization should always take precedence. Best practices and local regulations are important, but they do not take into account the total needs of an organization.

T4-22 The **BEST** way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

A. simulate an attack and review IDS performance.
B. use a honeypot to check for unusual activity.
C. review the configuration of the IDS.
D. benchmark the IDS against a peer site.

A Simulating an attack on the network will demonstrate whether the IDS is properly tuned. Reviewing the configuration may or may not reveal weaknesses as an anomaly-based system uses trends to identify potential attacks. A honeypot is not a good first step, as it would have to have already been penetrated. Benchmarking against a peer site would generally not be practical or useful.

T4-23 The **BEST** time to perform a penetration test is after a(n):

A. attempted penetration has occurred.
B. audit has discovered a lack of security controls.
C. number of systems infrastructure changes are made.
D. turnover in systems administrative staff.

C Changes in the systems infrastructure are the most likely to inadvertently introduce new exposures. Conducting a test after an attempted penetration is not as productive, as an organization should not wait until it is attacked to test its defenses. Any exposure identified by an audit should be corrected before it would be appropriate to test. A turnover in administrative staff does not warrant a penetration test, although it may warrant a review of password change practices and configuration management.

T4-24 Successful social engineering attacks can **BEST** be prevented through:

A. preemployment screening.
B. close monitoring of users.
C. periodic awareness training.
D. efficient termination procedures.

C Security awareness training is most effective in preventing the success of social engineering attacks by providing users with the awareness they need to resist such attacks. Screening of new employees, monitoring and rapid termination will not be effective against external attacks.

T4-25 What is the **BEST** way to ensure that an intruder who successfully penetrates a network will be detected before significant damage is inflicted?

A. Perform periodic penetration testing.
B. Establish minimum security baselines.
C. Implement vendor default settings.
D. Install a honeypot on the network.

D Honeypots attract hackers away from sensitive systems and files. Since honeypots are closely monitored, the intrusion is more likely to be detected before significant damage is inflicted. Security baselines will only provide assurance that each platform meets minimum criteria. Penetration testing is not as effective and can only be performed periodically. Vendor default settings are not effective.

T4-26 Which of the following presents the **GREATEST** threat to the security of an enterprise resource planning (ERP) system?

A. User *ad hoc* reporting is not logged.
B. Network traffic is through a single switch.
C. O/S security patches have not been applied.
D. Database security defaults to ERP settings.

C The fact that O/S security patches have not been applied is a serious weakness. Routing network traffic through a single switch is not unusual. Although the lack of logging for user *ad hoc* reporting is not necessarily good, it does not represent as serious a security weakness as the failure to install security patches. Database security defaulting to the ERP system's settings is not as significant.

T4-27 A perpetrator calls an authorized user and pretends to be a network administrator who needs to know the user's password to perform a test of the user's connectivity to the network. In this scenario, which of the following will **MOST** likely reduce the likelihood of this unauthorized individual gaining access to computing resources?

A. Implementing on-screen masking of passwords
B. Conducting periodic security awareness programs
C. Increasing the frequency of password changes
D. Requiring that passwords not be disclosed to others in security policies

B Social engineering can best be mitigated through periodic security awareness training for users who may be the target of such an attempt. Implementing on-screen masking of passwords and increasing the frequency of password changes are desirable, but these will not be effective in reducing the likelihood of a successful social engineering attack. Requiring that passwords be kept secret in security policies is a good control but is not as effective as periodic security awareness programs that will alert users of the dangers posed by social engineering.

T4-28 Which of the following will **BEST** ensure that management takes ownership in the decision-making process for information security?

A. Security policies and procedures
B. Annual self-assessment by management
C. Security steering committees
D. Security awareness campaigns

C Security steering committees provide a forum for management to express its opinion and take some ownership in the decision-making process. Security awareness campaigns, security policies and procedures, and self-assessment exercises are all good but do not exemplify the taking of ownership by management.

T4-29 It is **MOST** likely that a data owner will not need to sign authorization request forms for each user who will access the owner's data when:

A. the data are read-only historical data.
B. discretionary access control is utilized.
C. the authorization was provided by the requestor's supervisor.
D. role-based access control is utilized.

D Role-based access control eliminates the need to sign individual forms as the data owner has preapproved all users assigned to a specific role to have such access. Discretionary access requires individually signed request forms. The fact that data are read-only or that the requestor's supervisor provided their approval does not eliminate the need for a signature.

T4-30 Which of the following is the **MOST** appropriate individual to implement and maintain the level of information security needed for a specific business application?

A. System developer
B. Quality control manager
C. System custodian
D. System data owner

C Data custodians implement information protection controls as determined by the data owners. Data owners have the most knowledge about security requirements for the business application for which they are responsible. The system's developer and quality control manager do not possess the necessary knowledge or authority to implement and maintain the appropriate level of security.

T4-31 What is the **BEST** way to ensure that contract programmers comply with organizational security policies?

A. Explicitly refer to contractors in the security standards.
B. Have the contractors acknowledge in writing that they have read-all security policies.
C. Create penalties for noncompliance in the contracting agreement.
D. Perform periodic security reviews of the contractors.

D Periodic reviews are the most effective way of obtaining compliance. None of the other options will detect the failure of contract programmers to comply.

T4-32 Which of the following is often poorly handled when administering IDs for contract programmers?

A. Creation
B. Modification
C. Resetting
D. Revocation

D Since contract programmers are temporary employees, the removal from the system is often poorly handled, for example, there departure may not trigger an event on any HR system—the usual means of triggering ID revocation. Creation, modification and resetting are all less subject to improper handling.

T4-33 Which of the following activities is **MOST** likely to increase the difficulty of totally eradicating malicious code that is not immediately detected?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

D If malicious code is not immediately detected, it will most likely be backed up as a part of the normal tape backup process. When later discovered, the code may be eradicated from the device but still remain undetected on a backup tape. Any subsequent restores using that tape may reintroduce the malicious code. Applying patches, changing access rules and upgrading hardware does not significantly increase the level of difficulty.

T4-34 Which of the following metrics is the **MOST** appropriate for measuring how effectively the organization is securing systems? The percentage of:

A. servers with up-to-date patches.
B. vulnerabilities still open.
C. number of viruses detected.
D. systems where change control processes apply.

B The best metric is the number of vulnerabilities still open, as this provides an overall snapshot of progress. The number of servers with patches installed, the number of viruses detected and the number of systems where change control applies are all measures of specific aspects vs. the overall picture.

T4-35 In a financial services organization, security awareness training should be provided to new employees:

A. on an as-needed basis when specific duties warrant.
B. during user training on the system they are to access.
C. before they receive access to information.
D. at the same time that existing employees are trained.

C Security awareness training should occur before access is granted. All other choices imply that security awareness training is delivered subsequent to the granting of system access.

T4-36 What is the **BEST** method to verify that all security patches applied to servers were properly documented?

A. Trace change control requests to O/S patch logs.
B. Trace O/S patch logs to the O/S vendor's update site.
C. Trace O/S patch logs to change control requests.
D. Review change control documents for key servers.

C To ensure that all patches applied went through the change control process, it is necessary to use the O/S patch logs as a starting point and then check to see if change control documents are on file for each of these changes. Tracing from the documentation to the patch log will not indicate if some patches were applied without being documented. Similarly, reviewing change control documents for key servers or comparing patches applied to those recommended by the O/S vendor's web site will not confirm that these security patches were properly approved and documented.

T4-37 A security awareness program should:

A. present the message from a top management perspective.
B. address technical details on specific exploits.
C. be customized to specific groups and roles.
D. be used to promote the need for a strong security department.

C Different groups of employees have different levels of technical understanding and need awareness training that is customized to their needs. It should not be presented from a specific perspective. Specific details on technical exploits should be avoided, since this may provide individuals with knowledge that they might misuse. Also, this is not the best forum to sell the security department in a policing role.

T4-38 The **PRIMARY** objective of security awareness is to:

A. ensure that security policies are read and understood.
B. encourage security-conscious employee behavior.
C. meet legal and regulatory requirements.
D. put employees on notice in case follow-up action for noncompliance is necessary.

B It is most important that security-conscious behavior be encouraged among employees. Ensuring that policies are read and understood, giving employees fair warning of potential disciplinary action, and meeting legal and regulatory requirements are not as important.

T4-39 Which of the following will **BEST** protect against deletion of data files by a disgruntled former employee?

A. Preemployment screening
B. Close monitoring of users
C. Periodic awareness training
D. Efficient termination procedures

D When an employee leaves an organization involuntarily, the former employee may attempt to delete files they were responsible for maintaining. Accordingly, it is very important to ensure timely revocation of all access at the time an individual is terminated. Security awareness training, preemployment screening and monitoring are all important but are not as effective in preventing this situation.

T4-40 Which of the following represents a key area of focus when conducting a penetration test?

A. Data mining
B. Network mapping
C. Task scheduling
D. Customer data

B Network mapping is the process of determining the topology of the network one wishes to penetrate. This is one of the first steps toward determining points of attack in a network. Data mining is associated with *ad hoc* reporting. Task scheduling and customer data are not key areas of focus for penetration testing.

T4-41 Information security can **BEST** be evaluated through which of the following?

A. Value analysis
B. Security metrics
C. Security deliverables list
D. Process improvement models

A Value analysis can be used to illustrate the value proposition of how information security supports the achievement of business objectives. Security metrics measure improvement within the security practice but do not tie to business objectives. Similarly, listing deliverables and creating process improvement models does not tie into business objectives.

T4-42 To help ensure that contract personnel do not obtain access to sensitive information, the information security manager should ensure that contract personnel:

A. have expiration dates set to six months or less.
B. do not function in a system administration role.
C. successfully pass background checks.
D. are assigned system access by the data owner.

B Contract personnel should not be given job duties that provide them with power user or other administrative roles that they could then use to grant themselves access to sensitive files. Setting expiration dates, requiring background checks and having the data owner assign access are all positive elements, but these will not prevent contract personnel from obtaining access to sensitive information.

T4-43 Information security policies should:

A. address operating system vulnerabilities.
B. address the process for communicating a violation.
C. be straightforward and easy to understand.
D. be customized to specific groups and roles.

C As high-level statements, information security policies should be straightforward and easy to understand. They are high-level and, therefore, do not address O/S vulnerabilities or the process for communicating a violation. As policies, they should provide a uniform message to all groups and user roles.

T4-44 When internal auditors are conducting an audit of the security management function, how should security personnel react?

A. Security personnel should focus audit's attention on problems in other areas.
B. Questions by internal audit should be answered briefly and without elaboration.
C. Auditors should be viewed and treated as partners with a common purpose.
D. Any missing log files should be reconstructed and presented to the auditors.

C Internal audit shares a common purpose with information security. Therefore, it should be viewed and treated as a partner in the process to improve information security. Information should not be withheld, deficiencies should not be covered up, and questions should be answered openly and honestly.

T4-45 Which of the following is the **MOST** appropriate method to ensure that the password to open a confidential file is not intercepted along with the file that is transmitted?

A. Delivery path tracing
B. Reverse lookup translation
C. Out-of-band channels
D. Digital signatures

C Out-of-band channels are useful when it is necessary for confidentiality to break a message into two parts that are then sent by different means. Digital signatures only provide nonrepudiation. Reverse lookup translation involves converting an IP address to a username. Delivery path tracing shows the route taken but does not confirm the identity of the sender.

