

Chapter 5:

Protection of Information Assets

Section One: Overview

Definition 282
Objectives 282
Task and Knowledgement Statements 282
Suggested Resources for Further Study 289
Practice Questions 290
Answers to Practice Questions 291

Section Two: Content

5.1 Quick Reference 292
5.2 Importance of Information Security Management 292
5.3 Logical Access 307
5.4 Network Infrastructure Security 319
5.5 Auditing Information Security Management Framework 340
5.6 Auditing Network Infrastructure Security 346
5.7 Environmental Exposures and Controls 351
5.8 Physical Access Exposures and Controls 354
5.9 Mobile Computing 356
5.10 Case Studies 357
5.11 Answers to Case Study Questions 360

Section One: Overview

DEFINITION

This chapter addresses the key components that ensure confidentiality, integrity and availability (CIA) of information assets. The design, implementation and monitoring of logical and physical access controls to ensure CIA are evaluated. Also evaluated are network infrastructure security, environmental controls and processes and procedures used to store, retrieve, transport and dispose of confidential information assets. The various methods and procedures followed by organizations are described, focusing on the auditor's role in evaluating these procedures for suitability and effectiveness.

OBJECTIVES

The objective of this area is to ensure that the CISA candidate understands and can provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.

This area represents 31 percent of the CISA examination (approximately 62 questions).

TASK AND KNOWLEDGEMENT STATEMENTS

TASKS

There are five (5) tasks within the protection of information assets area:

T5.1 Evaluate the design, implementation and monitoring of logical access controls to ensure the confidentiality, integrity, availability and authorized use of information assets.

T5.2 Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorized use of the network and the information transmitted.

T5.3 Evaluate the design, implementation and monitoring of environmental controls to prevent or minimize loss.

T5.4 Evaluate the design, implementation and monitoring of physical access controls to ensure that information assets are adequately safeguarded.

T5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of confidential information assets.

KNOWLEDGE STATEMENTS

The CISA candidate must have a good understanding of each of the areas delineated by the knowledge statements. These statements are the basis for the exam.

There are 17 knowledge statements within the protection of information assets area:

KS5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment)

KS5.2 Knowledge of logical access controls for the identification, authentication and restriction of users to authorized functions and data (e.g., dynamic passwords, challenge/response, menus, profiles)

KS5.3 Knowledge of logical access security architectures (e.g., single sign-on, user identification strategies, identity management)

KS5.4 Knowledge of attack methods and techniques (e.g., hacking, spoofing, Trojan horses, denial of service, spamming)

KS5.5 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)

KS5.6 Knowledge of network and Internet security devices, protocols and techniques (e.g., secure sockets layer [SSL], secure electronic transaction [SET], virtual private network [VPN], network address translation [NAT])

KS5.7 Knowledge of intrusion detection systems and firewall configuration, implementation, operation and maintenance

KS5.8 Knowledge of encryption algorithm techniques (e.g., Advanced Encryption Standard [AES], RSA)

KS5.9 Knowledge of public key infrastructure (PKI) components (e.g., certification authorities, registration authorities) and digital signature techniques

KS5.10 Knowledge of virus detection tools and control techniques

KS5.11 Knowledge of security testing and assessment tools (e.g., penetration testing, vulnerability scanning)

KS5.12 Knowledge of environmental protection practices and devices (e.g., fire suppression, cooling systems, water sensors)

KS5.13 Knowledge of physical security systems and practices (e.g., biometrics, access cards, cipher locks, tokens)

KS5.14 Knowledge of data classification schemes (e.g., public, confidential, private and sensitive data)

KS5.15 Knowledge of voice communications security (e.g., voice-over IP)

KS5.16 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets

KS5.17 Knowledge of controls and risks associated with the use of portable and wireless devices (e.g., personal digital assistants [PDAs], Universal Serial Bus [USB] devices, Bluetooth devices)

Relationship of Task to Knowledge Statements

The task statements are what the CISA candidate is expected to know how to do. The knowledge statements delineate what the CISA candidate is expected to know in order to perform the tasks. The task and knowledge statements are mapped in **exhibit 5.1** insofar as it is possible to do so. Note that although there is often overlap, each task statement will generally map to several knowledge statements.

Exhibit 5.1— Tasks and Knowledge Statements Mapping	
Task Statements	**Knowledge Statements**
T5.1 Evaluate the design, implementation and monitoring of logical access controls to ensure the confidentiality, integrity, availability and authorized use of information assets.	KS5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment) KS5.2 Knowledge of logical access controls for the identification, authentication and restriction of users to authorized functions and data (e.g., dynamic passwords, challenge/response, menus, profiles) KS5.3 Knowledge of logical access security architectures (e.g., single sign-on, user identification strategies, identity management) KS5.5 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team) KS5.14 Knowledge of data classification schemes (e.g., public, confidential, private and sensitive data) KS5.17 Knowledge of controls and risks associated with the use of portable and wireless devices (e.g., personal digital assistants [PDAs], Universal Serial Bus [USB] devices, Bluetooth devices)
T5.2 Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorized use of the network and the information transmitted.	KS5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment) KS5.4 Knowledge of attack methods and techniques (e.g., hacking, spoofing, Trojan horses, denial of service, spamming) KS5.5 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team) KS5.6 Knowledge of network and Internet security devices, protocols and techniques (e.g., secure sockets layer [SSL], secure electronic transaction [SET], virtual private network [VPN], network address translation [NAT]) KS5.7 Knowledge of intrusion detection systems and firewall configuration, implementation, operation and maintenance KS5.8 Knowledge of encryption algorithm techniques (e.g., Advanced Encryption Standard [AES], RSA) KS5.9 Knowledge of public key infrastructure (PKI) components (e.g., certification authorities, registration authorities) and digital signature techniques KS5.10 Knowledge of virus detection tools and control techniques KS5.11 Knowledge of security testing and assessment tools (e.g., penetration testing, vulnerability scanning) KS5.15 Knowledge of voice communications security (e.g., voice-over IP) KS5.17 Knowledge of controls and risks associated with the use of portable and wireless devices (e.g., personal digital assistants [PDAs], Universal Serial Bus [USB] devices, Bluetooth devices)
T5.3 Evaluate the design, implementation and monitoring of environmental controls to prevent or minimize loss.	KS5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment) KS5.12 Knowledge of environmental protection practices and devices (e.g., fire suppression, cooling systems, water sensors)
T5.4 Evaluate the design, implementation and monitoring of physical access controls to ensure that information assets are adequately safeguarded.	KS5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment) KS5.5 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team) KS5.13 Knowledge of physical security systems and practices (e.g., biometrics, access cards, cipher locks, tokens)
T5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of confidential information assets.	KS5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment) KS5.8 Knowledge of encryption algorithm techniques (e.g., Advanced Encryption Standard [AES], RSA) KS5.14 Knowledge of data classification schemes (e.g., public, confidential, private and sensitive data) KS5.16 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential KS5.17 Knowledge of controls and risks associated with the use of portable and wireless devices (e.g., personal digital assistants [PDAs], Universal Serial Bus [USB] devices, Bluetooth devices)

Knowledge Statement Reference Guide

Each knowledge statement is explained in terms of underlying concepts and relevance of the knowledge statement to the IS auditor. It is essential that the exam candidate understand the concepts. The knowledge statements are what the IS auditor must know in order to accomplish the tasks. Consequently, only the knowledge statements are detailed in this section.

Additional information can be found in section two of this chapter (in the sections identified below in KS5.1-KS5.17).

KS5.1 Knowledge of the techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Security needs to be aligned with business objectives to provide a reasonable reduction in risk. Security objectives may include the following: • Ensure the continued availability of information systems. • Ensure the integrity of information stored on its computer systems and while the information is in transit. • Preserve the confidentiality of sensitive data while stored and in transit. • Ensure compliance with applicable laws, regulations and standards. • Ensure adherence to trust and obligation requirements for any information relating to an identified or identifiable individual (i.e., data subject) in accordance with the applicable privacy policy or privacy laws and regulations. The IS auditor should be aware of the ways in which the above objectives may be achieved through technical and associated manual controls so that existing controls may be identified and assessed and new or amended controls can be recommended. The design, implementation and monitoring of security should be aligned with business goals and objectives. The focus should be on those items that, if their security were compromised, would impact the organization in tangible (if not always quantifiable) ways. Controls generally incur a business cost, either directly or in their effect on business activities, and organizations should ensure that the cost of control does not materially exceed the business risk. The primary focus should be to ensure that risks which would have a material adverse impact on business are appropriately managed. This is typically established through a business impact analysis (BIA).	Understanding the elements of information security management	5.2.1 Key Elements of Information Security Management 5.2.7 Critical Success Factors to Information Security
	Ability to assess the classification of information assets within an information security context	5.2.3 Inventory and Classification of Information Assets
	Understanding information security as it applies to key network infrastructure components	5.4 Network Infrastructure Security

KS5.2 Knowledge of logical access controls for the identification, authentication and restriction of users to authorized functions and data (e.g., dynamic passwords, challenge/response, menus, profiles)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Logical access controls are used to manage and protect information assets. Controls enact and substantiate policies and procedures designed by management to protect information assets, and controls are designed to reduce risks to a level acceptable to an organization. Controls exist at both the operating system level and the application level, so it is important to understand logical access controls as they apply to systems that may reside on multiple operating system platforms and involve more than one application system or authentication point. Logical security is often determined based on the job function of users. The success of logical access controls is tied to the strength of the authentication method (e.g., strong passwords). All user access to systems and data should be appropriately authorized and should be commensurate with the role of the individual. Authorization generally takes the form of signatures (physical or electronic) of relevant management. The strength of the authentication is proportional to the quality of the method used: "strong authentication" may include dual or multifactor authentication using user ID, password, tokens and biometrics.	Understanding the key elements of logical access controls	5.3 Logical Access

KS5.3 Knowledge of logical access security architectures (e.g., single sign-on, user identification strategies, identity management)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Access control software utilizes both identification and authentication (I&A): once authenticated, the system or application then restricts access based on the specific role of the user. I&A is the process by which the system obtains identity from a user, the credentials needed to authenticate identity, and validates both pieces of information. I&A is a critical building block of computer security since it is needed for most types of access control and is necessary for establishing user accountability. For most systems, I&A is the first line of defense because it prevents unauthorized access (or unauthorized processes) to a computer system or an information asset. Logical access can be implemented in various ways. The IS auditor should be aware of the strengths and weaknesses of various architectures such as single sign-on (SSO), where a single authentication will enable access to all authorized applications; identity management; multifactor authentication; etc. The IS auditor must understand the risks associated with the different architectures as well as how they may be addressed. For example, SSO may enable unauthorized access to applications and data if a single password is compromised. If this risk is considered manageable, it should drive the implementation of multifactor authentication.	Understanding best practices as they apply to identification and authentication	5.3.6 Identification and Authentication

KS5.4 Knowledge Of Attack Methods And Techniques (E.G., Hacking, Spoofing, Trojan Horses, Denial of Service [DoS], Spamming)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Risks arise from vulnerabilities (whether technical or human) within an environment. Attack techniques exploit those vulnerabilities and may originate either within or outside the organization. Computer attacks can result in proprietary or confidential data being stolen or modified, loss of customer confidence and market share, embarrassment to management and legal actions against an organization. Understanding the methods, techniques and exploits used to compromise an environment provides the IS auditor with a more complete context for understanding the risks an organization faces. Taking these techniques into consideration and understanding that they can be launched from any location allows for more thorough evaluations, ultimately providing a more secure environment. The IS auditor should understand enough of these attack types to recognize their risk to the business and how they should be addressed by appropriate controls. The IS auditor should understand the concept of "social engineering" since these attacks can circumvent the strongest technical security. The only effective control is regular user education.	Understanding general issues regarding attack methods and computer crime	5.2.10 Computer Crime Issues and Exposures
	Ability to identify controls that are most effective in preventing or detecting attacks involving social engineering, wireless access and threats originating from the Internet	5.3.2 Social Engineering 5.4.3 Wireless Security Threats and Risk Mitigation 5.4.4 Internet Threats and Security

KS5.5 Knowledge of processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Explanation: A formal incident response capability should be established in order to minimize damage from security incidents, recover in a timely and controlled manner, and learn from such incidents. The organization and management of an incident response capability should be coordinated or centralized with the establishment of key roles and responsibilities. While security management will typically be responsible for monitoring and investigating events and be the origination point for escalation procedures, other functions must be involved to ensure a proper response. Those functions must have well-defined and communicated processes in place that are tested periodically. These processes may include communications with executive management, forensic evidence collection and incident response as well as procedures to handle legal issues and public relations. The IS auditor should be aware of the need for organizations to establish procedures to identify, report, record, respond, analyze, escalate and monitor security incidents.	Understanding the roles and responsibilities for incident response as well as the order and purpose of the key phases	5.2.11 Security Incident Handling and Response

KS5.6 Knowledge of network and Internet security devices, protocols and techniques (e.g., secure sockets layer [SSL], secure electronic transaction [SET], virtual private network [VPN], network address translation [NAT])

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Application and evaluation of technologies to reduce risk and secure data is dependent on proper understanding of security devices, their functions and protocols used in delivering functionality. An organization implements specific applications of cryptographic systems in order to ensure confidentiality of important data. There are a number of cryptographic protocols which provide secure communications on the Internet. Additionally, the security landscape is filled with technologies and solutions to address a myriad of needs. Solutions include firewalls, intrusion detection and prevention devices, proxy devices, web filters, antivirus and antispam filters, data leak protection functionality, identity and access control mechanisms, secured remote access and wireless security. Understanding the solution's function and its application to the underlying infrastructure requires knowledge of the infrastructure itself and the protocols in use. The IS auditor is not expected to possess a detailed, technical knowledge but rather a general understanding of the concepts, how they may be implemented and what business risks may be involved.	Understanding best practices for the implementation of encryption	5.4.5 Encryption
	Understanding the use and application of security devices and methods for securing data	5.3.6 Identification and Authentication 5.4 Network Infrastructure Security

KS5.7 Knowledge of intrusion detection systems (IDSs) and firewall configuration, implementation, operation and maintenance

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Enterprises can effectively prevent and detect most attacks on their networks by employing perimeter security controls. Firewalls and IDSs provide protection and critical alert information at borders between trusted and untrusted networks. The proper implementation and maintenance of firewalls and IDSs is critical to a successful in-depth security program. The IS auditor must understand the level of intruder detection provided by the different possible locations of the IDS as well as the importance of policies and procedures to determine the action required by security and technical staff when an intruder is reported.	Understanding network security threats and knowing the most appropriate controls to mitigate these threats	5.4.4 Internet Threats and Security

KS5.8 Knowledge of encryption algorithm techniques (e.g., advanced encryption standard [AES], RSA)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
One of the best ways to protect the confidentially of information is through the use of encryption. Effective encryption systems depend on: • Algorithm strength, secrecy and difficulty of compromising a key • The nonexistence of back doors by which an encrypted file can be decrypted without knowing the key • The inability to decrypt an entire ciphertext message if the way a portion of it decrypts is known (called a known-text attack) • Properties of the plaintext being known by a perpetrator Although the IS auditor is not expected to be an expert in how these algorithms are designed, the auditor should be able to understand how these techniques are used and the relative advantages and disadvantages of each.	Understanding the fundamentals of encryption techniques and the relative advantages and disadvantages of each	5.4.5 Encryption

KS5.9 Knowledge of public key infrastructure (PKI) components (e.g., certification authorities, registration authorities) and digital signature techniques

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Encryption is the process of converting a plaintext message into a secure-coded form of text, called cipher text, which cannot be understood without converting back via decryption (the reverse process) to plaintext. PKIs use encryption to facilitate the following: • Protect data in transit over networks from unauthorized interception and manipulation • Protect information stored on computers from unauthorized viewing and manipulation • Deter and detect accidental or intentional alterations of data • Verify authenticity of a transaction or document—e.g., when transmitted over a web-based connection in online banking, share dealing, etc. • Protect data in such situations from unauthorized disclosure The IS auditor is not expected to have a detailed comprehension of cryptography, but should understand the relationships between types of encryption (symmetric and asymmetric) and their respective algorithms (e.g., DES3, RSA) as well as the basic concepts and components of PKI in terms of business use. For example, if a message is encrypted with a private key, it provides authentication of the sender rather than privacy. Understanding the business use of digital signatures is also expected, especially its use in providing nonrepudiation of and replay protection to messages.	Understanding the key components of public key infrastructures and how they are controlled	5.4.5 Encryption

KS5.10 Knowledge of virus detection tools and control techniques

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Computer viruses and other malware continue to emerge at increasing rates and sophistication and present significant threats to individuals and organizations. Layered tools should be implemented and distributed throughout the environment in order to mitigate the ability of this malware to adversely impact the organization. Antivirus and antispam software is a necessary and critical component of an organization's security program, providing a mechanism to detect, contain and notify whenever malicious code is detected. It is essential that the IS auditor understand not only the need for the implementation of antimalware software, but that it should be constantly updated to ensure that it will detect and eradicate the latest attacks detected by the solutions providers.	Understanding the threats posed by malicious code and the best practices for mitigating these threats	5.4.4 Internet Threats and Security 5.4.6 Viruses

KS5.11 Knowledge of security testing and assessment tools (e.g., penetration testing, vulnerability scanning)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Tools are available to assess the effectiveness of network infrastructure security. These tools permit identification of real-time risks to an information processing environment and corrective actions taken to mitigate these risks. Such risks often involve the failure to stay updated on patch management for operating systems or the misconfiguration of security settings. Assessment tools (whether open source or commercially produced) can quickly identify weaknesses that would have taken hundreds of hours to identify manually. The IS auditor should also be aware that security testing may be carried out by an approved third party, e.g., a company specializing in penetration testing.	Understanding how assessment tools can be used to identify vulnerabilities within the network infrastructure so that corrective actions can be taken to remediate these risks	5.6 Auditing Network Infrastructure Security

KS5.12 Knowledge of environmental protection practices and devices (e.g., fire suppression, cooling systems, water sensors)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Certain natural and man-made events have the ability to do great damage to an organization's information systems and business processes. Most data centers have mechanisms to prevent, detect or mitigate the impact of these threats. However, it is important that the readiness and sufficiency of these controls be periodically tested by management to ensure that they will function as intended. The IS auditor should understand the nature of these controls and how to ensure that they are functioning properly and are adequate to protect the organization. Environmental controls generally include fire and smoke detectors, fire suppression systems, water detectors, and temperature and humidity controls. The IS auditor should know the relative merits of different fire suppression systems and in what circumstances one type is more appropriate than another.	Understanding the common types of environmental controls and best practices for their deployment and periodic testing	5.7 Environmental Exposures and Controls

KS5.13 Knowledge of physical security systems and practices (e.g., biometrics, access cards, cipher locks, tokens)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Physical security weaknesses can result in financial loss, legal repercussions, loss of credibility or loss of competitive edge. Thus, information assets must be protected against physical attacks, such as vandalism and theft, through controls that restrict access to sensitive areas containing computer equipment or confidential data files. Such controls usually employ the use of access door locks that require the use of a password, key, token, or biometric authentication of the person attempting entry. In high-security areas, access may require authentication through multiple means and the use of strong security measures such as the air lock type or "man trap entrances." The IS auditor should understand the nature of physical controls and the ways in which they can be circumvented as well as the concept of the "security boundary" to establish where such devices should be placed and how effective they must be.	Understanding physical access controls and their potential for circumvention	5.8 Physical Access Exposures and Controls

KS5.14 Knowledge of data classification schemes (e.g., public, confidential, private and sensitive data)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Information assets have varying degrees of sensitivity and criticality in meeting business objectives. An important first step to data classification is discovery, inventory and risk assessment. Once this is accomplished, data classification can then be put into use. By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules for each class, enterprises can define the level of access controls and the retention time and destruction requirements that should be applied to each information asset. Data are therefore classified and protected in accordance with the degree of sensitivity and criticality assigned to them. The IS auditor should understand the process of classification and the interrelationship between data classification and the need for inventorying information assets and assigning responsibility to data owners. Data owner responsibilities should be clearly identified, documented and implemented.	Understanding data classification schemes and the need for assignment of data owners	5.2.3 Inventory and Classification of Information Assets

KS5.15 Knowledge of voice communications security (e.g., voice-over IP)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
The increasing complexity and convergence of voice and data communications introduces additional risks that must be taken into account by the IS auditor. VoIP and PBX environments involve many security risks, both within and outside the organization, that must be addressed to ensure the security and reliability of voice communications. The IS auditor should have enough understanding of these concepts to establish the business risk and identify appropriate controls.	Understanding the risks and associated controls related to voice communications and the impact of VoIP on overall network security	5.4.7 Voice-over IP 5.4.8 Private Branch Exchange

KS5.16 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Confidential information assets are vulnerable during storage, retrieval and transport, and must be disposed of properly. Management should define and implement procedures to prevent unauthorized access to, or loss of, sensitive information and software from computers, disks and other equipment or media when they are stored, transported or transmitted, during processing, retrieval and output. The IS auditor should also understand the need for correct disposal of information (and media) in order to ensure that no unauthorized person gain access to the information by restoration or recreation.	Understanding best practices for protecting information during storage, retrieval, transport and disposal	5.3.8 Storing, Retrieving, Transporting and Disposing of Confidential Information

KS5.17 Knowledge of controls and risks associated with the use of portable and wireless devices (e.g., personal digital assistants [PDAs], universal serial bus [USB] devices, Bluetooth devices)

Explanation	Key Concepts	Reference in 2010 CISA Review Manual
Portable and wireless devices present a new threat to an organization's information assets and must be properly controlled. Policies and procedures as well as additional protection mechanisms must be put into place to ensure that data are protected to a greater extent on portable devices since such devices will most likely operate in environments where physical controls are lacking or nonexistent. Most transportable media, including PDAs, BlackBerry® devices, etc. are easily lost or stolen and thus require the use of encryption technologies as well as strong authentication. It also may be necessary to classify some data as inappropriate for storage on a mobile device. The IS auditor should understand that all such media and devices, which may include personal music (MP3) devices, can also be used by an individual to steal both data and programs for personal use or gain.	Understanding best practices for securing data on mobile computing devices	5.9 Mobile Computing

SUGGESTED RESOURCES FOR FURTHER STUDY

Brancik, Kenneth C.; *Insider Computer Fraud*, Auerbach Publications, USA, 2007

Cendrowski, Harry; James P. Martin; Louis W. Petro; *The Handbook of Fraud Deterrence*, John Wiley & Sons Inc., USA, 2006

Davis, Chris; Mike Schiller; Kevin Wheeler; *IT Auditing Using Controls to Protect Information Assets*, McGraw Hill, USA, 2007

Dubin, Joel; *The Little Black Book of Computer Security, 2nd Edition*, Penton Media Inc., USA, 2008

Harris, Shon; Allen Harper; Chris Eagle; Jonathan Ness; Michael Lester; *Gray Hat Hacking, 2nd Edition*, McGraw Hill, USA, 2007

Jaquith, Andrew; *Security Metrics*, Addison Wesley, USA, 2007

Kairab, Sudhanshu; *A Practical Guide to Security Assessments*, Auerbach Publications, USA, 2004

Killmeyer, Jan; *Information Security Architecture: An Integrated Approach to Security in the Organization, 2nd Edition*, Auerbach Publications, USA, 2006

Marcella Jr., Albert J.; Dough Menendez; *Cyber Forensics, 2nd Edition*, Auerbach Publications, USA, 2008

McClure, Stuart; Joel Sambray; George Kurtz; *Hacking Exposed, 6th Edition*, McGraw Hill, USA, 2009

Mitnick, Kevin D.; William L. Simon; *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers*, Intruders and Deceivers, Wiley Publishing, Inc., USA, 2005

Natan, Ron Ben; *Implementing Database Security and Auditing*, Elsevier Digital Press, USA, 2005

Peltier, Thomas R.; *Information Security Risk Analysis, 2nd Edition*, Auerbach Publications, USA, 2005

Stamp, Mark; *Information Security: Principles and Practice*, John Wiley & Sons, USA, 2005

Stanley, Richard A.; *Managing Risk in the Wireless Environment: Security*, Audit and Control Issues, ISACA, USA, 2005

Vacca, John R.; *Biometric Technologies and Verification Systems*, Elsevier Inc., USA, 2007

Wells, Joseph T.; *Fraud Casebook, Lessons From the Bad Side of Business*, John Wiley & Sons Inc., USA, 2007

Note: Publications in bold are stocked in the ISACA Bookstore.

PRACTICE QUESTIONS

CISA exam questions are developed with the intent of measuring and testing practical knowledge in information systems auditing. All questions are multiple choice and are designed for one best answer. Every CISA question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario or a description problem may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. Many times a CISA examination question will require the candidate to choose the most likely or best answer.

In every case, the candidate must read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked, and how to study to gain knowledge of what can be tested, will go a long way toward answering them correctly.

5-1 A utility is available to update critical tables in case of data inconsistency. This utility can be executed at the operating system (OS) prompt or as one of the menu options in an application. The **BEST** control to mitigate the risk of unauthorized manipulation of data is to:

A. delete the utility software and install it as and when required.
B. provide access to the utility on a need-to-use basis.
C. provide access to the utility to user management.
D. define access so that the utility can be executed only in the menu option.

5-2 Which of the following **BEST** provides access control to payroll data being processed on a local server?

A. Logging access to personal information
B. Using separate passwords for sensitive transactions
C. Using software that restricts access rules to authorized staff
D. Restricting system access to business hours

5-3 An IS auditor has just completed a review of an organization that has a mainframe and a client-server environment where all production data reside. Which of the following weaknesses would be considered the **MOST** serious?

A. The security officer also serves as the database administrator.
B. Password controls are not administered over the client-server environment.
C. There is no business continuity plan for the mainframe system's noncritical applications.
D. Most local area networks (LANs) do not back up file-server-fixed disks regularly.

5-4 An organization is proposing to install a single sign-on facility giving access to all systems. The organization should be aware that:

A. maximum unauthorized access would be possible if a password is disclosed.
B. user access rights would be restricted by the additional security parameters.
C. the security administrator's workload would increase.
D. user access rights would be increased.

5-5 An IS auditor reviewing the log of failed logon attempts would be **MOST** concerned if which of the following accounts was targeted?

A. Network administrator
B. System administrator
C. Data administrator
D. Database administrator

5-6 A B-to-C e-commerce web site as part of its information security program wants to monitor, detect and prevent hacking activities and alert the system administrator when suspicious activities occur. Which of the following infrastructure components could be used for this purpose?

A. Intrusion detection systems
B. Firewalls
C. Routers
D. Asymmetric encryption

5-7 Which of the following **BEST** determines whether complete encryption and authentication protocols for protecting information while being transmitted exist?

A. A digital signature with RSA has been implemented.
B. Work is being done in tunnel mode with the nested services of authentication header (AH) and encapsulating security payload (ESP).
C. Digital certificates with RSA are being used.
D. Work is being done in transport mode with the nested services of AH and ESP.

5-8 Which of the following concerns about the security of an electronic message would be addressed by digital signatures?

A. Unauthorized reading
B. Theft
C. Unauthorized copying
D. Alteration

5-9 Which of the following would be **MOST** appropriate to ensure the confidentiality of transactions initiated via the Internet?

A. Digital signature
B. Data Encryption Standard (DES)
C. Virtual private network (VPN)
D. Public key encryption

5-10 Which of the following is the **MOST** effective antivirus control?

A. Scanning e-mail attachments on the mail server
B. Restoring systems from clean copies
C. Disabling USB ports
D. An online antivirus scan with up-to-date virus definitions

ANSWERS TO PRACTICE QUESTIONS

5-1 **B** Utility software, in this case, is a data correction program for correcting any inconsistency in data. However, this utility can be used to override the incorrect update of tables directly. Therefore, access to this utility should be restricted on a need-to-use basis, and a log should be generated automatically whenever this utility is executed. Senior management should review this log periodically. Deleting the utility and installing it as and when required may not be practically feasible since there would be a time delay. Access to utilities should not be provided to user management. Defining access so that the utility can be executed in a menu option may not generate a log.

5-2 **C** The server and system security should be defined to allow only authorized staff members access to information about the staff whose records they handle on a day-to-day basis. Choice A is a good control in that it will allow access to be analyzed if there is concern of unauthorized access. However, it will not prevent access. Choice B, restricting access to sensitive transactions, will restrict access only to some of the data. It will not prevent access to other data. Choice D, system access restricted to business hours, only restricts when unauthorized access can occur and would not prevent such access at other times. It is important to consider that the data owner is responsible for determining who is allowed access via the written software access rules.

5-3 **B** The absence of password controls on the client-server, where production data reside, is the most critical weakness. All other findings, while they are control weaknesses, do not carry the same disastrous impact.

5-4 **A** If a password is disclosed when single sign-on is enabled, there is a risk that unauthorized access to all systems will be possible. User access rights should remain unchanged by single sign-on, as additional security parameters are not implemented necessarily. One of the intended benefits of single sign-on is the simplification of security administration and the unlikelihood of an increased workload.

5-5 **B** It is not possible to lock out the system administrator account after several failed logon attempts, because it would be impossible to unlock it. Therefore, it is subject to online brute force attacks. The IS auditor should be most concerned with any failed logon attempts targeted to this account. All other choices can be locked automatically by the system.

5-6 **A** IDSs detect intrusion activity based on the intrusion rules. They can detect external and internal intrusion activity and send an automated alarm message. Firewalls and routers prevent the unwanted and well-defined communications between the internal and external networks. They do not have any automatic alarm messaging systems.

5-7 **B** Tunnel mode provides encryption and authentication of the complete IP package. To accomplish this, the authentication header (AH) and encapsulating security payload (ESP) services can be nested. The transport mode provides primary protection for the protocols' higher layers; that is, protection extends to the data field (payload) of an IP package. The other two mechanisms provide authentication and integrity.

5-8 **D** A digital signature includes an encrypted hash total of the size of the message as it was transmitted by its originator. This hash would no longer be accurate if the message was altered subsequently, indicating that the alteration had occurred. Digital signatures will not identify or prevent any of the other options. The signature would neither prevent nor deter unauthorized reading, copying or theft.

5-9 **D** Encryption is the only way to ensure that Internet transactions are confidential and, of the choices available, the use of public key encryption is the best method. Digital signatures would ensure that the transaction is not changed and cannot be repudiated, but would not ensure confidentiality.

5-10 **D** Antivirus software can be used to prevent virus attacks. By running regular scans, it can also be used to detect virus infections that have already occurred. Regular updates of the software are required to ensure it is able to update, detect and treat viruses as they emerge. Scanning e-mail attachments on the mail server is a preventive control. It will prevent infected e-mail files from being opened by the recipients, which would cause their machines to become infected. Restoring systems from clean copies is a preventive control. It will ensure that viruses are not introduced from infected copies or backups, which would reinfect machines. Disabling USB ports is a preventive control. It prevents infected files from being copied from a USB drive onto a machine, which would cause the machine to become infected.

Section Two: Content

5.1 QUICK REFERENCE

Quick Reference Review

Chapter 5 addresses the need for the protection of information assets within an organization. Protection of information assets includes the key components that ensure confidentiality, integrity and availability (CIA) of information assets. The chapter evaluates design, implementation and monitoring of logical and physical access controls to ensure CIA. The chapter also evaluates network infrastructure security, environmental controls and processes and procedures used to store, retrieve, transport and dispose of confidential information assets. The chapter describes the various methods and procedures followed by organizations and focuses on the auditor's role in evaluating these procedures. Many of these topics may, on the surface, seem very familiar to candidates; however, it is important to note that the topics addressed in this chapter require a thorough knowledge of the technologies used and the potential control weaknesses that may develop. CISA candidates should be fully aware of and conversant with the components of network infrastructure security, logical access issues and the key elements of information security management.

CISA candidates should have a sound understanding of the following items, not only within the context of the present chapter, but also to correctly address questions in related subject areas. It is important to keep in mind that it is not enough to know these concepts from a definitional perspective. The CISA candidate must also be able to identify which elements may represent the greatest risk and which controls are most effective at mitigating this risk. Examples of key topics in this chapter include:

- Key elements of information security management include: senior management commitment and support, policies and procedures, organization, security awareness and education, monitoring and compliance, and incident handling and response.
- General points of logical entry into a system should be understood, including logical protection at the network, platform, database and application layers. CISA candidates may be asked to identify how a failure at one layer could allow an unauthorized individual to bypass certain logical security mechanisms and gain access to confidential data.
- It is important to know best practices for identification and authentication. This includes practices for handling default system accounts, normal user accounts and privileged user accounts such as system administrators.
- CISA candidates should understand the differences between various types of biometric technologies, and the advantages and disadvantages of each.
- CISA candidates should be familiar with network infrastructure security, various issues and risks associated with different technologies used in network infrastructures, and best practices for risk mitigation. Special attention should be focused on firewall implementation, the advantages and disadvantages of different types of intrusion detection/prevention systems, and encryption technologies.
- The importance of O/S patching to remediate vulnerabilities and how patching should be deployed should also be understood.

5.2 IMPORTANCE OF INFORMATION SECURITY MANAGEMENT

The most critical factor in protecting information assets and privacy is laying the foundation for effective information security management. The advent of electronic trading through service providers and directly with customers; the loss of organizational barriers through use of remote access facilities; and high-profile security exposures, such as viruses, denial of service (DoS) attacks, intrusions, unauthorized access, disclosures and identity theft over the Internet, have raised the profile of information and privacy risk, and the need for effective information security management.

Security objectives to meet organization's business requirements include the following:

- Ensure the continued availability of their information systems.
- Ensure the integrity of the information stored on their computer systems and while in transit.
- Preserve the confidentiality of sensitive data while stored and in transit.
- Ensure conformity to applicable laws, regulations and standards.
- Ensure adherence to trust and obligation requirements in relation to any information relating to an identified or identifiable individual (i.e., data subject) in accordance with its privacy policy or applicable privacy laws and regulations.

It is important to recognize that these objectives are necessary, but not sufficient since patterns often come into play regarding the objective of retaining competitive advantage. However, this section will not deal with ways and approaches to maintain such advantage, but rather how to protect the IT systems from security pitfalls affecting their contents or operation.

With regard to data integrity as it relates to security objectives, it should be noted that the data/information integrity concept refers generally to the accuracy, completeness, consistency (or neutrality), validity and verifiability of the data once they have been input or loaded on the system (see chapter 4, IT Service Delivery and Support, on system usage and for ways of validating information to be fed into the system). Integrity refers to reliability of the data. Information relevance is an afterthought.