T4-46 What is the **MOST** effective method for ensuring that users do not share files with other users not approved for access?

A. Mandatory access controls
B. Discretionary access controls
C. Lattice-based access controls
D. Role-based access controls

A Mandatory access controls restrict access to files based on the security classification of the file. This prevents users from sharing files with unauthorized users. Role-based access controls grant access according to the role assigned to a user. They do not prohibit file sharing. Discretionary and lattice-based access controls are not as effective as mandatory access controls in preventing file sharing.

T4-47 Which of the following is an inherent weakness of signature-based intrusion detection systems?

A. There are a higher number of false-positives.
B. New attack methods will be missed.
C. Long duration probing will be missed.
D. Attack profiles can be easily spoofed.

B Signature-based intrusion detection systems do not detect new attack methods for which signatures have not yet been developed. False-positives are not necessarily any higher, and spoofing is not relevant in this case. Long duration probing is more likely to fool anomaly-based systems (boiling frog technique).

T4-48 For an organization with operations in multiple countries, when security policies that were based on an international standard are found to be in contradiction with newly created national laws and regulations, it should:

A. be rewritten to conform to the new requirements.
B. remain as is to be in conformity with the international standard.
C. be customized to have a conformity version developed for the country in question.
D. be generalized so as not to contradict any specific national requirements.

C International standards provide an excellent basis upon which to formulate policies and standards. However, organizations with international operations may find it necessary to develop country-specific policies where needed to meet regional requirements. This is preferable to changing the policy for all operations to meet the requirements of one region. In any case, it is important to ensure that local/regional laws and regulations are always adhered to and that policies do not create a contradiction.

T5 RESPONSE MANAGEMENT

T5-1 Which of the following should be determined **FIRST** when establishing a business continuity program?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of the unavailability of systems
C. Location and cost of offsite recovery facilities
D. Composition and mission of individual recovery teams

B Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives to be determined, which in turn affects the location and cost of offsite recovery facilities and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

T5-2 A desktop computer that was involved in a computer security incident should be secured as evidence by:

A. disconnecting the computer from all power sources.
B. using remote access software them to access the computer.
C. encrypting the files and uploading them to a secure server.
D. copying the files using the O/S to write-once media.

A To preserve the integrity of the desktop computer as an item of evidence, it should be immediately disconnected from all sources of power. Any attempt to access the information on the computer by copying, uploading or accessing them remotely will change O/S and temporary files on the computer and invalidate it as admissible evidence.

T5-3 A company has a network of branch offices each possessing their own local file/print and mail servers; however, all key systems reside at corporate headquarters. Branch offices individually contract with vendors who provide hot sites that include backup servers and work area space. Which of the following would indicate a weakness in branch office recovery capability?

A. Exclusive use of the hot site is limited to six weeks.
B. The hot site may have to be shared with other customers.
C. A time stamp of declaration determines the priority of access to the facility.
D. The contract does not include network connectivity.

D Without network connectivity, the branch office will not have access to e-mail or key corporate systems. Sharing a hot site facility is sometimes necessary in the case of a major disaster. Also, the first-come, first-served policy usually determines priority of access based on general industry practice. Access to a hot site is not indefinite. Customers will be relocated to a long-term facility.

T5-4 Which of the following actions should be taken when an online trading company discovers a network attack in progress?

A. Shut off all network access points.
B. Dump all event logs to removable media.
C. Isolate the affected network segment.
D. Enable trace logging on all events.

C Isolating the affected network segment will mitigate the immediate threat while allowing unaffected portions of the business to continue processing. Shutting off all network access points would create a denial of service that could result in loss of revenue. Dumping event logs and enabling trace logging, while perhaps useful, would not mitigate the immediate threat posed by the network attack.

T5-5 The **BEST** method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. firewalls.
B. bastion hosts.
C. decoy files.
D. screened subnets.

C Decoy files, often referred to as honeypots, are the best choice for diverting a hacker away from critical files and alerting security of the hacker's presence. Firewalls and bastion hosts attempt to keep the hacker out while screened subnets or DMZs provide a middle ground between the trusted internal network and the external untrusted Internet.

T5-6 The **FIRST** priority when responding to a major security incident is:

A. documentation.
B. monitoring.
C. restoration.
D. containment.

D The first priority in responding to a security incident is to contain it to limit the impact. Documentation, monitoring and restoration are all important, but they should follow containment.

T5-7 Which of the following is the **MOST** important to ensure a successful recovery?

A. Backup media is stored offsite.
B. Patches and firmware are up to date.
C. More than one hot site is available.
D. Data communication lines are regularly tested.

A Unless backup media is available, all other preparations become meaningless. Patches and firmware are important, but can usually be remedied. Having a secondary hot site is also important, but not as important as having backup media available. Similarly, data communication lines should be tested, but this is not as critical.

T5-8 Which of the following is the **MOST** important element in ensuring the success of a disaster recovery test at a vendor provided hot site?

A. Tests are scheduled on weekends.
B. Network IP addresses are predefined.
C. Equipment at the hot site is identical.
D. Organizational management is supportive.

D Disaster recovery testing requires the allocation of sufficient resources to be successful. Without the support of management, these resources will not be available and, as a result, testing will suffer. Testing on weekends can be advantageous, but this is not the most important choice. As vendor-provided hot sites are in a state of constant change, it is not always possible to have network addresses defined in advance. Although it would be ideal to provide for identical equipment at the hot site, this is not always practical as multiple customers must be served and equipment specifications will, therefore, vary.

T5-9 At the conclusion of a disaster recovery test, which of the following should always be performed prior to leaving the vendor's hot site facility?

A. Erase data and software from devices.
B. Conduct a meeting to evaluate the test.
C. Complete an assessment of the hot site provider.
D. Schedule the date and time of the next test.

A For security and privacy reasons, all organizational data and software should be erased prior to departure. Evaluations should occur back at the office after everyone is rested. Future tests should normally be scheduled months in advance.

T5-10 An incident response policy should contain:

A. telephone trees.
B. escalation criteria.
C. press release templates.
D. list of critical backup files.

B Escalation criteria, indicating the circumstances under which specific actions are to be undertaken, should be contained within an incident response policy. Telephone trees, press release templates and lists of critical backup files are too detailed to be included in a policy document.

T5-11 The **PRIMARY** objective for managing a security incident involving a successful penetration should be to:

A. allow business processes to continue during the response.
B. allow the security team to assess the attack profile.
C. permit the incident to continue to trace the source.
D. evaluate the incident management process for deficiencies.

A Since information security objectives should always be linked to the objectives of the business, it is imperative that business processes be allowed to continue whenever possible. Only when there is no alternative should these processes be interrupted. Although it is important to allow the security team to assess the characteristics of an attack, this is subordinate to the needs of the business. Permitting an incident to continue may expose the organization to additional damage. Evaluating the incident management process for deficiencies is valuable, but it too is subordinate to allowing business processes to continue.

T5-12 The **MOST** likely cause when a commercially developed security mechanism fails to perform as intended is:

A. buffer overflow.
B. misconfiguration.
C. corrupted files.
D. a hard drive crash.

B Misconfiguration is the most likely cause when a commercially developed security mechanism fails. Any mechanism, no matter how well designed, is subject to compromise when it is misconfigured. Buffer overflows, corrupted files and hard drive crashes are less likely causes.

T5-13 A postincident review should be conducted by the incident management team to determine:

A. what electronic evidence is relevant.
B. ways to improve the response process.
C. why the attack was launched by the hacker.
D. which individuals failed to perform their duties.

B Postincident reviews are beneficial in determining ways to improve the response process. Evaluating the relevance of evidence, why the attack was launched and who failed to respond appropriately are not the primary purposes for such a meeting.

T5-14 An organization with multiple data centers has terminated its external hot site contract and has designated one of its own data centers as the recovery site. The **MOST** important concern is the:

A. communication line capacity between data centers.
B. current processing capacity loads at data centers.
C. differences in logical and physical security at each center.
D. synchronization of system software release versions.

B If data centers are operating at or near capacity, it may prove difficult to recover critical operations at an alternate data center. Although line capacity is important from a mirroring perspective, this is secondary to having the necessary capacity to restore critical systems. Differences in logical and physical security and synchronization of system software releases are, by comparison, much easier issues to overcome and, therefore, are of less concern.

T5-15 Which of the following is the **MOST** important factor in determining whether a disaster recovery test is successful?

A. Only materials taken from offsite storage are used.
B. Participants are not informed in advance when the test is to be held.
C. Degree of attainment of predetermined test objectives is measured.
D. Key systems are restored to identical O/S releases and hardware.

C To ensure that a disaster recovery test is successful, it is most important to determine the degree to which predetermined test objectives are met. Although ensuring that only materials taken from offsite storage are used in the test is important, this is not as critical in determining a test's success. Similarly, whether or not a test was unannounced does not necessarily make it a more successful test. The use of identical O/S versions and hardware is not always possible at a hot site and, in any case, does not assure the success of a test.

T5-16 Which of the following is **MOST** important when deciding whether to build an alternate facility or subscribe to a hot site operated by a third party?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of losing different systems
C. Location and cost of commercial recovery facilities
D. Estimated annualized loss expectancy (ALE) from key risks

C The location and cost of commercial recovery facilities will largely determine the viability of such an option. The cost to rebuild an information processing facility is not relevant since only a fraction of the total processing capacity would be considered critical at the time of the disaster. The incremental daily cost of losing different systems and the estimated ALE would not distinguish between whether or not a commercial facility should be chosen.

T5-17 A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. The virus is highly malicious and immediately erases all user files. Antivirus signature files to identify this virus are not yet available from the software vendor. Which of the following should be performed first in response to this e-mail virus?

A. Quarantine all picture files stored on file servers.
B. Block all e-mails containing picture file attachments.
C. Shut down all mail servers connected to the Internet.
D. Block incoming Internet mail but permit outgoing mail.

B Until signature files can be updated, incoming e-mail containing picture file attachments should be blocked. Quarantining picture files already stored on file servers would not be effective, as these files must be intercepted before they are opened. Shutting down all mail servers or blocking all incoming mail would be overkill, as only those e-mails containing attached picture files are in question.

T5-18 When a large organization discovers that it is the subject of a network probe, which of the following actions should be taken?

A. Reboot the router connecting the DMZ to the firewall.
B. Power down all servers located on the DMZ segment.
C. Monitor the probe and isolate the affected segment.
D. Enable server trace logging on the affected segment.

C In the case of a probe, the situation should be monitored and the affected network segment isolated. Rebooting the router, powering down the DMZ servers and enabling server trace routing are not warranted.

T5-19 Which of the following are the **MOST** important criteria for the selection of business continuity planning software?

A. Product market share and annualized cost
B. Ability to interface with financial systems
C. Links to commercial hot site databases
D. Scalability and ease of customization

D For a product to be useful, it must be scalable to the size of the organization, and it must be customizable to include specific forms and documentation required by the organization. Market share and annualized cost, links to databases, and ability to interface with financial are secondary in nature.

T5-20 Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

A. A hot site facility is subject to sharing, if there are multiple disaster declarations.
B. All equipment is provided at time of disaster, not on floor.
C. The facility is subject to a first-come, first-served declaration policy.
D. Equipment may be substituted with equivalent models.