5.2.1 KEY ELEMENTS OF INFORMATION SECURITY MANAGEMENT

Security failures can be costly to business. Losses may be suffered as a result of the failure itself or costs may be incurred when recovering from the incident, followed by more costs to secure systems and prevent further failure.

An IT system packed with security features and devices will not be protected unless it is properly implemented and managed and carefully operated, monitored and reviewed; just as the best safety features of a vehicle might prove useless if the driver is careless or if that vehicle is not properly maintained. Security objectives cannot be met by simply affecting technical and procedural protections. An educated security attitude and attention by all employees, management as well as external service providers and

external trusted IT users/partners are vital to the achievement of security objectives. IS security is more than just a mechanism. IS security also includes cultural aspects that must be embraced by all individuals within an organization for IS security to be effective.

Note: For a detailed overview of Information Security Governance, please refer to that section in chapter 2 on IT governance.

Exhibit 5.2 depicts the related key elements of information security management.

Exhibit 5.2—Key Elements of Information Security Management	
Senior management commitment and support	Commitment and support from senior management are important for successful establishment and continuance of an information security management program.
Policies and procedures	The policy framework should be established with a concise top management declaration of direction, addressing the value of information assets, the need for security, and the importance of defining a hierarchy of classes of sensitive and critical assets. After approval by the governing body of the organization and by related roles and responsibilities, the information security program will be substantiated with the following: • Standards to develop minimum security baselines • Measurement criteria and methods • Specific guidelines, practices and procedures The policy should ensure resource conformity with laws and regulations. Security policies and procedures must be up to date and reflect business objectives, as well as generally accepted security standards and practices.
Organization	Responsibilities for the protection of individual assets should be clearly defined. The information security policy should provide general guidance on the allocation of security roles and responsibilities in the organization and, where necessary, detailed guidance for specific sites, assets, services and related security processes, such as IT recovery and business continuity planning.
Security awareness and education	All employees of an organization and, where relevant, third-party users should receive appropriate training and regular updates to foster security awareness and compliance with written security policies and procedures. For new employees, this training should occur before access to information or service is granted. A number of different mechanisms available for raising security awareness include: • Regular updates to written security policies and procedures • Formal information security training • Internal certification program for relevant personnel • Statements signed by employees and contractors agreeing to follow the written security policy and procedures, including nondisclosure obligations • Use of appropriate publication media for distribution of security-related material (e.g., company newsletter, web page, videos, etc.) • Visible enforcement of security rules and periodic audits • Security drills and simulated security incidents
Monitoring and compliance	IS auditors are usually charged to assess, on a regular basis, the effectiveness of an organization's security program(s). To fulfill this task, they must have an understanding of the protection schemes, the security framework and the related issues, including compliance with applicable laws and regulations. As an example, these issues may relate to organizational due diligence for security and privacy of sensitive information, particularly as it relates to specific industries (e.g., banking and financial institutions, health care).
Incident handling and response	A computer security incident is an event adversely affecting the processing of computer usage. This includes loss of confidentiality of information, compromise of integrity of information, denial of service, unauthorized access to systems, misuse of systems or information, theft and damage to systems. Other incidents include virus attacks and intrusion by humans within or outside the organization.

5.2.2 INFORMATION SECURITY MANAGEMENT ROLES AND RESPONSIBILITIES

All defined and documented responsibilities and accountabilities must be established and communicated to all relevant personnel and management. **Exhibit 5.3** presents roles and responsibilities of groups who interact with information security management.

Exhibit 5.3—Group Roles and Responsibilities as Related to Information Security Management	
IS security steering committee	Security policies, guidelines and procedures affect the entire organization and, as such, should have the support and suggestions of end users, executive management, auditors, security administration, IS personnel and legal counsel. Therefore, individuals representing various management levels should meet as a committee to discuss these issues, and establish and approve security practices. The committee should be formally established with appropriate terms of reference.
Executive management	Responsible for the overall protection of information assets, and for issuing and maintaining the policy framework.
Security advisory group	Responsible for the review of the security plans of the organization. This group should include people involved in the business. The group should provide comments on security issues to the chief security officer and communicate to the business whether the security programs meet the business objectives.
Chief privacy officer (CPO)	A senior level corporate official responsible for articulating and enforcing the policies that companies use to protect their customers' and employees' privacy rights.
Chief information security officer (CISO)	A senior level corporate official responsible for articulating and enforcing the policies that companies use to protect their information assets. This is a much broader roll than a chief security officer (CSO), who is normally only responsible for physical security within the organization.

Exhibit 5.3—Group Roles and Responsibilities as Related to Information Security Management *(cont.)*	
Process owners	Ensure appropriate security measures are consistent with organizational policy and are maintained.
Information assets owners and data owners	Ownership entails responsibility for the owned asset.
Users	Follow procedures set out in the organization's security policy and adhere to privacy and security regulations, which are often specific to sensitive application fields (e.g., health, finance, legal, etc.).
External parties	Include third-party providers and trading partners that deal with the organization's information assets or have access to company premises.
Security administrator	Staff level position responsible for providing adequate physical and logical security for IS programs, data and equipment. Normally, the information security policies will provide the basic guidelines under which the security administrator will operate.
Security specialists/ advisors	Assist with the design, implementation, management and review of the organization's security policy, standards and procedures.
IT developers	Implement information security within their applications.
IS auditors	Provide independent assurance to management on the appropriateness and effectiveness of information security objectives and the controls related to these objectives.

5.2.3 INVENTORY AND CLASSIFICATION OF INFORMATION ASSETS

Effective control requires a detailed inventory of information assets. Such a list is the first step in classifying the assets and determining the level of protection to be provided to each asset.

The inventory record of each information asset should include:
- Specific identification of the asset
- Relative value to the organization
- Location
- Security/risk classification
- Asset group (where the asset forms part of a larger information system)
- Owner
- Designated custodian

Information assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules for each class, it is possible to define the level of access controls that should be applied to each information asset. Classification of information assets reduces the risk and cost of over- or under-protecting information resources in linking security to business objectives since it helps to build and maintain a consistent perspective of the security requirements for information assets throughout the organization. ISO 17799 recommends the inventorying of information assets and the classification, handling and labeling of information in accordance with preset guidelines.

Classifications should be simple such as designations by differing degrees for sensitivity and criticality. End-user managers and security administrators can then use these classifications in their risk assessment process to assist with determining who should be able to access what, and the most appropriate level of such access. Most organizations use a classification scheme with three to five levels of sensitivity. The number of classification categories should take into consideration the size and nature of the organization and the fact that complex schemes may become too impractical to use.

Data should always be treated as a core IS asset. Categorizing data is a major part of the task of classifying all information assets. Data classification as a control measure should define:
- the owner of the information asset
- who has access rights (need to know)
- the level of access to be granted
- who is responsible for determining the access rights and access levels
- What approvals are needed for access
- The extent and depth of security controls

For instance, application programmers or system development programmers should not have access to production data or programs.

Data classification must take into account legal/regulatory/ contractual/internal requirements for maintaining privacy, confidentiality, integrity and availability of information. Data classification is also useful to identify who should have access to the production data used to run the business versus those who are permitted to access test data and programs under development.

Adopting a classification scheme and assigning the information to one sensitivity level enables uniform treatment of data, through applying level-specific policies and procedures rather than addressing each type of information. It is highly difficult to follow information security policies if documents and media are not assigned to a sensitivity level and users are not instructed how to deal with each piece of information. If documents or media are not labeled according to a classification scheme, this is an indicator of a potential misuse of information. Users might reveal confidential information because they did not know that the requirements prohibited disclosure. Social engineering capitalizes on this kind of misunderstanding at the end user level.

Public Information	Company brochures
Private Information	Internal policies, procedures, normal business e-mail messages, newsletter, etc.
Sensitive Information	Unpublished financials, company secrets, etc.

5.2.4 SYSTEM ACCESS PERMISSION

System access permission is the prerogative to act on a computer resource. This usually refers to a technical privilege, for example, the ability to read, create, modify or delete a file or data; execute a program; or open or use an external connection.

System access to computerized information resources is established, managed and controlled at the physical and/or logical level. Physical system access controls restrict the entry and exit of personnel to an area such as an office building, suite, data center or room containing information processing equipment such as a local area network (LAN) server. There are many types of physical access controls including badges, memory cards, guard keys, true floor-to-ceiling wall construction fences, locks and biometrics. Logical system access controls restrict the logical resources of the system (transactions, data, programs, applications) and are applied when the subject resource is needed. On the basis of identification and authentication of the user that requires a given resource and by analyzing the security profiles of the user and the resource, it is possible to determine if the requested access is to be allowed, i.e., what information users can utilize, the programs or transactions they can run, and the modifications they can make. Such controls may be built into the operating system, invoked through separate access control software and incorporated into application programs, database systems, network control devices and utilities (e.g., real-time performance monitors).

Physical or logical system access to any computerized information should be on a documented need-to-know basis where there is a legitimate business requirement based on least privilege and segregation of duties. These principles should be used by IS auditors when they evaluate the appropriateness of criteria for defining permissions and granting security privileges. Organizations should establish such basic criteria for assigning technical access to specific data, programs, devices and resources, including who will have access and what level of access they will be allowed. For instance, it may be desirable for everyone in the organization to have access to specific information on the system such as the data displayed on an organization's daily calendar of routine meetings. The program that formats and displays the calendar, however, might be modifiable by only a few system administrators, while the operating system controlling that program might be directly accessible by still fewer.

The IT assets under logical security can be grouped in four layers—networks, platforms (operating systems), databases and applications. This concept of layered security for system access provides greater scope and granularity of control to information resources. For example, network and platform layers provide pervasive general systems control over users authenticating into systems, system software and application configurations, data sets, load libraries, and any production data set libraries. Database and application controls generally provide a greater degree of control over user activity within a particular business process by controlling access to records, specific data fields and transactions.

The information owner or manager who is responsible for the accurate use and reporting of information should provide written authorization for users or defined roles to gain access to information resources under their control. The manager should hand over this documentation directly to the security administrator to ensure that mishandling or alteration of the authorization does not occur.

Logical access capabilities are implemented by security administration in a set of access rules that stipulate which users (or groups of users) are authorized to access a resource at a particular level (e.g., read-, update- or execute-only) and under which conditions (e.g., time of the day or a subset of computer terminals). The security administrator invokes the appropriate system access control mechanism upon receipt of a proper authorization request from the information owner or manager to grant a specified user the rights for access to, or use of, a protected resource. The IS auditor should be aware that access is granted to the organization's information systems utilizing the principles of need-to-know, least privilege and segregation of duties.

Reviews of access authorization should be evaluated regularly to ensure that they are still valid. Personnel and departmental changes, malicious efforts, and just plain carelessness result in authorization creep and can impact the effectiveness of access controls. Many times, access is not removed when personnel leave an organization, thus increasing the risk of unauthorized access. For this reason, the information asset owner should review access controls periodically with a predetermined authorization matrix that defines the least-privileged access level and authority for an individual/role with reference to his/her job roles and responsibilities. Any access exceeding the access philosophy in authorized matrix or in actual access levels granted on a system should be updated and changed accordingly. One of the best practices is to integrate the review of access rights with human resource processes. When an employee transfers to a different function, i.e., promotions, lateral transfers or demotions, access rights are adjusted at the same time. Development of a security-conscious culture increases the effectiveness of access controls.

Nonemployees with access to corporate IS resources should also be held responsible for security compliance and be accountable for security breaches. Nonemployees include contract employees, vendor programmers/analysts, maintenance personnel, clients, auditors, visitors and consultants. It should be understood that nonemployees are also accountable to the organization's security requirements.

5.2.5 MANDATORY AND DISCRETIONARY ACCESS CONTROLS

Mandatory access controls (MACs) are logical access control filters used to validate access credentials that cannot be controlled or modified by normal users or data owners; they act by default. Controls that may be configured or modified by the users or data owners are called discretionary access controls (DACs).

MACs are a good choice to enforce a ground level of critical security without possible exception, if this is required by corporate security policies or other security rules. A MAC could be carried out by comparing the sensitivity of the information resources, such as files, data or storage devices, kept on a user-unmodifiable tag attached to the security object with the security clearance of the accessing entity such as a user or an application. With MACs, only administrators may make decisions that are derived from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy. MACs are prohibitive; anything that is not expressly permitted is forbidden.

DACs are a protection that may be activated or modified by the data owner, at his/her discretion. This would be the case of data owner-defined sharing of information resources, where the data owner may select who will be enabled to access his/her resource and the security level of this access. DACs cannot override MACs; DACs act as an additional filter, prohibiting still more access with the same exclusionary principle.

When information systems enforce MAC policies, the systems must distinguish between MAC and the discretionary policies that offer more flexibility. This distinction must be ensured during object creation, classification downgrading and labeling.

5.2.6 PRIVACY MANAGEMENT ISSUES AND THE ROLE OF IS AUDITORS

Privacy means adherence to trust and obligation in relation to any information relating to an identified or identifiable individual (data subject).

Privacy is an organizationwide matter that, by its nature, requires a consistent approach throughout the organization. Therefore, it should be systematically built into policies, standards and procedures from the beginning. To best meet this challenge, management should perform privacy impact analysis or assessments that IT auditors may be called in to support or review. Such assessment should:

- Pinpoint the nature of personally identifiable information associated with business processes
- Document the collection, use, disclosure and destruction of personally identifiable information
- Ensure that accountability for privacy issues exists
- Be the foundation for informed policy, operations and system design decisions based on an understanding of privacy risk and the options available for mitigating that risk

Based on the results, it should be possible to create a consistent format and structured process for analyzing technical and legal compliance with relevant regulations and internal policies. This structured process would provide a framework to ensure that privacy is considered in all IT projects, from the conceptual and requirements analysis stage to the final design approval, funding, implementation and communication stage, so that privacy compliance is built into projects rather than retrofit.

The focus and extent of privacy impact analysis or assessment may vary depending on changes in:

Technology	Processes	People
• New programs • Changes in existing programs • Additional system linkages • Data warehouse • New products	• Change management • Business process reengineering • Enhanced accessibility rules • New systems • New operations	• Business partners • Vendors • Service providers

The IS auditor may also be called on to give assurance to the responsible managers concerning the compliance with privacy policy, laws and other regulations. To fulfill this role, the IS auditor should:

- Identify and understand legal requirements regarding privacy from laws, regulations and contract agreements
- Check whether personal data are correctly managed in respect to these requirements
- Verify that the correct security measures are adopted
- Review management's privacy policy to ascertain that it takes into consideration the requirement of applicable privacy laws and regulations. This includes transborder data flow requirements such as Safe Harbor and Organization for Economic Cooperation and Development (OECD) guidelines governing the protection of privacy and transborder flows of personal data.

In assessing applicable privacy laws and regulations that need to be complied with by any particular organization, particularly for organizations operating in a different part of the globe, IS auditors should seek expert opinion on the requirements of any laws and regulations, and should carry out the necessary compliance and substantive tests to form an opinion and report on the compliance of such laws and regulations.

5.2.7 CRITICAL SUCCESS FACTORS TO INFORMATION SECURITY MANAGEMENT

Managers and employees within an organization often tend to consider information security as a secondary priority if compared with their own efficiency or effectiveness matters because these have a direct and material impact on the outcome of their work.

For this reason, a strong commitment and support by the senior management on security training is needed, over and above the aforementioned role concerning the information security policy. This commitment should be supported with a comprehensive program of formal security awareness training. This may require special management-level training since security is not necessarily a part of management expertise. The security training for different functions within the organization needs to be customized to address specific security needs. Different functions have different levels of risk. For example infrastructure staff need technical security training, whereas security management requires training that will show the link between information security management and the needs of the organization.

A second vital point is that a professional risk-based approach must be used systematically to identify sensitive and critical information resources and to ensure that there is a clear understanding of threats and risks. Thereafter, appropriate risk assessment activities should be undertaken to mitigate unacceptable risks and ensure that residual risks are at an acceptable level.

5.2.8 INFORMATION SECURITY AND EXTERNAL PARTIES

The security of the organization's information and information processing facilities that are accessed, processed, communicated to or managed by external parties should be maintained, and

should not be reduced by the introduction of external party products or services. Any access to the organization's information processing facilities and processing, and communication of information by external parties should be controlled. Where there is a business need for working with external parties that may require access to the organization's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed to and defined in an agreement with the external party. Organizations shall gain the right to audit the implementation and operation of the resulting security controls.

These external party arrangements can include:
- Service providers such as internet service providers (ISPs), network providers, telephone services, maintenance and support services
- Managed security services
- Customers
- Outsourcing facilities and/or operations, e.g., IT systems, data collection services, call center operations
- Management and business consultants and auditors
- Developers and suppliers, e.g., of software products and IT systems
- Cleaning, catering and other outsourced support services
- Temporary personnel, student placement and other casual short-term appointments

Such agreements can help to reduce the risks associated with external parties.

Identification of Risks Related to External Parties

The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. Where there is a need to allow an external party access to the information processing facilities or information of an organization, a risk assessment should be carried out to identify any requirements for specific controls. The identification of risks related to external party access should take into account the issues depicted in **exhibit 5.4**.

Exhibit 5.4—Risks Related to External Party Access

- The information processing facilities an external party is required to access
- The type of access the external party will have to the information and information processing facilities, for example:
  - Physical access, e.g., to offices, computer rooms and filing cabinets
  - Logical access, e.g., to an organization's databases and information systems
  - Network connectivity between the organization's and the external party's network(s), e.g., permanent connection and remote access
  - Whether the access is taking place onsite or offsite
- The value and sensitivity of the information involved, and its criticality for business operations
- The controls necessary to protect information that is not intended to be accessible by external parties
- The external party personnel involved in handling the organization's information

Exhibit 5.4—Risks Related to External Party Access *(cont.)*

- How the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed
- The different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information
- The impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information
- Practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident
- Legal and regulatory requirements and other contractual obligations relevant to the external party that should be taken into account
- How the interests of any other stakeholders may be affected by the arrangements

Access by external parties to the organization's information should not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected by the agreement with the external party. It should be ensured that the external party is aware of its obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating or managing the organization's information and information processing facilities.

External parties might put information at risk if their security management is inadequate. Controls should be identified and applied to administer external party access to information processing facilities. For example, if there is a special need for confidentiality of the information, nondisclosure agreements might be used. Organizations may face risks associated with interorganizational processes, management and communication, if a high degree of outsourcing is applied or where there are several external parties involved.

Addressing Security When Dealing With Customers

All identified security requirements should be addressed before giving customers access to the organization's information or assets.

The items presented in **exhibit 5.5** should be considered to address security prior to giving customers access to any of the organization's assets (depending on the type and extent of access given, not all of them may apply).

Exhibit 5.5—Customer Access Security Considerations

- Asset protection, including:
  - Procedures to protect the organization's assets, including information and software, and management of known vulnerabilities
  - Procedures to determine whether any compromise of the assets, e.g., loss or modification of data, has occurred
  - Integrity
  - Restrictions on copying and disclosing information
- Description of the product or service to be provided
- The different reasons, requirements and benefits for customer access

Exhibit 5.5—Customer Access Security Considerations *(cont.)*

- Access control policy, covering:
  - Permitted access methods, and the control and use of unique identifiers such as user IDs and passwords
  - An authorization process for user access and privileges
  - A statement that all access that is not explicitly authorized is forbidden
  - A process for revoking access rights or interrupting the connection between systems
- Arrangements for reporting, notification and investigation of information inaccuracies (e.g., of personal details), information security incidents and security breaches
- The target level of service and unacceptable levels of service
- The right to monitor and revoke any activity related to the organization's assets
- The respective liabilities of the organization and the customer
- Responsibilities with respect to legal matters and ensuring that the legal requirements are met, e.g., data protection legislation, especially taking into account different national legal systems if the agreement involves cooperation with customers in other countries
- Intellectual property rights (IPRs) and copyright assignment, and protection of any collaborative work

The security requirements related to customers accessing organizational assets can vary considerably depending on the information processing facilities and information being accessed. These security requirements can be addressed using customer agreements that contain all identified risks and security requirements.

Agreements with external parties may also involve other parties. Agreements granting an external party access should include an allowance for designation of other eligible parties and conditions for their access and involvement.

Addressing Security in Third-party Agreements

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements. The agreement should ensure that there is no misunderstanding between the organization and the third party. The organization should ensure that the agreement includes adequate indemnification provisions to protect against potential losses caused by the actions of the third party.

The contract terms listed in **exhibit 5.6** should be considered for inclusion in the agreement to satisfy the identified security requirements.

Exhibit 5.6—Recommended Contract Terms for Third Party Agreements

- The information security policy
- Controls to ensure asset protection, including:
  - Procedures to protect organizational assets, including information, software and hardware
  - Any required physical protection controls and mechanisms
  - Controls to ensure protection against malicious software
  - Procedures to determine whether any compromise of the assets, e.g., loss or modification of information, software and hardware, has occurred

Exhibit 5.6—Recommended Contract Terms for Third Party Agreements *(cont.)*

  - Controls to ensure the return or destruction of information and assets at the end of or at an agreed point in time during the agreement
  - Confidentiality, integrity, availability and any other relevant property of the assets
  - Restrictions on copying and disclosing information, and using confidentiality agreements
- User and administrator training in methods, procedures and security
- A means to ensure user awareness of information security responsibilities and issues
- Provision for the transfer of personnel, where appropriate
- Responsibilities regarding hardware and software installation, and maintenance
- A clear reporting structure and agreed reporting formats
- A clear and specified process for change management
- Access control policy, covering
  - The different reasons, requirements and benefits that make the access by the third party necessary
  - Permitted access methods, and the control and use of unique identifiers such as user IDs and passwords
  - An authorization process for user access and privileges
  - A requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use
  - A statement that all access that is not explicitly authorized is forbidden
  - A process for revoking access rights or interrupting the connection between systems
- Arrangements for reporting, notification, and investigation of information security incidents and security breaches as well as violations of the requirements stated in the agreement
- A description of the product or service to be provided, and a description of the information to be made available along with its security classification
- The target level of service and unacceptable levels of service
- The definition of verifiable performance criteria, their monitoring and reporting
- The right to monitor and revoke any activity related to the organization's assets
- The right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors (and, where appropriate, the provision of a service auditor's report)
- The establishment of an escalation process for problem resolution
- Service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities
- The respective liabilities of the parties to the agreement
- Responsibilities with respect to legal matters and ensuring that the legal requirements are met, e.g., data protection legislation, especially taking into account different national legal systems if the agreement involves cooperation with organizations in other countries
- IPRs and copyright assignment and protection of any collaborative work
- Involvement of the third party with subcontractors, and the security controls these subcontractors need to implement
- Conditions for renegotiation/termination of agreements such as:
  - A contingency plan in case either party wishes to terminate the relationship before the end of the agreements
  - A provision for renegotiation of agreements if the security requirements of the organization change
- Current documentation of asset lists, licenses, agreements or rights relating to them

In general, it is very difficult to ensure the return or destruction of confidential information disclosed to a third party at the end of the agreement. To prevent unauthorized copies or use, printed documents should be consulted on site. Using technical controls

such as digital rights management (DRM) should be considered to set up the desired constraints such as the printing of the document, copying, authorized readers, or using it after a certain date.

The agreements can vary considerably for different organizations and among the different types of third parties. Therefore, care should be taken to include all identified risks and security requirements in the agreements. Where necessary, the required controls and procedures can be expanded in a security management plan.

If information security management is outsourced, the agreements should address how the third party will guarantee that adequate security, as defined by the risk assessment, will be maintained, and how security will be adapted to identify and deal with changes to risks. Some of the differences between outsourcing and the other forms of third-party service provision include the question of liability, planning the transition period and potential disruption of operations during this period, contingency planning arrangements and due diligence reviews, and collection and management of information on security incidents. Therefore, it is important that the organization plans and manages the transition to an outsourced arrangement and has suitable processes in place to manage changes and the renegotiation/termination of agreements.

The procedures for continuing processing in the event that the third party becomes unable to supply its services need to be considered in the agreement to avoid any delay in arranging replacement services. Agreements with third parties may also involve other parties. Agreements granting third-party access should include allowance for designation of other eligible parties and conditions for their access and involvement.

Generally, agreements are primarily developed by the organization. There may be occasions in some circumstances where an agreement may be developed and imposed upon an organization by a third party. The organization needs to ensure that its own security is not unnecessarily impacted by third-party requirements stipulated in imposed agreements.

5.2.9 HUMAN RESOURCES SECURITY AND THIRD PARTIES

Proper information security practices should be in place to ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities, specifically:

- Security responsibilities should be addressed prior to employment in adequate job descriptions, and in terms and conditions of employment.
- All candidates for employment, contractors and third-party users should be adequately screened, especially for sensitive jobs.
- Employees, contractors and third-party users of information processing facilities should sign an agreement on their security roles and responsibilities, including the need to maintain confidentiality.

Security roles and responsibilities of employees, contractors and third-party users should be defined and documented in accordance with the organization's information security policy.

Screening

Background verification checks on all candidates for employment, contractors and third-party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed and the perceived risks. A screening process should be carried out for contractors and third-party users. Where contractors are provided through an agency, the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third party should clearly specify all responsibilities and notification procedures for screening.

Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors and third-party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security. The terms and conditions of employment should reflect the organization's security policy in addition to clarifying and stating:

- That all employees, contractors and third-party users who are given access to sensitive information should sign a confidentiality or nondisclosure agreement prior to being given access to information processing facilities
- The employee, contractor and any other user's legal responsibilities and rights, e.g., regarding copyright laws or data protection legislation
- Responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third-party user
- Responsibilities of the employee, contractor or third-party user for the handling of information received from other companies or external parties
- Responsibilities of the organization for the handling of personal information, including personal information created as a result of, or in the course of, employment with the organization
- Responsibilities that are extended outside the organization's premises and outside normal working hours, e.g., in the case of working at home
- Actions to be taken if the employee, contractor or third-party user disregards the organization's security requirements

The organization should ensure that employees, contractors and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

During Employment

Management should require employees, contractors and third-party users to apply security in accordance with the established policies and procedures of the organization. Specific responsibilities should be documented in approved job descriptions. This will help ensure that employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work and to reduce the risk of human error. Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organization. An adequate level of awareness, education and training in security procedures and the correct use of information processing facilities should be provided to all employees, contractors and third-party users to minimize possible security risks. A formal disciplinary process for handling security breaches should be established.

Termination or Change of Employment

Responsibilities should be in place to ensure that an employee, contractor or third-party user's exit from the organization is managed and that the return of all equipment and the removal of all access rights are completed. The communication of termination responsibilities should include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement, and the terms and conditions of employment continuing for a defined period after the end of the employee, contractor or third-party user's employment. Responsibilities and duties still valid after termination of employment should be contained in the employee, contractor or third-party user's contracts.

Removal of Access Rights

The access rights of all employees, contractors and third-party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. The access rights that should be removed or adapted include physical and logical access, keys, identification cards, information processing facilities, subscriptions, and removal from any documentation that identifies them as a current member of the organization. This should include notifying partners and relevant third parties—if a departing employee has access to the third party premises. If a departing employee, contractor or third-party user has known passwords for accounts remaining active, these should be changed upon termination or change of employment, contract or agreement. Access rights for information assets and information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

- Whether the termination or change is initiated by the employee, contractor or third-party user, or by management and the reason of termination
- The current responsibilities of the employee, contractor or any other user
- The value of the assets currently accessible

Procedures should be in place to ensure that information security management is promptly informed of all employee movements, including employees leaving the organization.

5.2.10 COMPUTER CRIME ISSUES AND EXPOSURES

Computer systems can be used to steal money, goods, software or corporate information. Crimes can also be committed when the computer application process or data are manipulated to accept false or unauthorized transactions. There is also the simple, nontechnical method of computer crime: stealing computer equipment.

Computer crime can be performed with absolutely nothing physically being taken or stolen, and it can be done at the ease of logging in from home or a coffee shop. Simply viewing computerized data can provide an offender with enough intelligence to steal ideas or confidential information (intellectual property). In case of the systems connected to wide area networks (WANs) or the Internet, the crime scene could be anywhere in the world, making the investigation very difficult. Cyber-criminals take advantage of existing gaps in the legislation of different countries when planning cyber attacks in order to avoid prosecution.

Committing crimes that exploit the computer and the information it contains can be damaging to the reputation, morale and the continued existence of an organization. Loss of customers or market share, embarrassment to management and legal actions against the organization can be a result. Threats to business include the following:

- **Financial loss**—These losses can be direct, through loss of electronic funds, or indirect, through the costs of correcting the exposure.
- **Legal repercussions**—There are numerous privacy and human rights laws an organization should consider when developing security policies and procedures. These laws can protect the organization but also can protect the perpetrator from prosecution. In addition, not having proper security measures could expose the organization to lawsuits from investors and insurers if a significant loss occurs from a security violation. Most companies must also comply with industry-specific regulatory agencies' requirements. The IS auditor should obtain legal assistance when reviewing the legal issues associated with computer security.
- **Loss of credibility or competitive edge**—Many organizations, especially service firms such as banks, savings and loans and investment firms, need credibility and public trust to maintain a competitive edge. A security violation can damage this credibility severely, resulting in loss of business and prestige.
- **Blackmail/industrial espionage/organized crime**—By gaining access to confidential information or the means to adversely impact computer operations, a perpetrator can extort payments or services from an organization by threatening to exploit the security breach or publicly disclose the confidential information of the organization. Also, by gaining access, the perpetrator could obtain proprietary information and sell it to a competitor.
- **Disclosure of confidential, sensitive or embarrassing information**—As noted previously, such events can damage an organization's credibility and its means of conducting business. Legal or regulatory actions against the company may also be the result of disclosure.
- **Sabotage**—Some perpetrators are not looking for financial gain. They merely want to cause damage due to a dislike of the organization or for self-gratification. The recent wave of "hacktivism" is one in which the perpetrators make nonviolent

use of illegal or legally ambiguous digital tools in pursuit of political ends.

It is important that the IS auditor know and understand the differences between computer crime and computer abuse to support risk analysis methodologies and related control practices. What constitutes a crime depends on the statistics of the jurisdiction and the extent to which a breach of security is a civil or criminal offense. This brings into play requirements for what the organization needs to do should a crime be suspected, i.e., protection of evidence, reporting of a crime, etc.

Perpetrators in computer crimes are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex. Possible perpetrators include:

- **Hackers (also referred to as crackers)**—Persons with the ability to explore the details of programmable systems and the knowledge to stretch or exploit their capabilities, whether ethical or not. Hackers are typically attempting to test the limits of access restrictions to prove their ability to overcome the obstacles. Some often do not access a computer with the intent of destruction, although this is often the result. Other categories of hackers include "hacktivists" and criminal hackers. Some hackers seek to commit a crime through their actions for some level of personal gain or satisfaction. The terms hack and crack are often used interchangeably.
- **Script kiddies**—Script kiddies refer to individuals who use scripts and programs written by others to perform their intrusions and are often incapable of writing similar scripts on their own.
- **Crackers**—Persons who try to break the security of, and gain access to, someone else's system without being invited to do so
- **Employees (authorized or unauthorized)**—Affiliated with the organization and given system access based on job responsibilities, these individuals can cause significant harm to an organization. Therefore, screening prospective employees through appropriate background checks is an important means of preventing computer crimes within the organization.
- **IS personnel**—These individuals have the easiest access to computerized information, since they are the custodians of this information. In addition to logical access controls, good segregation of duties and supervision help in reducing logical access violations by these individuals.
- **End users**—Personnel who often have broad knowledge of the information within the organization and have easy access to internal resources
- **Former employees**—Be wary of former employees who have left on unfavorable terms, they still may have the access if it was not immediately removed at the time of the employee's termination.
- **Interested or educated outsiders**—These may include:
  - Competitors
  - Terrorists
  - Organized criminals
  - Hackers looking for a challenge
  - Script kiddies for the purpose of curiosity, joyriding and testing their newly acquired tools/scripts and exploits
  - Crackers
  - Phreakers
- **Part-time and temporary personnel**—Remember that office cleaners often have a great deal of physical access and could perpetrate a computer crime.
- **Third parties**—Vendors, visitors, consultants or other third parties who, through projects, gain access to the organization's resources and could perpetrate a crime
- **Accidental ignorant**—Someone who unknowingly perpetrates a violation

Other examples of criminals include small-time crooks, organized crime and state-sponsored criminal activities.

Although collaboration has been improved in solving cyber crimes committed from one country to another, political issues existing between some countries might hinder an investigation. Therefore, additional preventive measures should be taken to protect information systems vulnerable to international attacks.

To better understand how computers are used in or are the target of computer crimes, see **exhibits 5.7** and **5.8** which describe common attack methods and techniques.

Perpetrators may use one or more methods in tandem to commit a crime.