B When equipment is provided at time of disaster (ATOD), not on floor, means that the equipment is not available but will be acquired by the commercial hot site provider on a best-efforts basis. This leaves the customer at the mercy of the marketplace. If equipment is not immediately available, the recovery will be delayed. Many commercial providers do require sharing facilities in cases where there are multiple simultaneous declarations and that priority may be established on a first-come, first-served basis. It is also common for the provider to substitute equivalent or better equipment, as they are frequently upgrading and changing equipment.

T5-21 Which of the following should be performed **FIRST** in the aftermath of a denial-of-service attack?

A. Restore servers from backup media stored offsite.
B. Conduct an assessment to determine system status.
C. Perform a business impact analysis of the outage.
D. Implement internal network address translation.

B An assessment should be conducted to determine whether any permanent damage occurred. It is not necessary at this point to rebuild any servers. A business impact analysis of the outage will not provide any immediate benefit nor will implementing network address translation on the internal network.

T5-22 What is the **MOST** important element to ensure the success of a business continuity program?

A. Detailed technical recovery plans are maintained.
B. Network redundancy is maintained through separate providers.
C. Hot site equipment needs are reconfirmed on a quarterly basis.
D. Organizational management is very supportive.

D Business continuity requires allocation of sufficient resources to be successful. These resources have to be diverted away from normal business tasks. Without the support of organizational management, these resources will not be made available and, as a result, the overall business continuity program will suffer. Network redundancy, regular reevaluation of equipment needs and detailed technical plans are important, but not as important as management support.

T5-23 Which of the following would be the **BEST** choice for recovery of an Internet-based ordering system?

A. Cold site
B. Warm site
C. Mobile site
D. Mirrored site

D A mirrored site would be the best choice, since time would be of the essence in restoring such a system. Cold, warm and mobile sites would all require too much time to set up and become operational.

T5-24 A business continuity policy document should contain which of the following?

A. Telephone trees
B. Declaration criteria
C. Press release templates
D. A listing of critical backup files

B Declaration criteria indicating the circumstances under which specific actions will be undertaken should be contained within a business continuity policy. Telephone trees, press release templates and listings of critical backup files are too detailed to include in a policy document.

T5-25 The **PRIMARY** purpose of installing an intrusion detection system is to identify:

A. weaknesses in network security.
B. ways to improve the response process.
C. how an attack was launched on the network.
D. potential attacks on the internal network.

D The most important function of an intrusion detection system is to identify potential attacks on the network. Identifying how the attack was launched and ways to improve the response process are secondary. It is not designed specifically to identify weaknesses in network security.

T5-26 How should a production server that was involved in a computer security incident be secured as evidence?

A. Use remote access software to backup the server.
B. Copy the files using the O/S to write-once media.
C. Encrypt all files and upload to a backup server.
D. Disconnect the server from all power sources.

D To preserve the integrity of the server as an item of evidence, it should be immediately disconnected from all sources of power. Any attempt to access the information on the computer by copying, uploading or accessing them remotely will change O/S and temporary files on the computer and invalidate it as admissible evidence.

SAMPLE EXAM

1. Which of the following is **MOST** indicative of senior management support of an information security function?

   A. Security awareness training is offered.
   B. Security polices are reviewed annually.
   C. A computer incident management team exists.
   D. The security manager reports directly to the chief executive officer (CEO).

2. Risk mitigation would normally include:

   A. assessment.
   B. acceptance.
   C. evaluation.
   D. monitoring.

3. A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. The virus is highly malicious and immediately erases all user files. Antivirus signature files to identify this virus are not yet available from the software vendor. Which of the following should be performed first in response to this e-mail virus?

   A. Quarantine all picture files stored on file servers.
   B. Block all e-mails containing picture file attachments.
   C. Shut down all mail servers connected to the Internet.
   D. Block incoming Internet mail but permit outgoing mail.

4. Which of the following is the **MOST** likely to change an organization's culture to one that is more security conscious?

   A. Security policies and procedures
   B. Periodic penetration testing
   C. Security steering committees
   D. Security awareness campaigns

5. Acceptable risk is achieved when:

   A. residual risk is minimized.
   B. transferred risk is minimized.
   C. control risk equals acceptable risk.
   D. residual risk equals transferred risk.

6. What is the **MOST** important element to ensure the success of a business continuity program?

   A. Detailed technical recovery plans are maintained.
   B. Network redundancy is maintained through separate providers.
   C. Hot site equipment needs are reconfirmed on a quarterly basis.
   D. Organizational management is very supportive.

7. Which of the following would be the **BEST** choice for recovery of an Internet-based ordering system?

A. Cold site
B. Warm site
C. Mobile site
D. Mirrored site

8. Which of the following should be performed **FIRST** in the aftermath of a denial-of-service attack?

A. Restore servers from backup media stored offsite.
B. Conduct an assessment to determine system status.
C. Perform a business impact analysis of the outage.
D. Implement internal network address translation.

9. Information security policies should:

A. address operating system vulnerabilities.
B. address the process for communicating a violation.
C. be straightforward and easy to understand.
D. be customized to specific groups and roles.

10. The use of and relationships among security technologies are **BEST** defined through which of the following?

A. Security metrics
B. Network topology
C. Security architecture
D. Process improvement models

11. The **MOST** important factor in planning for the long-term retention of electronically stored business records is to take into account potential changes in:

A. storage capacity and shelf life.
B. regulatory and legal requirements.
C. business strategy and direction.
D. application systems and media.

12. How should a production server that was involved in a computer security incident be secured as evidence?

A. Use remote access software to backup the server.
B. Copy the files using the O/S to write-once media.
C. Encrypt all files and upload to a backup server.
D. Disconnect the server from all power sources.

13. Which of the following is **MOST** important when deciding whether to build an alternate facility or subscribe to a hot site operated by a third party?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of losing different systems
C. Location and cost of commercial recovery facilities
D. Estimated annualized loss expectancy (ALE) from key risks

14. Which of the following are mandatory rules and regulations?

A. Policies
B. Procedures
C. Standards
D. Best practices

15. Which of the following would normally **NOT** be covered in an insurance policy for computer equipment coverage?

A. Equipment leased to another company by the insured
B. Equipment leased to the insured by another company
C. Equipment under the direct control of the insured
D. Equipment purchased on an installment plan

16. The biometric access control method that has the **BEST** acceptance in terms of user attitudes is:

A. facial recognition.
B. iris scanning.
C. retina scanning.
D. fingerprint scanning.

17. In cases where application-level security controlled by business process owners is found to be poorly managed, improvement can **BEST** be obtained through:

A. periodic reminder memorandums.
B. circulation of best practices.
C. policies signed by IT management.
D. education sessions and periodic reviews.

18. Which of the following individuals would be in the **BEST** position to sponsor the creation of an information security steering group?

A. Chief security officer
B. Chief operating officer
C. Chief internal auditor
D. Chief legal counsel

19. Which of the following is **MOST** indicative of the failure of information security governance within an organization?

A. The information security department has had difficulty filling vacancies.
B. The information security policy manual is only available in electronic form.
C. The information security oversight committee only meets quarterly.
D. The data center manager has final sign-off responsibility on all security projects.

20. A firewall should be placed on a(n):

A. web server.
B. intrusion detection system (IDS) server.
C. screened subnet.
D. domain boundary.

21. During which phase of development is it **MOST** appropriate to begin assessing the risk of a new application system?

A. Feasibility
B. Design
C. Development
D. Testing

22. Which of the following tools is **MOST** appropriate for judging whether information security governance objectives are being met?

A. SWOT analysis
B. Waterfall chart
C. Gap analysis
D. Balanced scorecard

23. Identification and prioritization of risk enables project managers to:

A. establish implementation milestones.
B. reduce the overall amount of testing.
C. direct attention on areas of greatest impact.
D. accelerate completion of the feasibility study.

24. What is an appropriate frequency for updating antivirus signature files for antivirus software on production servers?

A. limit the scope to a benchmark of similar companies.
B. assume an equal degree of protection for all assets.
C. address the potential size and likelihood of loss.
D. give more weight to the likelihood vs. the size of the loss.

25. Minimum standards for securing the technical infrastructure should be defined in the security:

A. strategy.
B. guidelines.
C. model.
D. architecture.

26. Which of the following tools is **MOST** appropriate for determining how long a security project will take to implement?

A. Gantt chart
B. Waterfall chart
C. Critical path method
D. Balanced scorecard method

27. Which of the following would **BEST** indicate the success of information security governance within an organization?

A. The steering committee approves all security projects.
B. The security policy manual is distributed to all managers.
C. Security procedures are accessible on the company intranet.
D. The corporate network utilizes multiple screened subnets.

28. A risk assessment should be conducted:

A. once for each business process and subprocess.
B. every three to five years for critical business processes.
C. by external parties to maintain objectivity.
D. annually or whenever there is a significant change.

29. The **MOST** likely cause when a commercially developed security mechanism fails to perform as intended is:

A. buffer overflow.
B. misconfiguration.
C. corrupted files.
D. a hard drive crash.

30. Which of the following will **BEST** prevent externally generated security attacks?

A. Static IP addressing
B. Network address translation
C. Background checks for temporary employees
D. Writing all computer logs to removable media

31. Security technologies should be selected **PRIMARILY** on the basis of their:

A. ability to mitigate audit findings.
B. evaluations in trade publications.
C. use of new and emerging technologies.
D. benefits in comparison to their costs.

32. When residual risk is minimized:

A. acceptable risk is achieved.
B. transferred risk is minimized.
C. control risk is reduced to zero.
D. residual risk equals transferred risk.

33. What is the **BEST** way to ensure that contract programmers comply with organizational security policies?

A. Explicitly refer to contractors in the security standards.
B. Have the contractors acknowledge in writing that they have read-all security policies.
C. Create penalties for noncompliance in the contracting agreement.
D. Perform periodic security reviews of the contractors.

34. An organization with multiple data centers has terminated its external hot site contract and has designated one of its own data centers as the recovery site. The **MOST** important concern is the:

A. communication line capacity between data centers.
B. current processing capacity loads at data centers.
C. differences in logical and physical security at each center.
D. synchronization of system software release versions.

35. The cost of implementing a security control should not exceed the:

A. annualized loss expectancy.
B. cost of an incident.
C. expected benefits.
D. opportunity costs.

36. The **BEST** way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

A. perform penetration testing.
B. establish security baselines.
C. implement vendor default settings.
D. link policies to an independent standard.

37. A security awareness program should:

A. present the message from a top management perspective.
B. address technical details on specific exploits.
C. be customized to specific groups and roles.
D. be used to promote the need for a strong security department.

38. In a business impact analysis, the value of an information system should be based on the overall:

A. cost to design.
B. cost to re-create.
C. cost if unavailable.
D. value to competitors.

39. The **BEST** way to integrate risk management into life cycle processes is through:

A. policy development.
B. change management.
C. awareness training.
D. regular monitoring.

40. The **BEST** metric for evaluating the effectiveness of a firewall is the:

A. number of attacks blocked.
B. number of packets dropped.
C. average throughput rate.
D. number of firewall rules.

41. The recovery time objective is reached at which of the following milestones?

A. Disaster declaration
B. Recovery of the backups
C. Restoration of the system
D. Return to normal processing

42. The need for privacy policies is **PRIMARILY** driven by which of the following?
A. Customer demands
B. Competitive advantage
C. Threat of lawsuits
D. Regulatory requirements

43. Information security risk is increased the **MOST** when:

A. procedures are not enforced.
B. change management is lacking.
C. systems are developed in-house.
D. systems are complex and distributed.