Exhibit 5.7—Computer Crimes

Source of the Attack	Target of the Attack	Examples
Computer is the object of the crime. Perpetrator uses another computer to launch an attack.	Specific identified computer	• Denial of service (DoS) • Hacking
Computer is the subject of the crime. Perpetrator uses computer to commit crime and the target is another computer.	Target may or may not be defined. Perpetrator launches the attack with no specific target in mind.	• Distributed DoS • Virus
Computer is the tool of the crime. Perpetrator uses computer to commit crime but the target is not the computer.	Target is data or information stored on the computer.	• Fraud • Unauthorized access • Phishing • Installing key loggers
Computer symbolizes the crime. Perpetrator lures the user of computers to get confidential information.	Target is user of the computers.	• Social engineering methods: – Phishing – Fake websites – Scam mails – Spam Mails – Fake resumes for employment

Exhibit 5.8—Common Attack Methods and Techniques	
Alteration Attack	Occurs when unauthorized modifications affect the integrity of the data or code Examples: Unauthorized alteration of binary code during the software development life cycle (SDLC) or addition of unauthorized libraries during recompilation of existing programs Cryptographic hash is a primary defense against alteration attacks.
Botnets	Comprise a collection of compromised computers (called zombie computers) running software, usually installed via worms, Trojan horses or back doors Examples: Denial-of-service (DoS) attacks, adware, spyware and spam
Brute-force Attack	Attack launched by an intruder, using many of the password-cracking tools available at little or no cost, on encrypted passwords and attempts to gain unauthorized access to an organization's network or host-based systems
Denial of Service (DoS) Attack	Examples: ICMP flood attack: • Smurf attack—Occurs when misconfigured network devices allow packets to be sent to all hosts on a particular network via the broadcast address of the network • Ping flood—Occurs when the target system is overwhelmed with ping packets • SYN flood—Sends a flood of TCP/SYN packets with forged sender address, causing half-open connections and saturates available connection capacity of the target machine Teardrop attack—Involves sending mangled IP fragments with overlapping, oversized payloads to the target machine Peer-to-peer attack—Causes clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's web site instead. As a result, several thousand computers may aggressively try to connect to a target web site, causing performance degradation. Permanent denial-of-service (PDoS) attack (also known as phlashing)—Damages a system hardware to the extent of replacement Application-level flood attack: • Buffer overflow consumes available memory or CPU time. • Brute force attack—Floods the target with an overwhelming flux of packets, oversaturating its connection bandwidth or depleting the target's system resources • Bandwidth-saturating flood attack—Relies on the attacker having higher bandwidth available than the victim

Exhibit 5.8—Common Attack Methods and Techniques *(cont.)*	
Denial of Service (DoS) Attack *(cont.)*	• Banana attack—Redirects outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets • Pulsing zombie—A DoS attack in which a network is subjected to hostile pinging by different attacker computers over an extended time period. This results in a degraded quality of service and increased workload for the network's resources. Nuke—A DoS attack against computer networks in which fragmented or invalid ICMP packets are sent to the target. Modified ping utility is used to repeatedly send corrupt data, thus slowing down the affected computer to a complete stop. Distributed denial-of-service attack (DDoS)—Occurs when multiple compromised systems flood the bandwidth or resources of the targeted system Reflected attack—Involves sending forged requests to a large number of computers that will reply to the requests. The source IP address is spoofed to that of the targeted victim, causing the replies to flood. Unintentional attack—Web site ends up denied, not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity
Dial-in Penetration Attack, War Dialing	An intruder determines the dial-in phone number ranges from external sources, such as the Internet. The intruder may also employ social engineering tactics to get information from a company receptionist or a knowledgeable employee inside the company
Eavesdropping	An intruder gathers the information flowing through the network with the intent of acquiring and releasing the message contents for either personal analysis or for third parties who might have commissioned such eavesdropping. This is significant when considering that sensitive information, traversing a network, can be seen in real time by all other machines, including e-mail, passwords and, in some cases, keystrokes. These activities can enable the intruder to gain unauthorized access, to fraudulently use information such as credit card accounts and to compromise the confidentiality of sensitive information that could jeopardize or harm an individual's or an organization's reputation.

Exhibit 5.8—Common Attack Methods and Techniques *(cont.)*	
E-mail Bombing and Spamming	Characterized by abusers repeatedly sending an identical e-mail message to a particular address E-mail spamming is a variant of bombing and refers to sending e-mail to hundreds or thousands of users (or to lists that expand to that many users). E-mail spamming can be made worse if recipients reply to the message, causing all of the original addressee to receive the reply. It may also occur innocently as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users or as a result of using a responder message, such as a vacation alert, that is not set up correctly. May be combined with e-mail spoofing, which alters the identity of the account sending the message, making it more difficult to determine from whom the e-mail is coming
E-mail Spoofing	May occur in different forms, but all have a similar result: a user receives an e-mail message that appears to have originated from one source but actually was sent from another source. E-mail spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information such as passwords or account information. Examples of spoofed e-mail that could affect the security of a site include: • E-mail claiming to be from a system administrator and requesting users to change their passwords to a specified string and threatening to suspend their account if they do not make the change • E-mail claiming to be from a person in authority and requesting users to send a copy of a password file or other sensitive information
Flooding	A denial of service (DoS) attack that brings down a network or service by flooding it with large amounts of traffic. The host's memory buffer is filled by flooding it with connections that cannot be completed.
Interrupt Attack	Occurs when a malicious action is performed by invoking the operating system to execute a particular system call Example: A boot sector virus typically issues an interrupt to execute a write to the boot sector.

Exhibit 5.8—Common Attack Methods and Techniques *(cont.)*	
Malicious Codes	Trojan horses (often called Trojans)—Programs that are disguised as useful programs such as operating system patches, software packages or games. Once executed, however, Trojans perform actions that the user did not intend, such as opening certain ports for subsequent access by the intruder. Logic bomb—A program or a section of a program that is triggered when a certain condition, time or event occurs. Logic bombs typically result in sabotage of computer systems and are commonly deployed by disgruntled insiders who have access to programs. For example, when terminated from an organization, a disgruntled software programmer could devise a logical bomb to delete critical files or databases. Logic bombs can also used against attackers. Administrators sometimes intentionally install pseudo flaws, also called honey tokens, that look vulnerable to attack but really act as alarms or triggers of automatic actions when the intruder attempts to exploit the flaw. Trap doors—Commonly called back doors. Bits of code embedded in programs by programmers to quickly gain access during the testing or debugging phase. If an unscrupulous programmer purposely leaves in this code (or simply forgets to remove it), a potential security hole is introduced. Hackers often plant a back door on previously compromised systems to gain subsequent access. Threat Vector Analysis (a type of defense-in-depth architecture), separation of duties and code audits help to defend againstg logic bombs and trap/back doors.
Man-in-the-middle Attack	The following scenarios are possible: • The attacker actively establishes a connection to two devices. The attacker connects to both devices and pretends to each of them to be the other device. Should the attacker's device be required to authenticate itself to one of the devices, it passes the authentication request to the other device and then sends the response back to the first device. Having authenticated himself/herself in this way, the attacker can then interact with the device as he/she wishes. To successfully execute this attack, both devices have to be connectable. • The attacker interferes while the devices are establishing a connection. During this process, the devices have to synchronize the hop sequence that is to be used. The aggressor can prevent this synchronization so that both devices use the same sequence but a different offset within the sequence.

Exhibit 5.8—Common Attack Methods and Techniques *(cont.)*	
Masquerading	An active attack in which the intruder presents an identity other than the original identity. The purpose is to gain access to sensitive data or computing/network resources to which access is not allowed under the original identity. Masquerading also attacks the authentication attribute by letting a genuine session authentication take place and subsequently enters the information flow, masquerading as one of the authenticated users of the session. Impersonation both by people and machines falls under this category. Masquerading by machines (also known as IP spoofing)—A forged IP address is presented. This form of attack is often used as a means of breaking a firewall.
Message Modification	Involves the capturing of a message and making unauthorized changes or deletions (of full streams or parts of the message), changing the sequence or delaying transmission of captured messages. This attack can have disastrous effects if, for example, the messageis an instruction to a bank to make a payment.
Network Analysis	An intruder applies a systematic and methodical approach known as footprinting to create a complete profile of an organization's network security infrastructure. During this initial reconnaissance phase, the intruder uses a combination of tools and techniques to build a repository of information about a particular company's internal network. This probably would include information about system aliases, functions, internal addresses, and potential gateways and firewalls. Next, the intruder focuses on systems within the targeted address space that responded to these network queries. Once a system has been targeted, the intruder scans the system's ports to determine what services and operating system are running on the targeted system, possibly revealing vulnerable services that could be exploited.
Packet Replay	A combination of passive and active modes of attacks. The intruder passively captures a stream of data packets as the stream moves along an unprotected or vulnerable network. These packets are then actively inserted into the network as if the stream were another genuine message stream. This form of attack is effective particularly where the receiving end of the communication channel is automated and will act on receipt and interpretation of information packets without human intervention.
Phishing	Phishing—The criminally fraudulent process of attempting to acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication Spear phishing—A pinpoint attack against a subset of people (users of a web site or product, employees of a company, members of an organization) to undermine that company or organization Phishing techniques include social engineering, link manipulation and web site forgery.

Exhibit 5.8—Common Attack Methods and Techniques *(cont.)*	
Phishing *(cont.)*	Pharming—An attack that aims to redirect the traffic of a web site to a bogus web site. Pharming can be conducted either by changing the host's file on a victim's computer or by exploiting a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses—they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred to as "poisoned." In recent years, both pharming and phishing have been used to steal identity information. Pharming has become a major concern to businesses hosting e-commerce and to online banking web sites. Sophisticated measures known as antipharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming. Social engineering—The human side of breaking into a computer system. Organizations with strong technical security countermeasures (such as authentication processes, firewalls and encryption) may still fail to protect their information systems. This situation may happen if an employee unknowingly gives away confidential information (e.g., passwords and IP addresses) by answering questions over the phone with someone they do not know or replying to an e-mail message from an unknown person. Some examples of social engineering include impersonation through a telephone call, dumpster diving and shoulder surfing. The best means of defense for social engineering is an ongoing security awareness program, wherein all employees and third parties (who have access to the organization's facilities) are educated about the risks involved in falling prey to social engineering attacks.
Piggybacking	The act of following an authorized person through a secured door or electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions. Piggybacking is considered a physical access exposure.
Race Conditions	Also known as Time of Check (TOC)/Time of Use (TOU) attacks.Exploit a small window of time between the time that the security control is applied and the time that the service is used. The exposure to a race condition increases in proportion to the time difference between TOC and TOU. Interference occurs when a device or system attempts to perform two or more operations at the same time, but the nature of the device or system requires the operations to happen in proper sequence. Race conditions occur due to interferences caused by the following conditions: • Sequence or nonatomic—These conditions are caused by untrusted processes, such as those invoked by an attacker, that may get in between the steps of the secure program. • Deadlock, livelock, or locking failure—These conditions are caused by trusted processes running the same program. Since these different processes may have the same privileges, they may interfere with each other, if not properly controlled. Careful programming and good administration practices help to reduce race conditions.

Exhibit 5.8—Common Attack Methods and Techniques *(cont.)*	
Remote Maintenance Tools	If not securely configured and controlled, can be used as an attack method by malicious hackers to remotely gain elevated access and cause damage to the target system
Resource Enumeration and Browsing	When the attacker lists the various resources (names, directories, privileges, shares, policies) on targeted hosts and networks Browsing attack—A form of a resource enumeration attack and is performed by a manual search, frequently aided with commands and tools available in software, operating systems or add-on utilities
Salami	Involves slicing small amounts of money from a computerized transaction or account. Similar to the rounding down technique. The difference between the rounding down technique and the salami technique is that, in rounding down, the program rounds off by the smallest money fraction. For example, in the rounding down technique, a US $1,235,954.39 transaction may be rounded to US $1,235,954.35. On the other hand, the salami technique truncates the last few digits from the transaction amount, so US $1,235,954.39 becomes US $1,235,954.30 or $1,235,954.00, depending on the algorithm/formula built into the program. In fact, other variations of the same technique are applied to rates and percentages.
Spam	Also known as unsolicited commercial e-mail (UCE) or junk e-mail. Usually sent as mass-mailed messages and considered invasive by recipients. • Spam causes inconveniences and has severe impacts on productivity and thus is considered a business risk. • When spam is responded to, the e-mail address of the recipient is validated and gives away information. • Spam is managed using Sender Permitted Form (SPF) protocol and with the help of tools such as Bayesian filtering and greylisting.
Traffic Analysis	An inference attack technique that studies the communication patterns between entities in a system and deduces information. This typically is used when messages are encrypted and eavesdropping would not yield meaningful results. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security.
Unauthorized Access Through the Internet or World Wide Web	Unauthorized access through the Internet or web-based services. Many Internet software packages contain vulnerabilities that render systems subject to attack. Additionally, many of these systems are large and difficult to configure, resulting in a large percentage of unauthorized access incidents. Examples include: • E-mail forgery (simple mail transfer protocol) • Telnet passwords transmitted in the clear (via path between client and server)

Exhibit 5.8—Common Attack Methods and Techniques *(cont.)*	
Unauthorized Access Through the Internet or World Wide Web *(cont.)*	• Altering the binding between IP addresses and domain names to impersonate any type of server. As long as the domain name server (DNS) is vulnerable and used to map universal resource locators (URLs) to sites, there can be no integrity on the Web. • Releasing common gateway interface (CGI) scripts as shareware. CGI scripts often run with privileges that give them complete control of a server. • Client-side execution of scripts (via JAVA in JAVA Applets), which presents the danger of running code from an arbitrary location on a client machine
Viruses, Worms and Spyware	Viruses—Involve the insertion of malicious program code into other executable code that can self-replicate and spread from computer to computer, via sharing of removable computer media, USB removable devices, transfer of logic over telecommunication lines or direct link with an infected machine/code. A virus can harmlessly display cute messages on computer terminals, dangerously erase or alter computer files, or simply fill computer memory with junk to a point where the computer can no longer function. An added danger is that a virus may lie dormant for some time until triggered by a certain event or occurrence, such as a date or being copied a prespecified number of times, during which time the virus has silently been spreading. Worms—Destructive programs that may destroy data or use up tremendous computer and communication resources, but worms do not replicate like viruses. Such programs do not change other programs, but can run independently and travel from machine to machine across network connections by exploiting vulnerability and application/system weaknesses. Worms also may have portions of themselves running on many different machines. Spyware/Malware—Similar to viruses. Examples are keystroke loggers and system analyzers that collect potentially sensitive information, such as credit card numbers, bank details, etc. from the host and then transmit the information to the originator when an online connection is detected.
War Driving	The practice of driving around businesses or residential neighborhoods while scanning with a notebook computer, hacking tool software and sometimes with a global positioning system (GPS) to search for wireless network names. While driving around the vicinity of a wireless network, an attacker might be able to see the wireless network name, but the use of wireless security will determine whether the attacker can do anything beyond viewing the wireless network name. With wireless security enabled and properly configured, war drivers cannot see the network name and are unable to send data, interpret data sent on the wireless network, access the shared resources of the wireless or wired network (shared files, private web sites), or use the Internet connection.

Exhibit 5.8—Common Attack Methods and Techniques *(cont.)*	
War Driving *(cont.)*	Without wireless security enabled and properly configured, war drivers can send data, interpret data sent on the wireless network, access the shared resources of the wireless or wired network (shared files, private web sites), install viruses, modify or destroy confidential data, and use the Internet connection without the knowledge or consent of the owner. For example, a malicious user might use the Internet connection to send thousands of spam e-mail messages or launch attacks against other computers. The malicious traffic could be traced back to the owner's home.
War Walking	Similar to war driving, but a vehicle is not used. The potential hacker walks around the vicinity with a handheld device or a PDA. Currently, there are several free hacking tools that fit in these minidevices.
War Chalking	The practice of marking a series of symbols (outward-facing crescents) on sidewalks and walls to indicate nearby wireless access points. These markings are used to identify hotspots, where other computer users can connect to the Internet wirelessly and at no cost. War chalking was inspired by the practice of unemployed migrant workers, during the Great Depression in the US, using chalk marks to indicate which homes were friendly.

5.2.11 SECURITY INCIDENT HANDLING AND RESPONSE

To minimize damage from security incidents and to recover and to learn from such incidents, a formal incident response capability should be established, and it should include the following phases:
- Planning and preparation
- Detection
- Initiation
- Recording
- Evaluation
- Containment
- Eradication
- Escalation
- Response
- Recovery
- Closure
- Reporting
- Postincident review
- Lessons learned

The organization and management of an incident response capability should be coordinated or centralized with the establishment of key roles and responsibilities. This should include:
- A coordinator who acts as the liaison to business process owners
- A director who oversees the incident response capability
- Managers who manage individual incidents
- Security specialists who detect, investigate, contain and recover from incidents
- Nonsecurity technical specialists who provide assistance based on subject-matter expertise
- Business unit leader liaisons (legal, human resources, public relations, etc.)

In establishing this process, employees and contractors are made aware of procedures for reporting the different types of incidents (e.g., security breach, threat, weakness or malfunction) that might have an impact on the security of organizational assets. They should be required to report any observed or suspected incidents as quickly as possible to the designated point of contact. The organization should establish a formal disciplinary process for dealing with those who commit security breaches such as employees, third parties, etc. To address incidents properly, it is necessary to collect evidence as soon as possible after the occurrence. Legal advice may be needed in the process of evidence collection and protection.

Incidents occur because vulnerabilities are not addressed properly. Incident management processes should include vulnerabilities management practices. A postincident review phase should determine which vulnerabilities were not addressed and why, and input provided for improvement to the policies and procedures implemented to address vulnerabilities. Also, analyzing the cause of incidents may reveal errors in the risk analysis, indicating that the residual risks are higher than the calculated values and inappropriate countermeasures have been taken to reduce inherent risks.

Ideally, an organizational computer security incident response team (CSIRT) or computer emergency response team (CERT) should be formulated with clear lines of reporting, and responsibilities for standby support should be established. Organizational CSIRT will act as an efficient detective and corrective control. Additionally, with its members' participation and involvement in security awareness programs, exercises and workshops, it can demonstrate a preventive control.

Organizational CSIRT should also disseminate security alerts such as recent threats, security guidelines and security updates to the users and assist them in understanding the security risk of errors and omissions. Organizational CSIRT should act as single point of contact for all incidents and issues related to information security, should also respond to abuse reports pertaining to the network of its constituency.

An IS auditor should ensure that the CSIRT is actively involved with users to assist them in the mitigation of risks arising from security failures and also to prevent security incidents. Auditors should also ensure that there is a formal, documented plan and that it contains vulnerabilities identification, reporting and incident response procedures to common, security-related threats/issues, such as:
- Virus outbreak
- Web defacement
- Abuse notification
- Unauthorized access alert from audit trails
- Security attack alerts from intrusion detection systems
- Hardware/software theft
- System root compromises
- Physical security breach
- Spyware/malware/Trojans detected on PCs
- Fake defamatory information in media, including on web sites
- Forensic investigations

Additionally, automated intrusion detection systems should be in place, for example, in networks and platforms, to notify administrators in a real-time manner of a potential incident and define a process for determining the severity of the incidents and the steps to take in high-risk situations.

5.3 LOGICAL ACCESS

As explained in the above paragraphs, logical access controls are the primary means used to manage and protect information assets. Logical access controls enact and substantiate management-designed policies and procedures intended to protect these assets and the controls are designed to reduce risks to a level acceptable to an organization. IS auditors need to understand this relationship. In doing so, IS auditors should be able to analyze and evaluate the effectiveness of a logical access control in accomplishing information security objectives and avoiding losses resulting from exposures. These exposures can result in minor inconveniences to a total shutdown of computer functions.

5.3.1 LOGICAL ACCESS EXPOSURES

Technical exposures are one type of exposure that exist from accidental or intentional exploitation of logical access control weaknesses. Intentional exploitation of technical exposures might lead to computer crime. However, all computer crimes do not exploit technical exposures.

Technical exposures are the unauthorized (intentional or unintentional) activities interfering with normal processing, such as implementation or modification of data and software, locking or misusing user services, destroying data, compromising system usability, distracting processing resources, or spying data flow or users activities at either the network, platform (operating system), database or application level. Technical exposures include:

- **Data leakage**—Involves siphoning or leaking information out of the computer. This can involve dumping files to paper, or can be as simple as stealing computer reports and tapes. Unlike product leakage, data leakage leaves the original copy, so it may go undetected.
- **Wire tapping**—Involves eavesdropping on information being transmitted over telecommunications lines
- **Computer shutdown**—Initiated through terminals or personal computers connected directly (online) or remotely (dial-up lines) to the computer. Only individuals who know a high-level logon ID usually can initiate the shutdown process, but this security measure is effective only if proper security access controls are in place for the high-level logon ID and the telecommunications connections into the computer. Some systems have proven to be vulnerable to shutting themselves down under certain conditions of overload.

The following attacks are described in **exhibit 5.8**

- Trojan horses/back doors
- Viruses
- Worms
- Spyware
- Malware
- Logic bombs
- Denial of service (DoS)
- War driving
- Trap doors
- Race conditions
- Salami

5.3.2 FAMILIARIZATION WITH THE ORGANIZATION'S IT ENVIRONMENT

For IS auditors to effectively assess logical access controls within their organization, they first need to gain a technical and organizational understanding of the organization's IT environment. The purpose of this is to determine which areas from a risk standpoint warrant IS auditing attention in planning current and future work. This includes reviewing the network, OS platform, database and application security layers associated with the organization's IT information systems architecture.

5.3.3 PATHS OF LOGICAL ACCESS

Access or points of entry to an organization's IS infrastructure can be gained through several avenues. Each avenue is subject to appropriate levels of access security.

Sometimes these paths are direct, as is the case for a PC terminal user tying directly into a mainframe. This happens when the IS environment is under direct control of the main system and when the users are locally known individuals, with well-defined access profiles. More complex is the case of a LAN, where many specific IS resources are tied to a common linking structure. The LAN resources may have different access paths/levels, normally mediated through LAN connectivity, and the network itself is considered an important IS resource at a higher access level. In today's environment it is most common to find a combination of direct/local network/remote access paths. Complexity is increased by a number of intermediate devices that act as "security doors" among the various environments and by the need of crossing low-security or totally open IT spaces such as the Internet. A frequent example of access path through common nodes is either a back-end or front-end interconnected network of systems for internally or externally based users. Front-end systems are network-based systems connecting an organization to outside, untrusted networks, such as corporate web sites, where a customer can access the web site externally to initiate transactions that connect to a proxy server application which in turn connects, for example, to a back-end database system to update a customer database. Front-end systems can also be internally based to automate business, paperless processes that tie into back-end systems in a similar manner.

General Points of Entry

General points of entry to either front-end or back-end systems control the accesses from an organization's networking or telecommunications infrastructure into their information resources (e.g., applications, databases, facilities, networks). The approach followed is based on a client-server model. A large organization can have thousands of interconnected network servers. Connectivity in this environment needs to be controlled through a smaller set of primary domain controllers (servers), which enable a user to obtain access to specific secondary points of entry (e.g., application servers, databases, etc.).

General modes of access into this infrastructure occur through the following:

- **Network connectivity**—Access is gained by linking a PC to a segment of an organizations' network infrastructure, either through a physical or a wireless connection. At a minimum, such access requires user identification and authentication to a domain-controlling server. More specific access to a particular application or database may also require the users to identify and authenticate themselves to that particular server (secondary point of entry). Other modes of access into the infrastructure can also occur through network management devices, such as routers and firewalls, which should be strictly controlled.
- **Remote access**—A user dials in remotely to an organization's server, which generally requires the user to identify and authenticate him/herself to the server for access to specific functions that can be performed remotely (e.g., e-mail, File Transfer Protocol [FTP], Internet or some application-specific function). Complete access to view all network resources usually requires a virtual private network (VPN), which allows a secure authentication and connection into those resources where privileges have been granted. Remote access points of entry can be extensive and should be centrally controlled where possible.

From a security standpoint, it is incumbent upon the organization to know all of the points of entry into its information resource infrastructure which, in many organizations, will not be a trivial task (e.g., thousands of remote access users). This is significant because any point of entry not appropriately controlled can potentially compromise the security of an organization's sensitive and critical information resources. IS auditors, in performing detailed network assessments and access control reviews, should determine whether all points of entry are known and should support management's effort in obtaining the resources to identify and manage all access paths.

5.3.4 LOGICAL ACCESS CONTROL SOFTWARE

Information technology has made it possible for computer systems to store and contain large quantities of sensitive data, increase the capability of sharing resources from one system to another, and permit many users to access the system through Internet/intranet technologies. All of these factors have made organizations' IS resources more widely and promptly accessible and available.

To protect an organization's information resources, access control software has become even more critical in assuring the confidentiality, integrity and availability of information resources. The purpose of access control software is to prevent the unauthorized access and modification to an organization's sensitive data and the use of system critical functions.

To achieve this kind of control, it is necessary to apply access controls across all layers of an organization's IS architecture, including networks, platforms or operating system, databases, and application systems. Each of them usually features some form of identification and authentication, access authorization, checking of specific information resources, and logging and reporting of user activities.

The greatest degree of protection in applying access control software against internal and external users' unauthorized access is at the network and platform/operating system levels. These systems are also referred to as general support systems, and they make up the primary infrastructure on which applications and database systems will reside.

Operating system access control software interfaces with network access control software and resides on network layer devices (e.g., routers, firewalls) that manage and control external access to organizations' networks. Additionally, operating system access control software interfaces with database and/or application systems access controls to protect system libraries and user data sets.

General operating and/or application systems access control functions include the following:

- Create or change user profiles
- Assign user identification and authentication
- Apply user logon limitation rules
- Notification concerning proper use and access prior to initial login
- Create individual accountability and auditability by logging user activities
- Establish rules for access to specific information resources (e.g., system-level application resources and data)
- Log events
- Report capabilities

Database and/or application-level access control functions include the following:

- Create or change data files and database profiles
- Verify user authorization at the application and transaction level
- Verify user authorization within the application
- Verify user authorization at the field level for changes within a database
- Verify subsystem authorization for the user at the file level
- Log database/data communications access activities for monitoring access violations

In summary, access control software is provided at different levels within an IS architecture, where each level provides a certain degree of security. Properties of such relationships are that lower layers (applications, databases) are dependent on upper, infrastructure-type layers to protect general system resources. Lower layers provide the granularity needed at the application level in segregating duties by function.

5.3.5 IDENTIFICATION AND AUTHENTICATION

Identification and authentication (I&A) in logical access control software is the process of establishing and proving one's identity. It is the process by which the system obtains from a user his/her claimed identity and the credentials needed to authenticate this identity, and validates both pieces of information.

I&A is a critical building block of computer security since it is needed for most types of access control and is necessary for establishing user accountability. User accountability requires the linking of activities on a computer system to specific individuals and, therefore, requires the system to identify users. For most systems, I&A is the first line of defense because it prevents

unauthorized people (or unauthorized processes) from entering a computer system or accessing an information asset. If users are not properly identified and authenticated, particularly in today's open-system-networked environments, organizations have a higher exposure to risk of unauthorized access.

Some of I&A's more common vulnerabilities that may be exploited to gain unauthorized system access include:
- Weak authentication methods
- The potential for users to bypass the authentication mechanism
- The lack of confidentiality and integrity for the stored authentication information
- The lack of encryption for authentication and protection of information transmitted over a network
- The user's lack of knowledge on the risks associated with sharing authentication elements (e.g., passwords, security tokens)

Authentication is typically categorized as "something you know" (e.g., password), "something you have" (e.g., token card) and "something you are (or do)" (a biometric feature). These techniques can be used independently or in combination to authenticate and identify a user. For example, a single-factor technique (something you know) involves the use of the traditional logon ID and password. Something you know, such as a pin number, combined and associated with something you have, such as a token card, is known as a two-factor authentication technique. Something you are is a biometric authentication technique, such as a palm or iris biometric scan. Each of these techniques is described in detail in the following sections.

A combination of more than one method, such as token and password (or personal identification number [PIN] or token and biometric device, is referred to as "multifactor" authentication.

Identification and authentication are separate systems. They differ in respect to:
- Meaning
- Methods, peripherals and techniques supporting them
- Requirements in terms of secrecy and management
- Attributes—authentication does not have attributes in itself, while an identity may have a defined validity in time and other information attached to it.
- The fact that identity does not normally change, while authentication tokens bound to secrecy must be regularly replaced to preserve their reliability

Logon IDs and Passwords

Logon IDs and passwords are the components of a user identification and authentication process, where the authentication is based on something you know. The computer can maintain an internal list of valid logon IDs and a corresponding set of access rules for each logon ID. These access rules are related to the computer resources. As a minimum requirement, access rules are usually specified at the operating system level (controlling access to files) or within individual application systems (controlling access to menu functions and types of data or transactions).

The logon ID should be restricted to provide individual, but not group identification. If a group of users is to be formed for interchangeability, the system usually offers the ability to attach a logon ID to a named group, with common rights. Each user gets a unique logon ID that can be identified by the system. The format of logon IDs is typically standardized.

The password provides individual authentication.

FEATURES OF PASSWORDS

A password should be easy for the user to remember, but difficult for an intruder to determine.

Initial passwords may be allocated by the security administrator or generated by the system itself. When the user logs on for the first time, the system should force a password change to improve confidentiality. Initial password assignments should be randomly generated. The ID and password should be communicated in a controlled manner to ensure that only the appropriate user receives this information. New accounts without an initial password assignment should be suspended.

If the wrong password is entered a predefined number of times, typically three, the logon ID should be automatically locked out. Locking-out may be made permanent (only the administrator may unlock the ID) or temporary (the system automatically unlocks the ID after a prespecified time period).

Users that have forgotten their password must notify the security administrator. This is the only person with sufficient privileges to reset the password and, in case this is necessary, to unlock the logon ID. The security administrator should reactivate the logon ID only after verifying the user's identification (challenge/response system), much like a bank verifies an account holder's ID before giving information over the phone (such as mother's maiden name). To verify, the security administrator should return the user's call after verifying his/her extension or calling his/her supervisor for verification.

Passwords should be one-way encrypted internally to the computer, using a sufficiently strong algorithm. This allows checking passwords without the need of recording them explicitly. To reduce the risk of an intruder gaining access to other users' logon IDs, passwords should not be displayed in any form. Passwords are normally masked on a computer screen, and they are not shown on computer reports. Passwords should not be kept on index or card files, or written on pieces of paper taped somewhere near the terminal or inside a person's desk. These are the first places a potential intruder will look.

Passwords should be changed periodically. On a regular basis (for example, every 30 days), the user should change his/her password. The frequency of changing the password should depend upon the criticality of the information access level, the nature of the organization, the IS architecture and technologies used, etc. Passwords should be changed by the user at his/her terminal/workstation, rather than at the administrator's terminal or in any location where their new password might be observed. The best method is to force the change by notifying the user prior to the password expiration date. The risk of allowing voluntary password changes is that, generally, users will not change their passwords unless forced to do so. Password management is

stronger if a history of previously used passwords is maintained by the system and their re-use prohibited for a period, such as no re-use of the last 12 passwords.

Passwords must be unique to an individual; if a password is known to more than one person, the accountability of the user for all activity within the account cannot be enforced.

Special treatment should be applied to supervisor or administrator accounts. These accounts allow full access to the system. Normally there are a limited number of such accounts per system/authentication level. For accountability, the administrator password should be known only by one individual. On the other hand, the organization should be able to access the system in an emergency situation when the administrator is not available. To enable this, practices such as keeping the administrator password in a sealed envelope, kept in a locked cabinet and available only to top managers, should be implemented. This is sometimes referred to as a "firecall" ID.

All of the guidelines above should be formalized in a password policy and made as a mandatory requirement. An "acceptable use" policy should also include the requirement to follow the policy.

IDENTIFICATION AND AUTHENTICATION BEST PRACTICES

Logon ID requirements include:

- Logon ID syntax should follow an internal naming rule, however this rule should be kept as confidential as the IDs themselves.
- Default system accounts, such as Guest, Administrator and Admin, should be renamed whenever technically possible.
- Logon IDs not used after a predetermined period of time should be deactivated to prevent possible misuse. This can be done automatically by the system or manually by the security administrator.
- The system should automatically disconnect a logon session if no activity has occurred for a period of time. This reduces the risk of misuse of an active logon session left unattended, because the user went to lunch, left for home, went to a meeting or otherwise forgot to log off. This is often referred to as a session time out. Regaining access should require the reentry of the authentication method, password, token etc.

The password syntax rules include:

- Ideally, passwords should be a minimum of eight characters in length. The length of the password will, at times, depend on the capability of the system being used. A passphrase is generally accepted as a more secure password.
- Passwords should require a combination of at least three of the following characteristics: alpha, numeric, upper and lower case, and special characters.
- Passwords should not be particularly identifiable with the user (such as first name, last name, spouse name, pet's name, etc.). Some organizations prohibit the use of vowels, making word association/guessing of passwords more difficult.
- The system should enforce regular password changes every 30 days and not permit previous password(s) to be used for at least a year after being changed.

At a minimum, the above rules should be applied to individuals with privileged system account authority (system administrators, security administrators, etc.) vs. general users. Users with privileged authority need such access in establishing and managing appropriate system configurations. However, such privileges enable the user to bypass any access control software restrictions that may exist on the system. The general rule to apply is that, the greater the degree of sensitivity of the access rights, the stricter the access controls should be.

Token Devices, One-time Passwords

In a common two-factor authentication technique, the user is assigned a microprocessor-controlled smart card or a USB key, synchronized with a specific authentication device on the system. This smart card/key is set to generate unique, time-dependent, pseudo-random strings that are called "session passwords" and are recognized by the authenticating device and program. They attest that the caller is currently in possession of his/her own smart device. Each string is valid for only one logon session. Users must either physically read out and retype the string, or insert the smart card/USB key in a reader/USB slot along with typing in their own memorized password to gain access to the system. This technique involves something you have (a device subject to theft) and something you know (a personal identification number).

Biometrics

Biometric access controls are the best means of authenticating a user's identity based on a unique, measurable attribute or trait for verifying the identity of a human being. This control restricts computer access based on a physical (something you are) or behavioral (something you do) characteristic of the user. Traditionally, biometric systems have been used very little as an access control technique. However, due to advances in hardware efficiencies and storage, biometric systems are becoming a more viable option as an access control mechanism.

Using a biometric generally involves use of a reader device that interprets the individual's biometric features before permitting authorized access. However, this is not a flawless process because certain biometric features can change (e.g., scarred fingerprints, signature irregularities and change in voice). For this reason, biometric access control systems are not all equally effective and easy to use.

Entering a user's biometric into a system occurs through an enrollment process by storing a user's particular biometric feature. This occurs through an iterative averaging process of acquiring a physical or behavioral sample, extracting unique data from the sample (converted into a mathematical code), creating an initial template, comparing new sample(s) with what has been stored and developing a final template that can be used to authenticate the user. Subsequent samples will be used in determining whether a match or nonmatch condition exists for granting access.

Performance of biometric control devices is determined through three quantitative measures (percentage based) to rank the level of matching accuracy. One type, the false-rejection rate (FRR), or type-I error rate, is the number of times an individual granted authority to use the system is falsely rejected by the system. An

aggregate measure of type-I error rates is the failure-to-enroll rate (FER), the proportion of people who fail to be enrolled successfully. The other, referred to as the false-acceptance rate (FAR), or type-II error rate, is the number of times an individual not granted authority to use a system is falsely accepted by the system. Each biometric system may be adjusted to lower FRR or FAR, but as a general rule when one decreases, the other increases (and *vice versa*), and there is an adjustment point where the two errors are equal. An overall metric related to the two error types is the equal error rate (EER), which is the percent showing when false rejection and acceptance are equal. The lower the overall measure, the more effective the biometric.

Generally, the ordering of biometric devices with the best response times and lowest EERs are palm, hand, iris, retina, fingerprint and voice, respectively.

An analysis of each physically oriented biometric is shown below:

1. **Palm**—Analyzes physical characteristics associated with the palm such as ridges and valleys found on the palm. Use of this biometric entails placing the hand on a scanner where physical characteristics are captured.
2. **Hand geometry**—As one of the oldest biometric techniques, hand geometry is concerned with measuring the physical characteristics of the users' hands and fingers from a three-dimensional perspective. The user places his hand, palm-down, on a metal surface with five guidance pegs to ensure that fingers are placed properly and in the correct hand position. The template is built from measurements of physical geometric characteristics of a person's hand (usually 90 measurements) for example, length, width, thickness and surface area.