44. Which of the following should be determined **FIRST** when establishing a business continuity program?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of the unavailability of systems
C. Location and cost of offsite recovery facilities
D. Composition and mission of individual recovery teams

45. Which of the following are the **MOST** important criteria for the selection of business continuity planning software?

A. Product market share and annualized cost
B. Ability to interface with financial systems
C. Links to commercial hot site databases
D. Scalability and ease of customization

46. Access to a sensitive intranet application by mobile users can **BEST** be accomplished through:

A. data encryption.
B. digital signatures.
C. strong passwords.
D. two-factor authentication.

47. Which of the following is the **MOST** important sign-off for migrating an order processing system from a test environment to a production environment?

A. User management
B. Security management
C. Operations management
D. Database management

48. Ultimately, management's decision on the level of acceptable risk is a:

A. subjective decision.
B. qualitative decision.
C. probability decision.
D. quantitative decision.

49. The determination as to whether a risk has been reduced to an acceptable level should be determined by:

A. organizational requirements.
B. information systems requirements.
C. information security requirements.
D. international standards of best practice.

50. When an emergency security patch is received via electronic mail, the patch should **FIRST** be:

A. loaded onto an isolated test machine.
B. decompiled to check for malicious code.
C. validated to ensure its authenticity.
D. copied onto write-once media to prevent tampering.

51. It is **MOST** likely that a data owner will not need to sign authorization request forms for each user who will access the owner's data when:

A. the data are read-only historical data.
B. discretionary access control is utilized.
C. the authorization was provided by the requestor's supervisor.
D. role-based access control is utilized.

52. Which of the following is the **MOST** effective in preventing attacks that exploit weaknesses in operating systems?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

53. When an organization hires a new information security manager, which of the following goals should this individual pursue first?

A. Develop a security architecture.
B. Build senior management support.
C. Assemble an experienced staff.
D. Interview peer organizations.

54. Risk management programs are designed to reduce risk to:

A. a level that is too small to be measurable.
B. the point at which the expense exceeds the benefit.
C. a level that the organization is willing to accept.
D. a rate of return that equals the current cost of capital.

55. Which of the following is the **MOST** important factor in determining whether a disaster recovery test is successful?

A. Only materials taken from offsite storage are used.
B. Participants are not informed in advance when the test is to be held.
C. Degree of attainment of predetermined test objectives is measured.
D. Key systems are restored to identical O/S releases and hardware.

56. Which of the following would generally have the **MOST** significant negative impact on an organization?

A. Theft of computer software
B. Interruption of utility services
C. Loss of customer confidence
D. Internal fraud resulting in monetary loss

57. Which of the following risks would **BEST** be assessed using qualitative risk assessment techniques?

A. The theft of purchased software
B. A power outage lasting 24 hours
C. A permanent decline in customer confidence
D. The loss of e-mail for 72 hours due to a virus attack

58. The **BEST** way to ensure that an external service provider complies with organizational security policies is to:

A. explicitly refer to the provider in the security policies.
B. have the provider acknowledge in writing reading all policies.
C. refer to policies in the service level agreement.
D. perform periodic reviews of the service provider.

59. Which of the following will **MOST** reduce the likelihood of an unauthorized individual gaining access to computing resources by pretending to be an authorized individual needing to have their password reset?

A. Performing reviews of password resets
B. Conducting security awareness programs
C. Increasing the frequency of password changes
D. Implementing automatic password syntax checking

60. A business unit desires to deploy a new technology in a manner that places it in violation of existing information security standards. After discussions with the business unit, they insist on proceeding with the deployment to take advantage of highly desirable market conditions. What immediate action should the information security manager take?

A. Enforce the existing security standard.
B. Change the standard to permit the deployment.
C. Perform a risk analysis to quantify the risk.
D. Permit a 90-day window to see if a problem occurs.

61. In performing a risk assessment on the impact of losing a database server, the value of the server should be calculated using the:

A. original cost to acquire the server.
B. value of the data stored on the server.
C. annualized loss expectancy (ALE) for the server.
D. new cost to obtain a replacement server.

62. The chief information security officer (CISO) generally chairs which of the following?

A. The executive steering committee
B. The information technology management committee
C. The enterprise security governance board
D. The service delivery/operations management team

63. The **MOST** inappropriate reporting base for the information security management function would be to report to the:

A. director of financial management.
B. risk management director.
C. business division manager.
D. infrastructure director.

64. Of the following, the **BEST** metric for evaluating the effectiveness of security awareness training is the number of:

A. password resets.
B. reported incidents.
C. individuals trained.
D. access rule violations.

65. Which of the following metrics would be the **MOST** useful in measuring how well information security is monitoring violation logs? The number of:

A. penetration attempts investigated.
B. violation log reports reviewed.
C. violation log entries reviewed.
D. hours charged to the review process.

66. The recovery point objective (RPO) is at which of the following milestones?

A. Disaster declaration date
B. Offsite media creation date
C. Restoration of the system
D. Return to normal processing

67. Successful social engineering attacks can **BEST** be prevented through:

A. preemployment screening.
B. close monitoring of users.
C. periodic awareness training.
D. efficient termination procedures.

68. The main advantage of involving the owner of a business process in the evaluation and management of information security risks is their understanding of the:

A. infrastructure risks.
B. industry best practices.
C. security mechanisms.
D. specific business risks.

69. Information security priorities may occasionally override:

A. technical requirements.
B. regulatory requirements.
C. privacy requirements.
D. business requirements.

70. Which of the following is often poorly handled when administering IDs for contract programmers?

A. Creation
B. Modification
C. Resetting
D. Revocation

71. A perpetrator calls an authorized user and pretends to be a network administrator who needs to know the user's password to perform a test of the user's connectivity to the network. In this scenario, which of the following will **MOST** likely reduce the likelihood of this unauthorized individual gaining access to computing resources?

A. Implementing on-screen masking of passwords
B. Conducting periodic security awareness programs
C. Increasing the frequency of password changes
D. Requiring that passwords not be disclosed to others in security policies

72. Which of the following **BEST** indicates a successful risk management practice?

A. Overall risk is quantified.
B. Inherent risk is eliminated.
C. Residual risk is minimized.
D. Control risk is tied to business units.

73. Which of the following is the **MOST** appropriate individual to implement and maintain the level of information security needed for a specific business application?

A. System developer
B. Quality control manager
C. System custodian
D. System data owner

74. When an O/S patch that will enhance system security cannot be applied because it will adversely impact the ability of a critical application to operate on that platform, which of the following should occur?

A. The O/S patch should be applied and the application then rewritten to conform to the upgraded O/S.
B. A mitigating control should be identified that will compensate for not installing the O/S patch.
C. The O/S patch should be altered to allow the application to run in a privileged state.
D. The application should be switched to run on a test platform, while the production platform is tuned to allow the patch and application to coexist.

75. Qualitative risk analysis is **MOST** appropriate when assessment data:

A. spans multiple industries.
B. contains percentage estimates.
C. is more than seven years old.
D. contains subjective information.

76. Which of the following should be developed **FIRST**?

A. Standards
B. Procedures
C. Policies
D. Guidelines

77. Which of the following is the **MOST** important to ensure a successful recovery?

A. Backup media is stored offsite.
B. Patches and firmware are up to date.
C. More than one hot site is available.
D. Data communication lines are regularly tested.

78. Who is in the **BEST** position to champion the development and ensure the success of an information security program?

A. Internal audit
B. External audit
C. Senior management
D. Infrastructure management

79. Who should be the formal sponsor for the design and implementation of a new security infrastructure in a large global enterprise?

A. Chief security officer (CSO)
B. Chief operating officer (COO)
C. Chief privacy officer (CPO)
D. Chief legal counsel (CLC)

80. Owners of information should be responsible for its:

A. classification.
B. protection.
C. recoverability.
D. availability.

81. Investments in information security technologies should be based on:

A. a vulnerability assessment.
B. a value analysis.
C. the business climate.
D. audit recommendations.

82. The **MOST** important reason for conducting the same risk assessment more than once is because:

A. mistakes are often made in the initial reviews.
B. security risks are subject to frequent change.
C. different reviewers will analyze risk factors differently.
D. it shows management that the security staff is adding value.

83. What will **BEST** tie information security to business objectives?

A. Value analysis
B. Security metrics
C. Deliverables list
D. Process improvement model

84. Prior to having a third party perform an attack and penetration test against an organization, the **MOST** important action is to ensure that:

A. the third party provides a demonstration on a test system.
B. goals and objectives are clearly defined.
C. the technical staff has been briefed on what to expect.
D. special backups of production servers are taken.

85. Which of the following is the **MOST** effective in preventing weaknesses from being introduced during the life cycle of a system?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

86. When a minor security flaw is found in a new system that is about to be moved into production, this should be reported to:

A. senior management in a quarterly report.
B. users who may be impacted by the flaw.
C. senior management in an immediate report.
D. customers who may be impacted by the flaw.

87. When a significant security flaw is found in a new system that is about to be moved into production, it should be reported to:

A. senior management in a quarterly report.
B. users who may be impacted by the flaw.
C. senior management in an immediate report.
D. customers who may be impacted by the flaw.

88. When contracting with an outsourcer to provide security administration the most important contractual element is the:

A. right-to-terminate clause.
B. limitations of liability.
C. service level agreements.
D. hold-harmless agreements.

89. Which of the following will **BEST** protect against deletion of data files by a disgruntled former employee?

A. Preemployment screening
B. Close monitoring of users
C. Periodic awareness training
D. Efficient termination procedures

90. When internal auditors are conducting an audit of the security management function, how should security personnel react?

A. Security personnel should focus audit's attention on problems in other areas.
B. Questions by internal audit should be answered briefly and without elaboration.
C. Auditors should be viewed and treated as partners with a common purpose.
D. Any missing log files should be reconstructed and presented to the auditors.

91. Which of the following will **BEST** protect an organization from internal security attacks?

A. Static IP addressing
B. Internal address translation
C. Prospective employee background checks
D. Employees certifying that they have read policies

92. Of the following, the **BEST** method for ensuring that temporary employees do not receive excessive access rights is:

A. mandatory access controls.
B. discretionary access controls.
C. lattice-based access controls.
D. role-based access controls.

93. An extranet server should be placed:

A. outside the firewall.
B. on the firewall server.
C. on a screened subnet.
D. on the external router.

94. When a security standard conflicts with a business objective, the situation should be resolved by:

A. changing the security standard.
B. enforcing the security standard.
C. performing a risk analysis.
D. allowing an exception to the standard.

95. The **MOST** appropriate individual to determine the level of information security needed for a specific business application is the:

A. system developer.
B. infrastructure manager.
C. system custodian.
D. system data owner.

96. At the conclusion of a disaster recovery test, which of the following should always be performed prior to leaving the vendor's hot site facility?

A. Erase data and software from devices.
B. Conduct a meeting to evaluate the test.
C. Complete an assessment of the hot site provider.
D. Schedule the date and time of the next test.

97. The **PRIMARY** objective of security awareness is to:

A. ensure that security policies are read and understood.
B. encourage security-conscious employee behavior.
C. meet legal and regulatory requirements.
D. put employees on notice in case follow-up action for noncompliance is necessary.

98. When attempting to implement a new enterprise resource planning (ERP) system using a purchased solution, which of the following will take the **LONGEST** to complete?