   Advantages of these systems are the social acceptance that they have received as well as the very little computer storage space that is required for the template, generally 10-20 bytes. The main disadvantage compared to other biometrics methods is the lack of uniqueness of hand geometry data. Moreover, an injury to the hand may cause the measurements to change, resulting in recognition problems.
3. **Iris**—An iris, which has patterns associated with the colored portions surrounding the pupils, is unique for every individual and, therefore, a viable method for user identification. To capture this information, the user is asked to center his/her eye onto a device by seeing the reflection of their iris in the device. Upon this alignment occurring, a camera takes a picture of the user's iris and compares it with a stored image. The iris is stable over time, having over 400 characteristics, although only approximately 260 of these are used to generate the template. As is the case with fingerprint scanning, the template carries less information than a high-quality image.

   The key advantage to iris identification is that contact with the device is not needed, which contrasts with other forms of identification such as fingerprint and retinal scans. Disadvantages of iris recognition are the high cost of the system, as compared to other biometric technologies, and the high amount of storage requirements needed to uniquely identify a user.
4. **Retina**—Retina scan uses optical technology to map the capillary pattern of the eye's retina. The user has to put his eye within 0.4 to 0.8 inches (1-2 centimeters) of the reader while an image of the pupil is taken. The patterns of the retina are measured at over 400 points to generate a 96-byte template. Retinal scan is extremely reliable, and it has the lowest false-acceptance rate among the current biometric methods. Disadvantages of retinal scanning include the need for fairly close physical contact with the scanning device, which impairs user acceptance, and the high cost.
5. **Fingerprint**—This access control method is commonly used; the user places his/her finger on an optical device or silicon surface to get his/her fingerprint scanned. The template generated for the fingerprint, named "minutiae," measures bifurcations, divergences, enclosures, endings and valleys in the ridge pattern. It contains only specific data about the fingerprint (the minutiae), not the whole image of the fingerprint itself. Additionally, the full fingerprint cannot be reconstructed from the template. Depending on the provider, the fingerprint template may use between 250 bytes to more than 1,000 bytes. More storage space implies lower error rates. Fingerprint characteristics are described by a set of numeric values. While the user puts the finger in place for between two and three seconds, a typical image containing between 30 and 40 finger details is obtained and an automated comparison to the user's template takes place.

   Advantages of fingerprint scanning are low cost, small size of the device, ability to physically interface into existing client-server-based systems, and ease of integration into existing access control methods. Disadvantages include the need for physical contact with the device and the possibility of poor-quality images due to residues, such as dirt and body oils, on the finger. Additionally, fingerprint biometrics are not as effective as other techniques.
6. **Face**—In this method, the biometric reader processes an image captured by a video camera, which is usually within 24 inches (60 cm) of the human face, isolating it from the other objects captured within the image. The reader analyzes images captured for general facial characteristics. The template created is based on either generating two- or three-dimensional mapping arrays or by combining facial-metric measurements of the distance between specific facial features, such as the eyes, nose and mouth. Some vendors also include thermal imaging in the template.

   The face is considered to be one of the most natural and most "friendly" biometrics, and it is acceptable to users because it is fast and easy to use. The main disadvantage of face recognition is the lack of uniqueness, which means that people who look alike may fool the device. Moreover, some systems cannot maintain high levels of performance as the database grows in size.

An analysis of each behavior-oriented biometric is shown below:

1. **Signature recognition**—Also referred to as signature dynamics, the information from the reader is used to analyze two different areas of an individual's signature: the specific features of the signature and the specific features of the signing process. It includes speed, pen pressure, directions, stroke length and the points in time when the pen is lifted from the paper. Advantages of this method are that it is fast, easy to use and has a low implementation cost. Other advantages are that even

though a person might be able to duplicate the visual image of someone else's signature, it is difficult if not impossible to duplicate the dynamics (e.g., time duration in signing, pen-pressure, how often pen leaves signing block, etc.).

The main disadvantage is capturing the uniqueness of a signature particularly when a user does not sign his/her name in a consistent manner. For example this may occur due to illness/disease or use of initials versus a complete signature. Additionally, users' signing behavior may change when signing onto signature identification and authentication "tablets" versus writing the signature in ink onto a piece of paper.

2. **Voice recognition**—Voice recognition involves taking the acoustic signal of a person's voice, saying a "passphrase," and converting it to a unique digital code that can then be stored in a template (approximately 1,500-3,000 bytes). Voice recognition incorporates several variables or parameters to recognize one's voice/speech pattern including pitch, dynamics and waveform.

   The main attraction of this method is that it can be used for telephone applications, where it can be deployed with no additional user hardware costs. It also has a high rate of acceptance among users.

   Disadvantages of this method include:
   - The large volume of storage requirements
   - Changes to people's voices
   - The possibility of misspoken phrases
   - A clandestine recording of the user's voice saying the passphrase could be made and played back to gain access.
   - Background noises can interfere with the system.

MANAGEMENT OF BIOMETRICS

Management of biometrics should address effective security for the collection, distribution and processing of biometric data, encompassing:

- Data integrity, authenticity and nonrepudiation
- Management of biometric data across its life cycle—comprised of the enrollment, transmission and storage, verification, identification, and termination processes
- Usage of biometric technology, including one-to-one and one-to-many matching, for the identification and authentication of its users
- Application of biometric technology for internal and external, as well as logical and physical, access control
- Encapsulation of biometric data
- Techniques for the secure transmission and storage of biometric data
- Security of the physical hardware used throughout the biometric data life cycle
- Techniques for integrity and privacy protection of biometric data

Management should develop and approve a biometric information management and security (BIMS) policy. The auditor should use the BIMS policy to gain a better understanding of the biometric systems in use. With respect to testing, the auditor should make sure this policy has been developed and the biometric information is being secured appropriately.

As is the case with any critical information system, logical and physical controls including business continuity plans should address this area.

Life cycle controls for the development of biometric solutions should be in place to cover the enrollment request, the template creation and storage, and the verification and identification procedures. The identification and authentication procedures for individual enrollment and template creation should be specified in the BIMS policy. Management needs to have controls in place to ensure that these procedures are being followed in accordance with this policy. If the biometric device malfunctions or is inoperable, backup authentication methods should also be developed. Controls should also be in place to protect the sample data as well as the template from modification during transmission.

Single Sign-on

Users normally require access to a number of resources during the course of their daily routine. For example, users would first log into an operating system and thereafter into various applications. For each OS application or other resource in use, users are required to provide a separate set of credentials to gain access. This results in a situation where users' ability to remember passwords is significantly reduced. This also increases the chance that users will write them down on or near their workstation or area of work, and thereby increase the risks that a security breach within the organization may occur.

To address this situation, the concept of single sign-on (SSO) was developed. SSO can generally be defined as the process for consolidating all organization platform-based administration, authentication and authorization functions into a single centralized administrative function. This function would provide the appropriate interfaces to the organization's information resources, which may include:

- Client-server and distributed systems
- Mainframe systems
- Network security including remote access mechanisms

The SSO process begins with the first instance where the user credentials are introduced into the organization's IT computing environment. The information resource or SSO server handling this function is referred to as the primary domain. Every other information resource, application or platform that uses those credentials is called a secondary domain.

The challenges in managing diverse platforms through single sign-on principally involve overcoming the heterogeneous nature of diverse networks, platforms, databases and applications often found in organizations when establishing a set of credentials acceptable to all of these information resources. To effectively integrate into the SSO process, SSO administrators need to obtain an understanding of how each system manages credentialing information, access control list (ACL) authorization rules, and audit logs and reports. Requirements developed in this regard should be based on security domain policies and procedures.

SSO advantages include:

- Multiple passwords are no longer required; therefore, a user may be more inclined and motivated to select a stronger password.

- It improves an administrator's ability to manage users' accounts and authorizations to all associated systems.
- It reduces administrative overhead in resetting forgotten passwords over multiple platforms and applications.
- It reduces the time taken by users to log into multiple applications and platforms.

SSO disadvantages include:
- Support for all major operating system environments is difficult. SSO implementations will often require a number of solutions integrated into a total solution for an enterprise's IT architecture.
- The costs associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary.
- The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information assets. For this reason, "strong authentication" in the form of complex password requirements and the use of biometrics is frequently implemented.

One example of SSO is Kerberos. Created by the Massachusetts Institute of Technology (USA) through its Project Athena in the 1980s, it is an authentication service used to validate services and users in a distributed computing environment (DCE). The role of the authentication service is to allow principals to positively identify themselves and participate in a DCE. Both users and servers authenticate themselves in a DCE environment, unlike security in most other client-server systems where only users are authenticated. There are two distinct steps to authentication. At initial logon time, the Kerberos third-party protocol is used within DCE to verify the identity of a client requesting to participate in a DCE network. This process results in the client obtaining credentials initially registered with the trusted third party and cryptographically protected. These credentials form the basis for setting up secure sessions with DCE servers when the user tries to access resources.

5.3.6 AUTHORIZATION ISSUES

The authorization process used for access control requires that the system be able to identify and differentiate among users.

Access rules (authorization) specify who can access what. For example, access control is often based on least privilege, which refers to the granting to users of only those accesses required to perform their duties. Access should be on a documented need-to-know and need-to-do basis by type of access.

Computer access can be set for various levels, i.e., files, tables, data items etc. When IS auditors review computer accessibility, they need to know what can be done with the access and what is restricted. For example, access restrictions at the file level generally include the following:
- Read, inquiry or copy only
- Write, create, update or delete only
- Execute only
- A combination of the above

The least dangerous type of access is read only, as long as the information being accessed is not sensitive or confidential. This is because the user cannot alter or use the computerized file beyond basic viewing or printing.

The following is a list of computerized files and facilities generally applicable across security layers for networks, platforms, databases and applications that should be protected by logical access controls:
- Data
- Data dictionary/directory
- Telecommunications lines and dial-up lines
- Operating systems for network routers and switches
- Domain name servers
- System software
- Libraries/directories
- Application software (test and production)
- Web applications (public or private intranet-based)
- System procedure libraries
- System utilities
- Operator system exits
- Access control software
- Passwords
- Logging files
- Temporary disk files
- Tape files
- Bypass label processing feature
- Spool queues

Access Control Lists

To provide security authorizations for the files and facilities listed previously, logical access control mechanisms utilize access authorization tables, also referred to as access control lists (ACLs) or access control tables. ACLs refer to a register of:
- Users (including groups, machines, processes) who have permission to use a particular system resource
- The types of access permitted

ACLs vary considerably in their capability and flexibility. Some only allow specifications for certain preset groups (e.g., owner, group and world), while more advanced ACLs allow much more flexibility such as user-defined groups. Also, more advanced ACLs can be used to explicitly deny access to a particular individual or group. With more advanced ACLs, access can be at the discretion of the policy maker (and implemented by the security administrator) or individual user, depending upon how the controls are technically implemented. When a user changes job roles within an organization, often their old access rights are not removed before adding their new required accesses. Without removing the old access rights, there could be a potential segregation of duties issue.

Logical Access Security Administration

In today's client-server environment, the access identification and authentication, and the authorization process, can be administered either through a centralized or decentralized environment. The advantages of conducting security in a decentralized environment are:
- The security administration is onsite at the distributed location.
- Security issues are resolved in a timely manner.
- Security controls are monitored on a more frequent basis.

The risks associated with distributed responsibility for security administration include:
- The possibility that local standards might be implemented rather than those required by the organization
- Levels of security management might be below what can be maintained by a central administration.
- Unavailability of management checks and audits that are often provided by central administration to ensure that standards are maintained

There are many ways to control remote and distributed sites:
- Software controls over access to the computer, data files and remote access to the network should be implemented.
- The physical control environment should be as secure as possible, with additions such as lockable terminals and a locked computer room.
- Access from remote locations via modems and laptops to other microcomputers should be controlled appropriately.
- Opportunities for unauthorized people to gain knowledge of the system should be limited by implementing controls over access to system documentation and manuals.
- Controls should exist for data transmitted from remote locations such as sales in one location that update accounts receivable files at another location. The sending location should transmit control information, such as transaction control totals, to enable the receiving location to verify the update of its files. When practical, central monitoring should ensure that all remotely processed data have been received completely and updated accurately.
- When replicated files exist at multiple locations, controls should ensure that all files used are correct and current and, when data are used to produce financial information, that no duplication arises.

Remote Access Security

Today's organizations require remote access connectivity to their information resources for different types of users, such as employees, vendors, consultants, business partners and customer representatives. In providing this capability, a variety of methods and procedures are available to satisfy an organization's business need for this level of access.

Remote access users can connect to their organization's networks with the same level of functionality that exists within their office. In doing so, the remote access design uses the same network standards and protocols applicable to the systems that they are accessing, Transmission Control Protocol/Internet Protocol (TCP/IP)-based systems and systems network architecture (SNA) systems, for the mainframe where the user uses terminal emulation software to connect to a mainframe-based legacy application. Support for these connections includes asynchronous point-to-point modem connectivity, integrated services digital network (ISDN) dial-on-demand connectivity, and dedicated lines (e.g., frame relay and digital subscriber lines [DSL]).

A viable option gaining increased use is TCP/IP Internet-based remote access. This access method is a cost-effective, "inexpensive" approach that enables organizations to take advantage of the public network infrastructures and connectivity options available, under which ISPs manage modems and dial-in servers, and DSL and cable modems reduce costs further to an organization. To effectively use this option, organizations establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Available VPN technologies apply the Internet Engineering Task Force (IETF) IPSec security standard (see encryption section 5.4.5 in this chapter for more details on IPSec). Advantages are their ubiquity, ease of use, inexpensive connectivity, and read, inquiry or copy only access. Disadvantages include that they are significantly less reliable than dedicated circuits, lack a central authority, and can be difficult to troubleshoot.

Organizations should be aware that using VPNs to allow remote access to their systems can create holes in their security infrastructure. The encrypted traffic can hide unauthorized actions or malicious software that can be transmitted through such channels. Intrusion detection systems and virus scanners able to decrypt the traffic for analysis and then encrypt and forward it to the VPN endpoint should be considered as preventive controls. A good practice will terminate all VPNs to the same end-point in a so called VPN concentrator, and will not accept VPNs directed at other parts of the network.

COMMON CONNECTIVITY METHODS

In connecting to an organization's network, a common method is to use dial-up lines (modem asynchronous point-to-point or ISDN) in accessing an organization's network access server (NAS) that works in concert with an organization's network firewall and router configuration. The NAS handles user authentication, access control and accounting, while maintaining connectivity. The most common protocol for doing this is the Remote Access Dial-in User Service (RADIUS) and Terminal Access Control Access (TACACS). In a typical NAS implementation, calls into the network are received, and as a good security practice, the call is terminated after recording the calling number and performing preliminary authentication procedures. The standard security practice has been for the NAS to initiate a call back to a predetermined number of the user. This control can be circumvented through effective implementation of call-forwarding mechanisms.

Dial-up connectivity, not based on centralized control and least preferred from a security and control standpoint, is an organization's server whose operating system is set up to accept remote access, which is referred to as a remote access server (RAS). The latter approach is not recommended, as it is extremely difficult to control remote access from many servers using its own RAS capability.

Advantages of dial-up connectivity are its low end-user costs (local phone calls) and that it is intuitive and easy to use (familiarity). Disadvantages are related to performance; for example, reliability in establishing connections with the NAS (phone networks' electrical interference) and time-sensitive media-rich applications or a service's failure when data-rate throughput is low.

Another common connectivity method often used for remote access is dedicated network connections. Using private, often proprietary, network circuits is the approach generally considered

the safest because the only network traffic carried belongs to the same organization. It is commonly used by branch/regional offices or with business partners.

Advantages of dedicated network connections include greater performance gains in data throughput and reliability, and data on a dedicated link belonging to the subscribing organization, where an intruder would have to compromise the telecommunications provider itself to access the data link. A disadvantage is that cost is typically two- to five-times higher than connections to the Internet.

Remote access risks include:
- Denial of service where remote users may not be able to gain access to data or applications that are vital for them to carry out their day-to-day business
- Malicious third parties, who may gain access to critical applications or sensitive data by exploiting weaknesses in communications software and network protocols
- Misconfigured communications software, which may result in unauthorized access or modification of an organization's information resources
- Misconfigured devices on the corporate computing infrastructure
- Host systems not secured appropriately, which could be exploited by an intruder gaining access remotely
- Physical security issues over remote users' computers

Remote access controls include:
- Policy and standards
- Proper authorizations
- Identification and authentication mechanisms
- Encryption tools and techniques such as use of a VPN
- System and network management

Remote Access Using PDAs

The use of PDAs is widespread and they often augment desktop and laptop PCs within many organizations due to ease of use and functionality. Connectivity options for PDAs have significantly expanded. Those now being marketed include wireless connectivity and integrated telephone and camera features. Use of these devices often includes access to sensitive or confidential business information. Consequently, risks to the organization have increased due to the inherent lack of security of PDAs (e.g., easy to steal or lose due to their small size). Also, if a PDA is connected or synchronized without the appropriate controls being put in place, there is the potential for unauthorized access to the organization's infrastructure.