A. Feasibility study and product selection
B. Loading of program and database libraries
C. Product customization and integration
D. User acceptance testing and sign-off

99. Quantitative risk analysis is **MOST** appropriate when assessment data:

A. include customer perceptions.
B. contain percentage estimates.
C. are lacking in specific details.
D. contain subjective information.

100. Which of the following is the **BEST** method for setting up a new user's initial password for system access?

A. E-mail the password to the user.
B. Have the manager deliver the password.
C. Set the initial password to a null value.
D. Set the initial password equal to the user ID.

101. Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

A. Biometric authentication
B. Embedded steganographic techniques
C. Two-factor authentication
D. Embedded digital signature

102. Which of the following change management activities would be an indicator that normal operational procedures are being overridden? A high percentage of:

A. similar change requests.
B. change request postponements.
C. cancelled change requests.
D. emergency change requests.

103. It would be **MOST** difficult to accurately estimate the likelihood of which of the following threats?

A. Flood
B. Earthquake
C. Explosion
D. Windstorm

104. A desktop computer that was involved in a computer security incident should be secured as evidence by:

A. disconnecting the computer from all power sources.
B. using remote access software them to access the computer.
C. encrypting the files and uploading them to a secure server.
D. copying the files using the O/S to write-once media.

105. Which of the following activities is **MOST** likely to lead to the introduction of weaknesses in security software?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

106. Out-of-band communications are **MOST** appropriate when transmitting:

A. password changes.
B. encrypted files.
C. large data files.
D. nonstandard protocols.

107. Which of the following **BEST** describes the probability that a successful attack will occur?

A. The value of the target and level of protection is high.
B. The motivation and ability of the attacker is high.
C. The value of the target is high and protection is low.
D. The motivation of the attacker and value of the target is high.

108. Which of the following will **BEST** ensure that management takes ownership in the decision-making process for information security?

A. Security policies and procedures
B. Annual self-assessment by management
C. Security steering committees
D. Security awareness campaigns

109. What is the **BEST** way to ensure that an intruder who successfully penetrates a network will be detected before significant damage is inflicted?

A. Perform periodic penetration testing.
B. Establish minimum security baselines.
C. Implement vendor default settings.
D. Install a honeypot on the network.

110. Information security governance is **PRIMARILY** driven by:

A. technology constraints.
B. regulatory requirements.
C. litigation potential.
D. business strategy.

111. Which of the following represents the major focus of privacy regulations?

A. Data mining
B. Penetration testing
C. Supplier data
D. Customer data

112. Which of the following is an inherent weakness of signature-based intrusion detection systems?

A. There are a higher number of false-positives.
B. New attack methods will be missed.
C. Long duration probing will be missed.
D. Attack profiles can be easily spoofed.

113. Which of the following areas is **MOST** susceptible to the introduction of security weaknesses?

A. Database management
B. Tape backup management
C. Configuration management
D. Incident response management

114. A company has a network of branch offices each possessing their own local file/print and mail servers; however, all key systems reside at corporate headquarters. Branch offices individually contract with vendors who provide hot sites that include backup servers and work area space. Which of the following would indicate a weakness in branch office recovery capability?

A. Exclusive use of the hot site is limited to six weeks.
B. The hot site may have to be shared with other customers.
C. A time stamp of declaration determines the priority of access to the facility.
D. The contract does not include network connectivity.

115. The **BEST** way to ensure that information security policies are followed is to:

A. distribute printed copies to all employees.
B. perform periodic reviews for compliance.
C. tie policies to a recognized international standard.
D. establish a telephone number to report policy abuses.

116. An incident response policy should contain:

A. telephone trees.
B. escalation criteria.
C. press release templates.
D. list of critical backup files.

117. Custodians of information are generally responsible for its:

A. classification.
B. accuracy.
C. recoverability.
D. completeness.

118. Which of the following activities is **MOST** likely to increase the difficulty of totally eradicating malicious code that is not immediately detected?

A. Applying patches
B. Changing access rules
C. Upgrading hardware
D. Backing up files

119. An intrusion detection system (IDS) should be placed:

A. outside the firewall
B. on the firewall server
C. on a screened subnet
D. on the external router.

120. The **PRIMARY** purpose of installing an intrusion detection system is to identify:

A. weaknesses in network security.
B. ways to improve the response process.
C. how an attack was launched on the network.
D. potential attacks on the internal network.

121. Which of the following should be the **FIRST** step in developing an information security strategy?

A. Perform a technical vulnerabilities assessment.
B. Analyze the current business strategy.
C. Perform a business impact analysis.
D. Assess the current levels of security awareness.

122. The **FIRST** priority when responding to a major security incident is:

A. documentation.
B. monitoring.
C. restoration.
D. containment.

123. A web-based business application that utilizes public keys and two-factor authentication is being migrated from test to production. Which of the following is the **MOST** important sign-off for this migration?

A. User management
B. Network management
C. Operations management
D. Database management

124. Which of the following actions should be taken when an online trading company discovers a network attack in progress?

A. Shut off all network access points.
B. Dump all event logs to removable media.
C. Isolate the affected network segment.
D. Enable trace logging on all events.

125. A risk analysis should:

A. limit the scope to a benchmark of similar companies.
B. assume an equal degree of protection for all assets.
C. address the potential size and likelihood of loss.
D. give more weight to the likelihood vs. the size of the loss.

126. Which of the following environments would be the **MOST** likely to deviate from organizational security policies?

A. Locally managed file server
B. Enterprise data warehouse
C. Load-balanced, web server cluster
D. Centrally managed data switch

127. Which of the following would be the **MOST** appropriate application of gap analysis?

A. Evaluating a business impact analysis (BIA)
B. Developing a balanced business scorecard
C. Demonstrating the relationship between variables
D. Measuring current state vs. desired future state

128. Which of the following are **MOST** likely to be discretionary?

A. Policies
B. Procedures
C. Guidelines
D. Standards

129. Security policies should be aligned **MOST** closely to:

A. industry best practices.
B. the needs of the organization.
C. globally accepted best practices.
D. local laws and regulations.

130. The value of information assets is **BEST** determined by:

A. individual business managers.
B. business systems developers.
C. information security management.
D. peer companies' industry averages.

131. Nonrepudiation can **BEST** be assured by using:

A. delivery path tracing.
B. reverse lookup translation.
C. out-of-band channels.
D. digital signatures.

132. Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

A. A hot site facility is subject to sharing, if there are multiple disaster declarations.
B. All equipment is provided at time of disaster, not on floor.
C. The facility is subject to a first-come, first-served declaration policy.
D. Equipment may be substituted with equivalent models.

133. Which of the following is in the **BEST** position to approve plans to implement the information security governance framework?

A. Internal audit
B. Legal counsel
C. Senior management
D. Infrastructure management

134. The greatest reduction in overhead costs for security administration would be provided by:

A. mandatory access control.
B. role-based access control.
C. decentralized access control.
D. discretionary access control.

135. What is the **BEST** method to verify that all security patches applied to servers were properly documented?

A. Trace change control requests to O/S patch logs.
B. Trace O/S patch logs to the O/S vendor's update site.
C. Trace O/S patch logs to change control requests.
D. Review change control documents for key servers.

136. Which of the following is **MOST** important in ensuring the success of an information security program?

A. Security awareness training
B. Achievable goals and objectives
C. Sufficient senior management support
D. Adequate start-up budget and staffing

137. Information security can **BEST** be evaluated through which of the following?

A. Value analysis
B. Security metrics
C. Security deliverables list
D. Process improvement models

138. For an organization with operations in multiple countries, when security policies that were based on an international standard are found to be in contradiction with newly created national laws and regulations, it should:

A. be rewritten to conform to the new requirements.
B. remain as is to be in conformity with the international standard.
C. be customized to have a conforming version developed for the country in question.
D. be generalized so as not to contradict any specific national requirements.

139. Which of the following **BEST** describes the level of risk that an organization is willing to accept?

A. Control risk
B. Monetary value
C. Risk exposure
D. Risk preference

140. The value of a physical asset should be based on:

A. original cost.
B. net cash flow.
C. net present value.
D. replacement cost.

141. Which of the following is the **MOST** important element in ensuring the success of a disaster recovery test at a vendor provided hot site?

A. Tests are scheduled on weekends.
B. Network IP addresses are predefined.
C. Equipment at the hot site is identical.
D. Organizational management is supportive.

142. A risk management program should **MOST** importantly seek to:

A. quantify overall risk.
B. minimize residual risk.
C. eliminate inherent risk.
D. maximize the sum of all annualized loss expectencies (ALEs).

143. The **PRIMARY** goal of information security governance should be to create value through the:

A. review of internal control mechanisms.
B. proactive involvement in business decision making.
C. total elimination of risk factors.
D. instillation of trust among stakeholders.

144. Which of the following ensures that newly identified security weaknesses are mitigated in a timely fashion?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

145. The **MOST** important component(s) of a privacy policy is/are:

A. notifications.
B. warranties.
C. liabilities.
D. geographic coverage.

146. Which of the following devices should be placed within a DMZ?

A. Router
B. Firewall
C. Mail relay
D. Authentication server

147. Which of the following threats would generally be the **EASIEST** to accurately estimate its likelihood?

A. Terrorism
B. Chemical spill
C. Explosion
D. Windstorm

148. Acceptable levels of information security risk should be determined by:

A. legal counsel.
B. security management.
C. external auditors.
D. senior management.

149. When a system change violates an existing security standard, the conflict should be resolved:

A. using a cost-benefit analysis.
B. in favor of the security standard.
C. in favor of the new system change.
D. using best practices for that industry.

150. When a departmental system continues to remain out of compliance with the information security policy's password strength requirements, the **BEST** action to undertake is to:

A. submit the issue to an external arbitration group.
B. conduct an impact analysis to quantify the risks.
C. isolate the system from the rest of the network.
D. grant a special waiver that is subject to annual renewal.

151. Which of the following are seldom changed in response to technological changes?

A. Standards
B. Procedures
C. Policies
D. Guidelines

152. The **BEST** time to perform a penetration test is after a(n):

A. attempted penetration has occurred.
B. audit has discovered a lack of security controls.
C. number of systems infrastructure changes are made.
D. turnover in systems administrative staff.

153. To help ensure that contract personnel do not obtain access to sensitive information, the information security manager should ensure that contract personnel:

A. have expiration dates set to six months or less.
B. do not function in a system administration role.
C. successfully pass background checks.
D. are assigned system access by the data owner.

154. The **BEST** reason for an organization to have two discrete firewalls connected directly to the Internet and the same DMZ would be to:

A. provide defense in-depth.
B. separate test and production.
C. permit traffic load balancing.
D. prevent a denial-of-service attack.

155. Senior management commitment and support for information security will be diminished if the information security manager:

A. emphasizes organizational risk above technology risk.
B. establishes a set of organizationwide metrics.
C. emphasizes security needs above organizational needs.
D. explains that each organizational unit must take responsibility.

156. Which of the following is the **MOST** appropriate method to ensure that the password to open a confidential file is not intercepted along with the file that is transmitted?

A. Delivery path tracing
B. Reverse lookup translation
C. Out-of-band channels
D. Digital signatures

157. Which of the following is the **MOST** important item to include when developing web-hosting agreements with third-party providers?

A. Termination conditions
B. Liability limits
C. Service levels
D. Privacy restrictions

158. Which of the following is **MOST** appropriate for inclusion in an information security strategy?

A. Business controls designated as key controls
B. Security processes, methods, tools and techniques
C. Firewall rule sets, network defaults and IDS settings
D. Budget estimates to acquire specific security tools

159. Which of the following is **MOST** effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

A. Patch management
B. Change management
C. Security metrics
D. Version control

160. Which of the following, if absent, would be the **MOST** detrimental to the promotion of good security management practices?

A. Security metrics
B. Security baselines
C. Management support
D. Periodic training

161. The **BEST** method for detecting and monitoring a hacker's activities without exposing information assets to unnecessary risk is to utilize:

A. firewalls.
B. bastion hosts.
C. decoy files.
D. screened subnets.

162. Which of the following is the **BEST** metric for evaluating the effectiveness of an intrusion detection mechanism?

A. Number of attacks detected
B. Number of successful attacks
C. Ratio of false-positives to false-negatives
D. Ratio of successful to unsuccessful attacks

163. Which of the following is the **BEST** indicator that security awareness training has been effective?

A. Password resets have declined.
B. More incidents are being reported.
C. A majority of employees have received training.
D. Feedback forms from training are favorable.

164. Retention of business records should be based **PRIMARILY** on:

A. business strategy and direction.
B. regulatory and legal requirements.
C. storage capacity and longevity.
D. business case and value analysis.

165. When implementing a new system using a purchased software package, the time and duration of which of the following system life cycle phases will likely be reduced the **MOST**?

A. Feasibility
B. Development
C. Testing
D. Postimplementation review

166. Which of the following is the **MOST** effective solution for preventing internal users from modifying sensitive and classified information?

A. Screened subnets
B. System access logs
C. Role-based access controls
D. Intrusion detection system

167. The effectiveness of virus detection software is **MOST** dependent on which of the following?

A. Number of product upgrades
B. Number of available patches
C. License agreement warranties
D. Update frequency of DAT files (odat)

168. Which of the following is characteristic of decentralized information security management across a geographically dispersed organization?

A. More uniformity in quality of service
B. Better adherence to policies
C. More aligned to business unit needs
D. Less total cost of ownership (TCO)

169. An information security program should be sponsored by:

A. infrastructure management.
B. the corporate legal department.
C. key business process owners.
D. quality assurance management.

170. Which of the following **BEST** describes the scope of risk analysis?

A. Key financial systems
B. Organizational activities
C. Key systems and infrastructure
D. Systems subject to regulatory compliance

171. An intranet server should generally be placed on the:

A. internal network.
B. firewall server.
C. external router.
D. primary domain controller.

172. A business impact analysis (BIA) is the **BEST** tool for calculating:

A. total cost of ownership.
B. priority of restoration.
C. annualized loss expectancy (ALE).
D. residual risk to the organization.

173. For the information security manager, which of the following roles will represent a conflict of interest?

A. Evaluation of third parties requesting connectivity
B. Assessment of the adequacy of disaster recovery plans
C. Final approval of information security policies
D. Monitoring adherence to physical security controls

174. Which of the following devices should be placed within a DMZ?

A. Switch
B. Web server
C. Database server
D. File/print server

175. Which of the following is characteristic of centralized information security management?

A. More expensive to administer
B. Better adherence to policies
C. More aligned with business unit needs
D. Faster turnaround of requests

176. Risk acceptance is a component of which of the following?

A. Assessment
B. Mitigation
C. Evaluation
D. Monitoring

177. Which of the following metrics is the **MOST** appropriate for measuring how effectively the organization is securing systems? The percentage of:

A. servers with up-to-date patches.
B. vulnerabilities still open.
C. number of viruses detected.
D. systems where change control processes apply.

178. Which of the following represents a key area of focus when conducting a penetration test?

A. Data mining
B. Network mapping
C. Task scheduling
D. Customer data

179. When a large organization discovers that it is the subject of a network probe, which of the following actions should be taken?

A. Reboot the router connecting the DMZ to the firewall.
B. Power down all servers located on the DMZ segment.
C. Monitor the probe and isolate the affected segment.
D. Enable server trace logging on the affected segment.

180. Which of the following presents the **GREATEST** threat to the security of an enterprise resource planning (ERP) system?

A. User *ad hoc* reporting is not logged.
B. Network traffic is through a single switch.
C. O/S security patches have not been applied.
D. Database security defaults to ERP settings.

181. In a financial services organization, security awareness training should be provided to new employees:

A. on an as-needed basis when specific duties warrant.
B. during user training on the system they are to access.
C. before they receive access to information.
D. at the same time that existing employees are trained.

182. The **MOST** appropriate role for senior management in supporting information security is the:

A. evaluation of vendors offering security products.
B. assessment of risks to the organization.
C. approval of policy statements and funding.
D. monitoring of adherence to regulatory requirements.

183. Which of the following **BEST** ensures that information transmitted over the Internet will remain confidential?

A. Encryption
B. Steganography
C. Biometric authentication
D. Two factor authentication

184. Which of the following would be **MOST** useful in developing a series of recovery time objectives (RTOs)?

A. Gap analysis
B. Regression analysis
C. Correlation analysis
D. Business impact analysis

185. Accountability by business process owners can **BEST** be obtained through:

A. periodic reminder memorandums.
B. strict enforcement of policies.
C. policies signed by IT management.
D. education and awareness meetings.

186. Security awareness training should lead to a(n):

A. decrease in password resets.
B. increase in reported incidents.
C. decrease in security policy changes.
D. increase in access rule violations.

187. It is **MOST** important that an information security architecture be aligned with which of the following?

A. Industry best practices
B. Information technology plans
C. Information security best practices
D. Business objectives and goals

188. The decision on whether new risks should fall under periodic or event-driven reporting should be based on:

A. severity and duration.
B. visibility and duration.
C. likelihood and duration.
D. absolute monetary value.

189. The **MAIN** advantage of implementing automated password synchronization is that it:

A. reduces overall administrative workload.
B. increases security between multitier systems.
C. allows passwords to be changed less frequently.
D. reduces the need for two-factor authentication.

190. The **BEST** way to determine if an anomaly-based intrusion detection system (IDS) is properly installed is to:

A. simulate an attack and review IDS performance.
B. use a honeypot to check for unusual activity.
C. review the configuration of the IDS.
D. benchmark the IDS against a peer site.

191. Which of the following should management use to determine the amount of resources to devote to mitigating exposures?

A. Risk analysis results
B. Audit report findings
C. Penetration test results
D. A fixed percentage of the IT budget

192. Senior management commitment and support for information security can **BEST** be obtained through presentations that:

A. use illustrative examples of successful attacks.
B. explain the technical risks to the organization.
C. evaluate the organization against best practices.
D. tie security risks to key business objectives.

193. What is the **MOST** effective method for ensuring that users do not share files with other users not approved for access?

A. Mandatory access controls
B. Discretionary access controls
C. Lattice-based access controls
D. Role-based access controls

194. The **PRIMARY** objective for managing a security incident involving a successful penetration should be to:

A. allow business processes to continue during the response.
B. allow the security team to assess the attack profile.
C. permit the incident to continue to trace the source.
D. evaluate the incident management process for deficiencies.

195. The likelihood of successfully implementing information security governance will be minimized if there is a lack of:

A. security awareness training.
B. updated security polices.
C. a computer incident management team.
D. senior management support.

196. A postincident review should be conducted by the incident management team to determine:

A. what electronic evidence is relevant.
B. ways to improve the response process.
C. why the attack was launched by the hacker.
D. which individuals failed to perform their duties.

197. Which of the following will **BEST** identify areas of risk that have been addressed?

A. Gap analysis
B. Regression analysis
C. Correlation analysis
D. Business impact analysis

198. A business continuity policy document should contain which of the following?

A. Telephone trees
B. Declaration criteria
C. Press release templates
D. A listing of critical backup files

199. A risk management program should reduce risk to:

A. zero.
B. an acceptable level.
C. an annualized rate of less than 5 percent of revenue.
D. breakeven with the cost of the program.

200. Which of the following is the **BEST** method for ensuring that security procedures and guidelines are read and understood?

A. Periodic focus group meetings
B. Periodic reminder memos to management
C. Using computer-based training presentations (CBTs) with quizzes
D. Employees signing an acknowledgement of receipt

SAMPLE EXAM ANSWER AND REFERENCE KEY

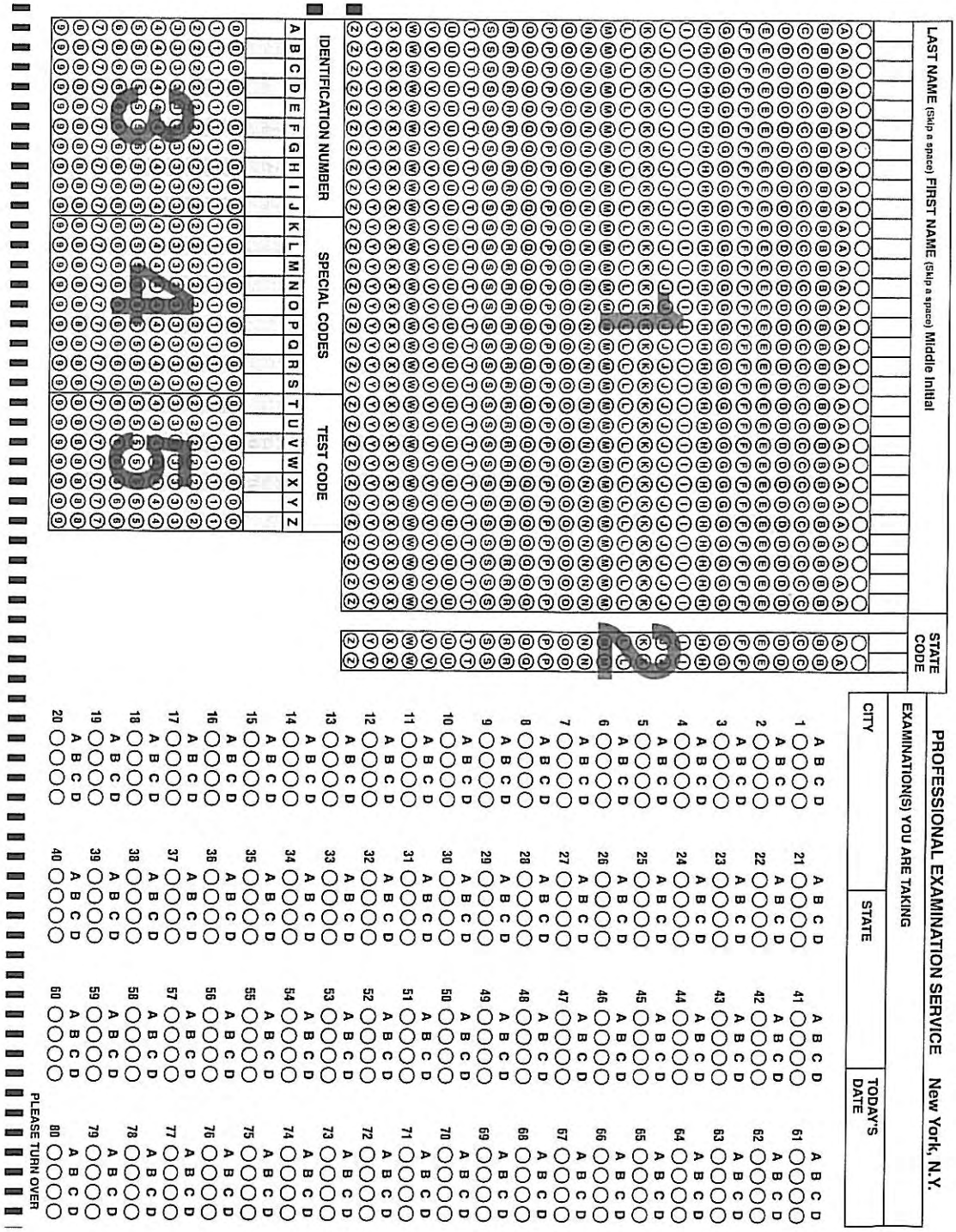
QUES #	ANSWER	REF	QUES #	ANSWER	REF	QUES #	ANSWER	REF	QUES #	ANSWER	REF
1	D	T1-36	51	D	T4-29	101	D	T3-24	151	C	T1-32
2	B	T2-1	52	A	T3-20	102	D	T4-12	152	C	T4-23
3	B	T5-17	53	B	T1-27	103	C	T2-12	153	B	T4-42
4	D	T4-6	54	C	T2-23	104	A	T5-2	154	C	T3-8
5	A	T2-10	55	C	T5-15	105	B	T4-9	155	C	T1-23
6	D	T5-22	56	C	T2-5	106	A	T3-5	156	C	T4-45
7	D	T5-23	57	C	T2-26	107	C	T2-38	157	C	T3-35
8	B	T5-21	58	D	T4-7	108	C	T4-28	158	B	T1-22
9	C	T4-43	59	B	T4-5	109	D	T4-25	159	B	T3-40
10	C	T1-40	60	C	T1-41	110	D	T1-5	160	C	T4-16
11	D	T1-33	61	D	T2-28	111	D	T1-7	161	C	T5-5
12	D	T5-26	62	C	T1-30	112	B	T4-47	162	C	T3-16
13	C	T5-16	63	D	T1-21	113	C	T4-20	163	B	T4-10
14	C	T1-6	64	B	T3-12	114	D	T5-3	164	B	T1-10
15	A	T1-20	65	A	T4-11	115	B	T4-3	165	B	T3-13
16	D	T3-19	66	B	T2-36	116	B	T5-10	166	C	T3-23
17	D	T3-30	67	C	T4-24	117	C	T1-34	167	D	T3-3
18	B	T1-14	68	D	T3-11	118	D	T4-33	168	C	T1-35
19	D	T1-25	69	A	T1-26	119	C	T3-7	169	C	T3-34
20	D	T3-27	70	D	T4-32	120	D	T5-25	170	B	T2-40
21	A	T2-15	71	B	T4-27	121	B	T1-1	171	A	T3-28
22	D	T3-39	72	C	T2-4	122	D	T5-6	172	B	T2-29
23	C	T2-34	73	C	T4-30	123	A	T4-2	173	C	T1-24
24	A	T3-25	74	B	T3-41	124	C	T5-4	174	B	T3-26
25	D	T1-19	75	D	T2-13	125	C	T2-35	175	B	T1-12
26	C	T3-18	76	C	T1-9	126	A	T4-17	176	B	T2-22
27	A	T1-4	77	A	T5-7	127	D	T2-33	177	B	T4-34
28	D	T2-24	78	C	T3-1	128	C	T1-29	178	B	T4-40
29	B	T5-12	79	B	T1-37	129	B	T4-21	179	C	T5-18
30	B	T2-27	80	A	T1-11	130	A	T2-11	180	C	T4-26
31	D	T1-31	81	B	T1-8	131	D	T4-18	181	C	T4-35
32	A	T2-30	82	B	T2-3	132	B	T5-20	182	C	T1-3
33	D	T4-31	83	A	T1-17	133	C	T3-22	183	A	T3-2
34	B	T5-14	84	B	T4-14	134	B	T3-4	184	D	T2-17
35	C	T1-16	85	B	T3-17	135	C	T4-36	185	D	T3-10
36	B	T4-1	86	A	T2-37	136	C	T3-42	186	B	T3-31
37	C	T4-37	87	C	T2-20	137	A	T4-41	187	D	T1-28
38	C	T2-9	88	C	T3-15	138	C	T4-48	188	D	T2-21
39	B	T2-16	89	D	T4-39	139	D	T2-19	189	A	T3-38
40	A	T3-36	90	C	T4-44	140	D	T2-8	190	A	T4-22
41	C	T2-18	91	C	T2-7	141	D	T5-8	191	A	T2-6
42	D	T1-38	92	D	T4-19	142	B	T2-25	192	D	T1-2
43	B	T2-39	93	C	T3-9	143	D	T1-39	193	A	T4-46
44	B	T5-1	94	C	T1-18	144	A	T3-37	194	A	T5-11
45	D	T5-19	95	D	T4-4	145	A	T1-15	195	D	T1-13
46	D	T3-29	96	A	T5-9	146	C	T3-6	196	B	T5-13
47	A	T4-13	97	B	T4-38	147	D	T2-31	197	A	T2-14
48	A	T2-41	98	C	T3-32	148	D	T1-42	198	B	T5-24
49	A	T2-42	99	B	T2-32	149	A	T3-21	199	B	T2-2
50	C	T4-8	100	B	T3-33	150	B	T4-15	200	C	T3-14

Reference example: T1-1 = See section T1, question 1 for the explanation of the answer.

SAMPLE EXAM ANSWER SHEET (PRE-TEST)

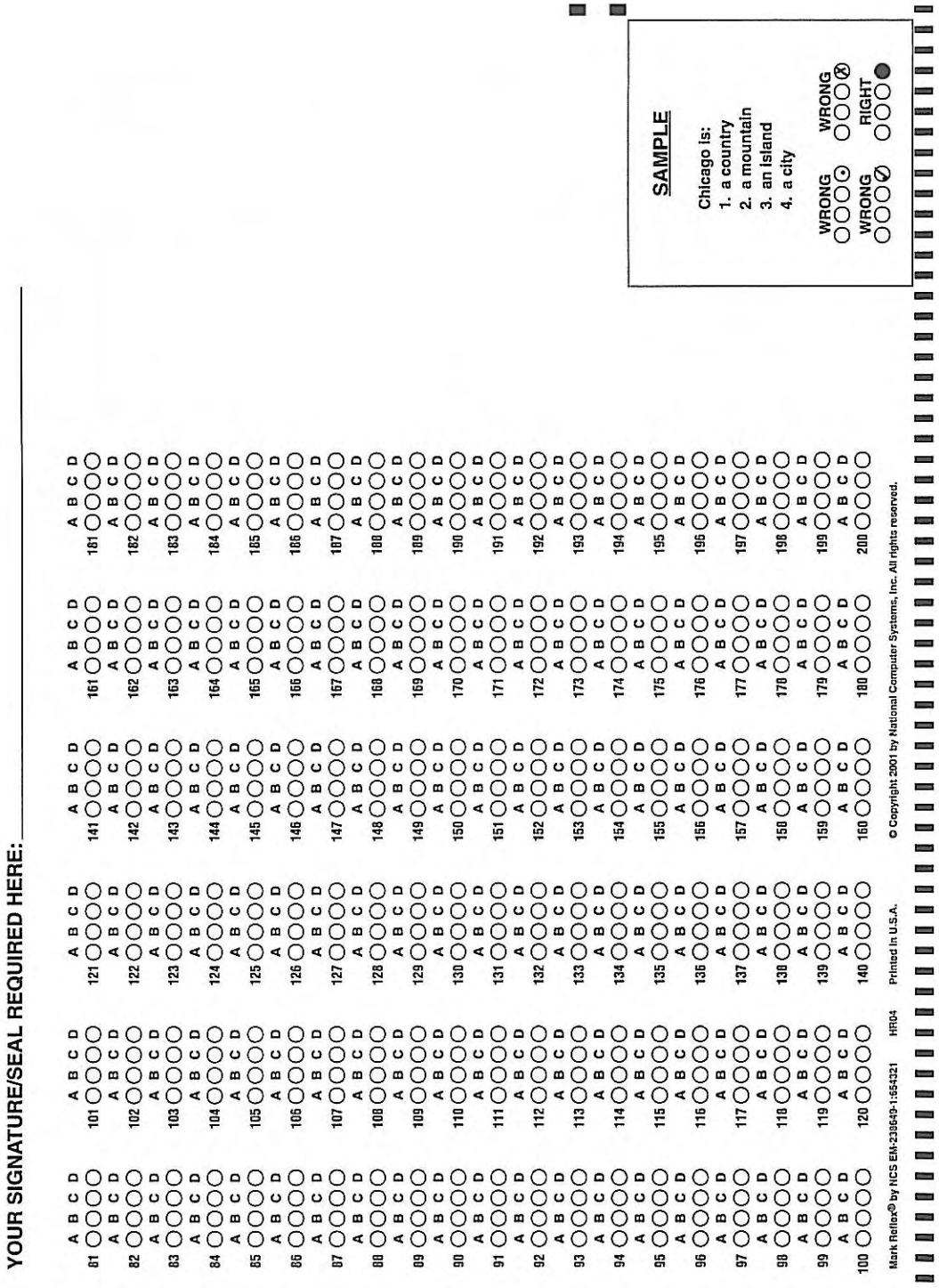
(side 1)

Please use this answer sheet if you intend to take the sample exam as a pre-test to determine strengths and weaknesses. The answer key/reference grid is on page 89.



(side 2)

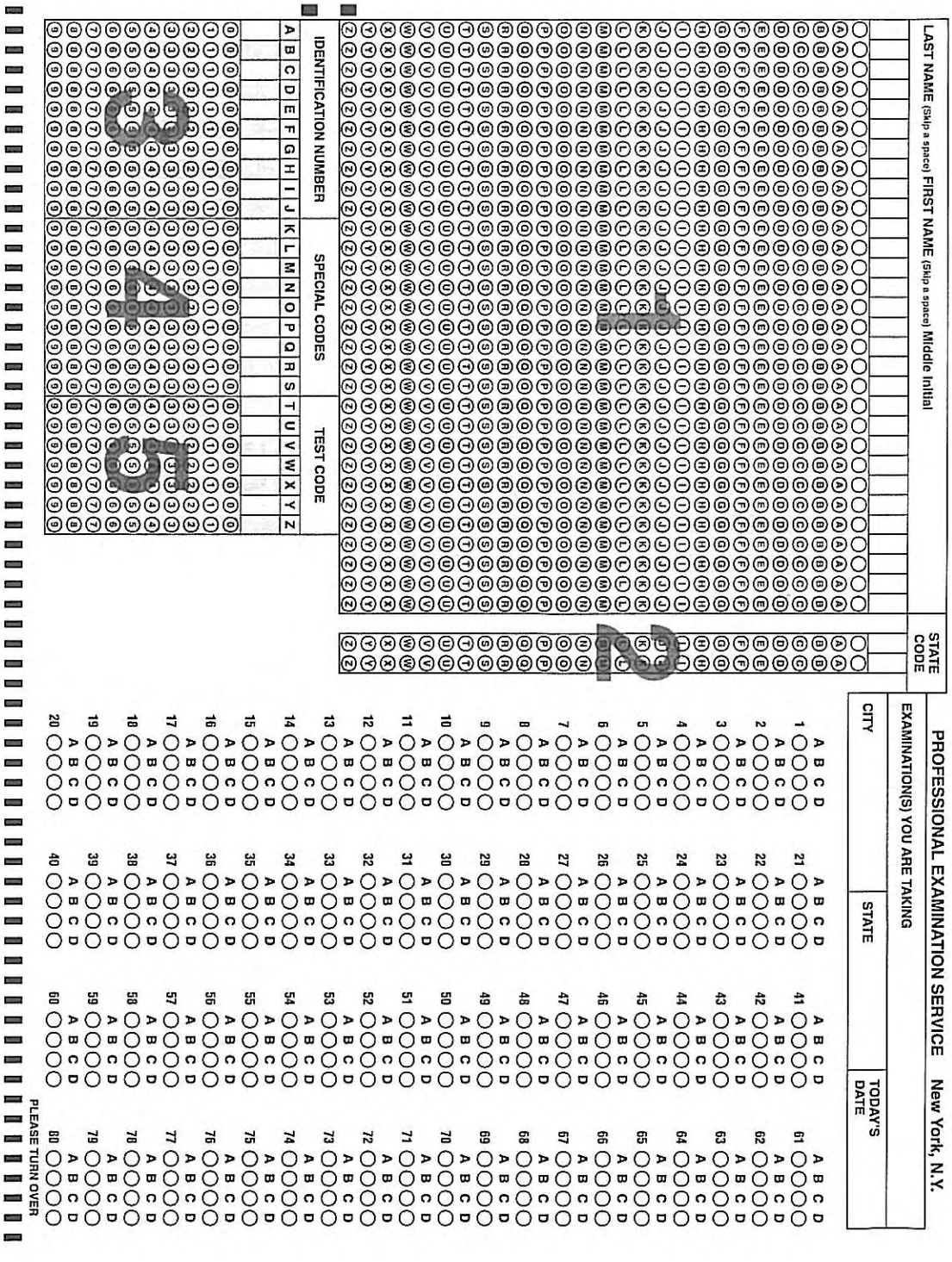
Please use this answer sheet if you intend to take the sample exam as a pre-test to determine strengths and weaknesses. The answer key/reference grid is on page 89.



SAMPLE EXAM ANSWER SHEET (POST-TEST)

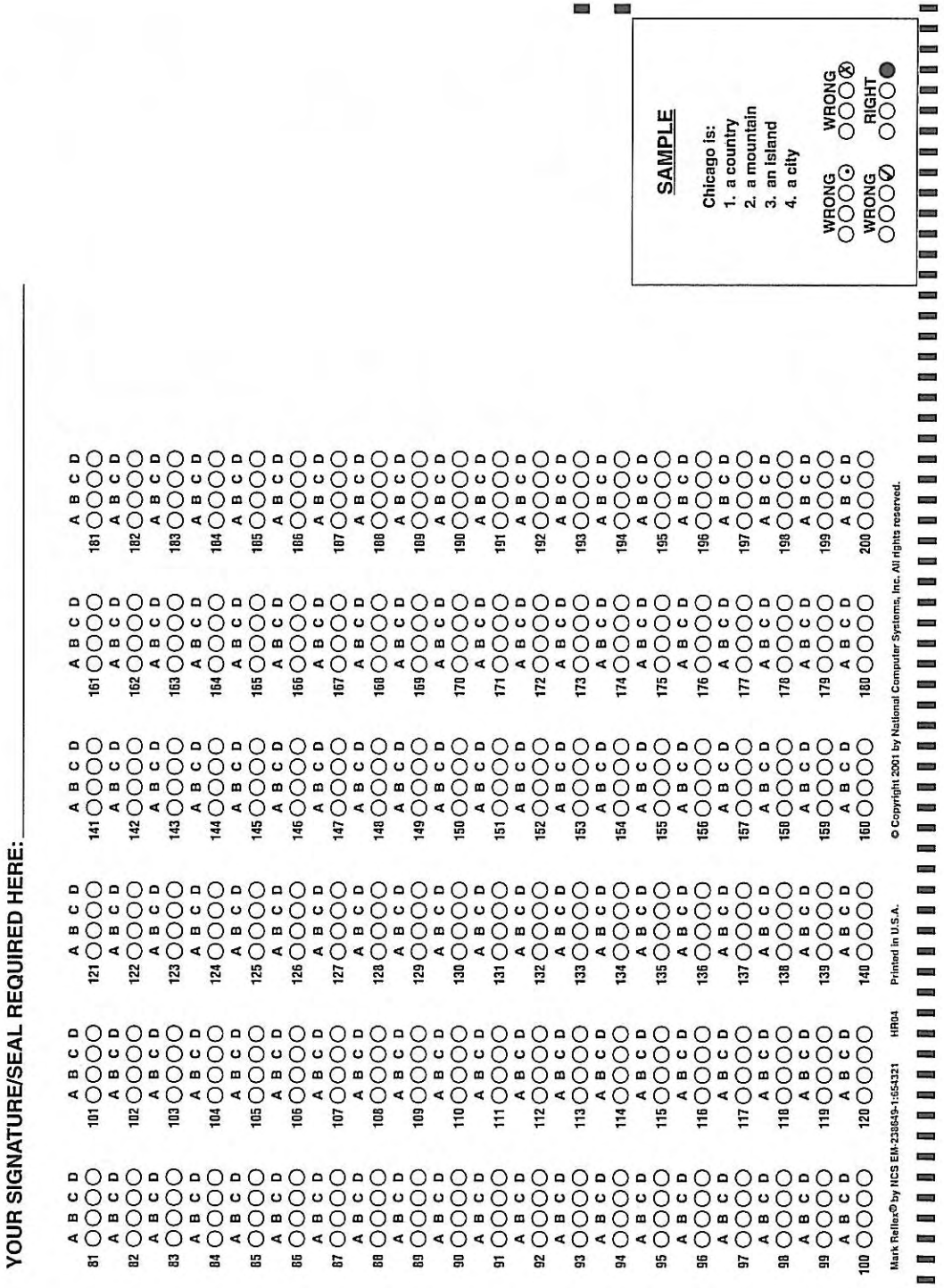
(side 1)

Please use this answer sheet if you intend to take the sample exam as a post-test to determine strengths and weaknesses. The answer key/reference grid is on page 89.



(side 2)

Please use this answer sheet if you intend to take the sample exam as a post-test to determine strengths and weaknesses. The answer key/reference grid is on page 89.



EVALUATION

The Information Systems Audit and Control Association continuously monitors the swift and profound professional, technological and environmental advances affecting information security managers. Recognizing these rapid advances, the CISM review materials are updated annually.

To assist the association with keeping abreast of these advances, ISACA's Board of Directors would appreciate it if you would take a moment to evaluate the *CISM Review Questions, Answers & Explanations Manual 2006*. Such feedback is valuable to fully serve the profession and future CISM examination registrants.

Please complete the questionnaire below and return to:

Attention: Manager—Certification Study Program and Educational Development
Mail: ISACA
3701 Algonquin Road, Suite 1010, Rolling Meadows, Illinois 60008, USA
Fax: +1.847.253.1443
E-mail: *efernandez@isaca.org*
Web site: *www.isaca.org*

1. What was your overall impression of the *CISM Review Questions, Answers & Explanations Manual 2006*?

___Very helpful ___Helpful ___Not very helpful

2. Did you find the questions/answers helpful in preparing for the CISM examination?

___Yes ___Partially ___No

Please explain:

_____

_____

_____

3. How would you rate the format of the *CISM Review Questions, Answers & Explanations Manual 2006* (questions by area/sample exam)?

___Very helpful ___Helpful ___Not very helpful

4. What recommendations do you have for improving the *CISM Review Questions, Answers & Explanations Manual 2006*?

_____

_____

_____

Thank You

OTHER COMMENTS/SUGGESTIONS

NOTES

NOTES

NOTES

Prepare for the **June/December 2006** *CISM Exam*

Order Now—2006 CISM® Review Materials for Exam Preparation and Professional Development

To pass the CISM exam a candidate should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers study aids and review courses to exam candidates (see *www.isaca.org/cismexam* for more details).

CISM Review Manual 2006

Information Systems Audit and Control Association

The *CISM Review Manual 2006* is a reference guide designed to assist individuals in preparing for the Certified Information Security Manager® (CISM®) examination and for individuals wanting to learn more about the role and responsibilities of an information security manager. The 2006 edition is significantly enhanced with changes of structure for a more comprehensive flow, updates to the content reflecting regulatory and technical changes and expanded coverage of critical areas. The manual features detailed descriptions of the tasks performed by information security managers, and the knowledge necessary to manage, design and oversee an enterprise's information security program. These task and knowledge statements were developed by the CISM Certification Board, validated by subject matter experts and serve as the blueprint for the CISM examination content and emphasis.

Information provided includes an explanation of each task and related knowledge statement, applicable information security management principles, practices and strategies. Detailed references of where to find additional guidance materials is also provided. This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and review courses.

This manual has been developed and organized to assist in the study of the following job practice areas:
- Information security governance
- Risk management
- Information security program(me) management
- Information security management
- Response management

The *CISM Review Manual 2006* also provides definitions and practical examples to facilitate the learning process.

CM-6 English Edition

CISM Questions, Answers & Explanations Manual 2006

Information Systems Audit and Control Association

This manual consists of 200 multiple-choice study questions arranged in the same proportion as the CISM job analysis. Many of these items appeared in the 2004 and 2005 editions of the *CISM Review Questions, Answers & Explanations Manual*, but have been rewritten to recognize a change in practice, be more representative of the exam item format, and/or provide further clarity or explanation of the suggested correct answer. These questions are not actual exam items, and are intended to provide the CISM candidate with an understanding of the type and structure of questions and subject matter that has previously appeared on the examination.

These questions are provided in two formats.
- **Questions sorted by content area**—Questions, answers and explanations are provided (sorted) by CISM job content area. This allows the CISM candidate to study material by content area and refer to specific questions, as well as evaluate their comprehension of the topics covered within each content area.
- **Sample test**—The two hundred questions are scrambled to represent a CISM-length examination. Candidates are urged to use this sample test and the answer sheet provided to simulate an examination. Many candidates use this exam as a pretest to determine their strengths or weaknesses and/or as a final exam. Sample exam answer sheets have been provided for both uses. In addition, a sample exam answer/reference key is included. All sample test questions have been cross-referenced to the questions sorted by content area, making it convenient to refer back to the explanations of the correct answers.

This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement.*

CQA-6 English Edition

CISM Questions, Answers & Explanations Manual 2006 Supplement

Information Systems Audit and Control Association

This manual consists of 100 multiple-choice study questions arranged in the same proportion as the CISM job practice analysis. The questions include the answers and detailed explanations for the candidates to use in preparation for the CISM exam. Unlike some review manuals that use questions from other certification exams, these questions were prepared especially for use in studying for the CISM exam. These questions are intended to provide the CISM candidate with an understanding of the type and structure of questions that have typically appeared on the examination and are not actual test items.

This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and the *CISM Review Questions, Answers & Explanations Manual 2006.*

CQA-6ES English Edition

To order the CISM review materials for the June/December 2006 CISM exam, visit our web site at *www.isaca.org/cismbooks.*

2005 CISM Review Materials are available in Japanese and Spanish.

See *www.isaca.org/nonenglishbooks.*