The level of controls implemented to protect PDAs must, therefore, be consistent with the nature of the information that is stored and/or processed. It is important that organizations set appropriate policies and procedures, and individuals are made fully aware of their responsibilities regarding use of PDAs for business purposes. Control issues to address include the following:
- **Compliance**—PDAs should comply with the security requirements as defined in corporate standards. Existing policies that define computing resources should be expanded to include PDAs in addition to standard workstations and laptops.
- **Approval**—PDA use should be appropriately authorized and approved in accordance with the organization's policies and procedures.
- **Standard PDA applications**—Configuration and use of the PDA should be baselined and controlled.
- **Due care**—Employees should exercise due care within office environments and especially during travel. Any loss or theft of a PDA must be treated as a security breach and reported immediately in accordance to security management policies and procedures.
- **Awareness training**—Employee orientation and security awareness training should include coverage of PDA policy and guidelines. The training will allow propagation of awareness that PDAs are important business tools when used properly and have risks associated with them, if not managed accordingly.
- **PDA applications**—Only applications that either meet with the corporate security architecture or are delivered as standard on the PDA should be authorized for use, and all software applications must be appropriately licensed and installed by the organization's IS support team.
- **Synchronization**—PDAs should be backed up and updated. PDA information should be synchronized only with the organization's resources contained on both laptops and desktop PCs. Remote access to the organization's infrastructure must be made only via an approved route where multiple methods of synchronization are available. Generally, the only methods that should be approved and supported are a direct connection to a workstation (via cable or infrared link) and dial-in access via an approved, secure remote access service. Additionally, when the PDA is connected to the organization's infrastructure, it must not have additional communication sessions running. For example, dial-up connections must be blocked when the PDA is synchronizing directly with the LAN. This may also include users authentication to the PDA and the workstation prior to synchronization. The synchronization process must log all actions performed during synchronization and report any irregularities.
- **Encryption**—PDAs used to store sensitive or confidential information should be encrypted in accordance with the organization's information security policies, mandating use of a strong encryption mechanism. The encryption standard should be established by the organization's IT function in establishing a standard baseline.
- **Virus detection and control**—The threat associated with computer viruses applies equally to PDAs as it does to laptops and PCs. Therefore, the same level of control should be maintained for PDAs (see the Virus and Worm Controls section later in this chapter).
- **Device registration**—PDAs authorized for business use should be registered in a database to distinguish them from those that are individually owned. Organizations can push updates or manage authorized devices and exclude personally-owned PDAs.
- **Camera use**—Some PDAs include megapixel cameras that could expose sensitive information through pictures taken. The policy should regulate the use of cameras and sensitive locations should have clearly visible signage to disallow such use.

Access Issues With Mobile Technology

Devices used to move data from networks and desktop systems to mobile equipment such as miniature hard and flash drives which simply plug into the USB port are popular and can be purchased

at a low cost. Individual employees may even use such devices of their own to misuse enterprise computing facilities and take unauthorized copies of data or even programs. These devices should be strictly controlled both by policy and denial of use. Possible actions include:

- Banning all use of transportable drives in the security policy
- Where no authorized use of USB ports exists, disabling use with a logon script which removes them from the system directory
- If they are considered necessary for business use, encrypting all data transported or saved by these devices

Audit Logging in Monitoring System Access

Most access control software today has security features that enable a security administrator to automatically log and report all levels of access attempts—successes and failures. For example, access control software can log computer activity initiated through a logon ID or computer terminal. This information provides management an audit trail to monitor activities of a suspicious nature, such as a hacker attempting brute-force attacks on a privileged logon ID. Also, keystroke logging can be turned on for users that have sensitive access privileges. What is logged is determined by the action of the organization. Issues include what is logged, who/what has access to the logs and how long logs are retained (record-retention item).

ACCESS RIGHTS TO SYSTEM LOGS

Access rights to system logs for security administrators to perform the above activities should be strictly controlled.

Computer security managers and system administrators/managers should have access for review purposes; however, security and/or administration personnel who maintain logical access functions may have no need for access to audit logs.

It is particularly important to ensure the integrity of audit trail data against modification. One way to do this is to use digital signatures. Another way is to use write-once devices. The audit trail files need to be protected since, for example, intruders may try to cover their tracks by modifying audit trail records. Audit trail records should be protected by strong access controls to help prevent unauthorized access. The integrity of audit trail information may be particularly important when legal issues arise, such as the use of audit trails as legal evidence. (This may, for example, require daily printing and signing of the logs.) Questions regarding such legal issues should be directed to the appropriate legal counsel.

The confidentiality of audit trail information may also be protected, for example, if the audit trail is recording information about users that may be disclosure-sensitive, such as transaction data containing personal information (e.g., before and after records of modification to income tax data). Strong access controls and encryption can be particularly effective in preserving confidentiality.

The logging of media is used to support accountability. Logs can include control numbers (or other tracking data) such as the times and dates of transfers, names and signatures of individuals involved, and other relevant information. Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals named in control logs. Automated media tracking systems may be helpful for maintaining inventories of tape and disk libraries.

A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours. Certain reports are generated for security recorded in activity logs.

TOOLS FOR AUDIT TRAIL (LOGS) ANALYSIS

Many types of tools have been developed to help reduce the amount of information contained in audit records and to delineate useful information from the raw data.

On most systems, audit trail software can create large files, which can be extremely difficult to analyze manually. The use of automated tools is likely to be the difference between unused audit trail data and an effective review. Some of the types of tools include:

- **Audit reduction tools**—They are preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. (This alone may cut in half the number of records in the audit trail.) These tools generally remove records generated by specified classes of events, for example, records generated by nightly backups might be removed.
- **Trend/variance-detection tools**—They look for anomalies in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major variations. For example, if a user typically logs in at 09.00, but appears at 04.30 one morning, this may indicate a security problem that may need to be investigated.
- **Attack-signature-detection tools**—They look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed logon attempts.

COST CONSIDERATIONS

Audit trails involve many costs. First, some system overhead is incurred while recording the audit trail. Additional system overhead will be incurred to store and process the records. The more detailed the records, the more overhead is required. Another cost involves human and machine time required to perform the analysis. This can be minimized by using tools to perform most of the analysis. Many simple analyzers can be constructed quickly and inexpensively from system utilities, but they are limited to audit reduction and the identification of particularly sensitive events. More complex tools that identify trends or sequences of events are slowly becoming available as off-the-shelf software. (If complex tools are not available for a system, development may be prohibitively expensive. Some intrusion detection systems, for example, have taken years to develop.)

The final cost of audit trails is the cost of investigating unexpected and anomalous events. If the system is identifying too many events as suspicious, administrators may spend undue time reconstructing events and questioning personnel.

The frequency of the security administrator's review of computer access reports should be commensurate with the sensitivity of the computerized information being protected. The IS auditor should ensure that the logs cannot be tampered with, or altered, without leaving an audit trail.

When reviewing or performing security access follow-up, the IS auditor should look for:
- Patterns or trends that indicate abuse of access privileges, such as concentration on a sensitive application
- Violations (such as attempting computer file access that is not authorized) and/or use of incorrect passwords

Today, attempted violations can be detected on either a real-time basis and acted upon immediately or after the fact. For interconnected networks, often the first line of defense for attacks on organization's trusted networks and systems is an intrusion detection system (IDS).

IDS refers to the process of discovering unauthorized use of computers and networks through the use of software designed for this purpose. An IDS works in a variety of ways, either host- or network-based, to analyze and log incoming data for signs of unauthorized access. In designing these systems, organization's should identify scenarios or events that constitute a high risk, provide for real-time notifications to system administrators of these events occurring (IDSs interfacing with pagers), and establish procedures for responding to those events.

An intrusion prevention system (IPS) is an extension of an IDS. An IDS detects and reports, while an IPS takes this a step further to block unauthorized connection in real time and in an automated manner. IPS works with access control devices such as routers, firewalls and application-level proxy. Once unauthorized access is detected, the IPS will send a message to appropriate devices to block such access. The drawback of an IPS is that it may inadvertently block legitimate traffic.

Once a violation has been identified:
- The person who identified the violator should refer the problem to the security administrator for investigation.
- The security administrator and responsible management should work together to investigate and determine the severity of the violation. Generally, most violations are accidental.
- If a violation attempt is serious, executive management should be notified, not law enforcement officials. Executive management normally is responsible for notifying law enforcement officials. Involvement of external agencies may result in adverse publicity that is ultimately more damaging than the original violation; therefore, the decision to involve external agencies should be left to executive management.
- Procedures should be in place to manage public relations and the press.
- To facilitate proper handling of access violations, written guidelines should exist that identify various types and levels of violations and how they will be addressed. This effectively provides direction for judging the seriousness of a violation.
- Disciplinary action should be a formal process that is applied consistently. This may involve a reprimand, probation or immediate termination. The procedures should be legally and ethically sound to reduce the risk of legal action against the company.
- Corrective measures should include a review of the computer access rules, not only for the perpetrator but for interested parties. Excessive or inappropriate access rules should be eliminated.

Restricting and Monitoring Access

There should be restrictions and procedures of monitoring access to computer features that bypass security. Generally, only system software programmers should have access to these features:
- **Bypass label processing (BLP)**—BLP bypasses the computer reading of the file label. Since most access control rules are based on file names (labels), this can bypass access control programs.
- **System exits**—This system software feature permits the user to perform complex system maintenance, which may be tailored to a specific environment or company. They often exist outside of the computer security system and, thus, are not restricted or reported in their use.
- **Special system logon IDs**—These logon IDs often are provided by vendors. The names can be determined easily because they are the same for all similar computer systems (i.e., "system"). Passwords should be changed immediately upon installation to secure the systems.

Naming Conventions for Logical Access Controls

Access capabilities are implemented by security administration in a set of access rules that stipulates which users (or groups of users) are authorized to access a resource (such as a dataset or file) and at what level (such as read or update). The access control mechanism applies these rules whenever a user attempts to access or use a protected resource.

Access control naming conventions are structures used to govern user access to the system and user authority to access/use computer resources such as files, programs and terminals. These general naming conventions and associated files are required in a computer environment to establish and maintain personal accountability and segregation of duties in the access of data. The owners of the data or application, with the help of the security officer, usually set up naming conventions. The need for sophisticated naming conventions over access controls depends on the importance and level of security that is needed to ensure that unauthorized access has not been granted. It is important to establish naming conventions that both promote the implementation of efficient access rules and simplify security administration.

Naming conventions for system resources (e.g., as datasets, volumes, programs and employees workstations) are an important prerequisite for efficient administration of security controls. Naming conventions can be structured so that resources beginning with the same high-level qualifier can be governed by one or more generic rule(s). This reduces the number of rules required to adequately protect resources which, in turn, facilitates security administration and maintenance efforts.

5.3.7 STORING, RETRIEVING, TRANSPORTING AND DISPOSING OF CONFIDENTIAL INFORMATION

Management should define and implement procedures to prevent access to, or loss of, sensitive information and software from computers, disks, and other equipment or media when they are stored, disposed of or transferred to another user.

This should be done for:

- Backup files of databases—Backup files on magnetic tapes are often unencrypted, so that even confidential information may be obtained by simply transferring backup databases to other systems for data analysis. Security problems of data media storage and transportation technologies involve ensuring that contractors used to transport and store backup tapes have adequate policies and procedures to protect the integrity and confidentiality of the information.
- Data banks—Research and commercial institutions collect the results of important survey or research projects on large tapes. These data have a high commercial value and may be subject to a requirement of availability and confidentiality that persist for many years, longer than the duration of the media containing them. Preserving the value requires precautions and possibly a planned media verification or duplication activity. In general, a solution is required to the problems of long-term computer storage of sensitive information. Optical disks are a possible medium, but their durability and standardization should be evaluated.
- Disposal of media previously used to hold confidential information—Procedures should be implemented to identify and erase the sensitive information and software inside computers, disks and other equipment or media that have been identified for disposal so that deleted data may not be retrieved by any internal or third party. Care must be taken not only to meet the requirements of data protection, but also when a machine is transferred to another user. The original user should remove any personal data that are not confidential by nature. If previously held data were sensitive, the disk should be reformatted and then a secure wipe of the disk should be carried out with appropriate utility software.

  In some cases, when information is highly confidential, it may prove insufficient to wipe the media. Random access memory (RAM) is included because favorable circumstances and appropriate technical analysis of these media could expose the data. This may require that such equipment or media should be disposed of in a secure manner (e.g., destruction). This may include "degaussing" (demagnetizing) the magnetic media, such as tapes or PC hard drives, and possibly their physical destruction.
- Management of equipment sent for offsite maintenance—Data files and proprietary software should be backed up, so that they can be erased from the equipment prior to sending it offsite for maintenance (e.g., computers, PDAs, miniature hard/flash drives). Computers holding confidential data should not be sent out for repair, unless memories are withheld.
- Public agencies and organizations concerned with sensitive, critical or confidential information—These organizations may have particular obligations to develop a comprehensive records management program. Policies addressing these needs should reflect laws concerning availability, substance, degree of confidentiality and disposal compared to available technical solutions and organizational needs. For instance, public records may be destroyed only in accordance with precise record-retention schedules, and the record holder may not mutilate, destroy, sell, loan or otherwise dispose of any record, except under a record-retention schedule or with the written consent of the owner. Proper record retention requires the preparation of separate retention schedules depending on subject files (administrative vs. other legal requirements).
- E-token electronic keys—For such sensitive information, data transportation on floppy and hard disks is not safe and should not be used. Taking proper care of the media can significantly reduce the chances of data loss.
- Storage records—Many commercial organizations fulfill legal or institutional obligations to preserve specific types of records, which may be confidential in nature, for a given number of years. In some cases these obligations are fulfilled by preserving database images and the source of the documents, either online or on backup tapes. In these cases, the conditions of recreating the original document must be integrally retained as well.

Preserving Information During Shipment or Storage

Manufacturers publish recommended temperature and humidity levels in which to store media. These recommendations should be consulted and adhered to before storing or shipping important media. However, some general tips can be followed to help avoid potential damage to media during shipping and storage. The following environmental issues are applicable to all types of media:

- Keep out of direct sunlight.
- Keep free of dust.
- Keep free of liquids.
- Minimize exposure to magnetic fields, radio equipment or any sources of vibration.
- Do not air transport in areas and at times of exposure to a strong magnetic storm.

Media-specific Storage Precautions

Some precautions need to be considered regarding media-specific storage (see **exhibit 5.9**).

Exhibit 5.9—Media-specific Storage Precautions

Media Storage	Precautions
Hard drives	• Store hard drives in antistatic bags, and be sure that the person removing them from the bag is static-free. • If the original box and padding for the hard drive is available, use it for shipping. • Avoid styrofoam packaging products or other materials that can cause static electricity. • Quick drops or spikes in temperature are a danger, since such changes can lead to hard drive crashes. • If the hard drive has been in a cold environment, bring it to room temperature prior to installing and using it. • Avoid sudden mechanical shocks or vibrations.
Magnetic media	• Store tapes vertically. • Store tapes in acid-free containers. • Write-protect tapes immediately.

Exhibit 5.9—Media-specific Storage Precautions *(cont.)*	
Media Storage	**Precautions**
Floppy disks	• When handling the floppy, pick it up by the label. The mylar surface must never be touched. • Write labels using a felt tip pen only.
CDs and DVDs	• Handle by the edges or by the hole in the middle. • Be careful not to bend the CD. • Avoid long-term exposure to bright light. • Store in a hard jewel case, not in soft sleeves.

5.4 NETWORK INFRASTRUCTURE SECURITY

Communication networks (wide area or local area networks) generally include devices connected to the network as well as programs and files supporting the network operations. Control is accomplished through a network control terminal and specialized communications software.

The following are controls over the communication network:
- Network control functions should be performed by individuals possessing adequate training and experience.
- Network control functions should be separated, and the duties should be rotated on a regular basis, where possible.
- Network control software must restrict operator access from performing certain functions (e.g., the ability to amend/delete operator activity logs).
- Network control software should maintain an audit trail of all operator activities.
- Audit trails should be periodically reviewed by operations management to detect any unauthorized network operations activities.
- Network operation standards and protocols should be documented and made available to the operators, and should be reviewed periodically to ensure compliance.
- Network access by the system engineers should be monitored and reviewed closely to detect unauthorized access to the network.
- Analysis should be performed to ensure workload balance, fast response time and system efficiency.
- A terminal identification file should be maintained by the communications software to check the authentication of a terminal when it tries to send or receive messages.
- Data encryption should be used, where appropriate, to protect messages from disclosure during transmission.

To improve the control and maintenance of the infrastructure and its use, besides the direct management of the network devices, consolidate the logs of these devices with the firewall's logs and the client-server operating system's logs.

In recent years, the management of large capacity storage units is frequently based on fiber channel connections (e.g., [SysAdmin, Audit, Network, Security] SANs).

Systems security is improved when a dynamic inventory of the devices is possible. In the case of an incident, it is important to know which computer is used by whom.

Another important security improvement is the ability to identify users at every step of their activity. Some application packages use predefined names (e.g., SYSTEM). New monitoring tools have been developed to resolve this problem.

The requirements above help facilitate the practice of IT governance. There are different models employed in this process. One of them is is Information Technology Infrastructure Library (ITIL). Its main goal is not only the support of resource management, but also the overall management of information systems through the use of service level agreements.

5.4.1 LAN SECURITY

LANs facilitate the storage and retrieval of programs and data used by a group of people. LAN software and practices also need to provide for the security of these programs and data. Unfortunately, most LAN software provides a low level of security. The emphasis has been on providing capability and functionality rather than security. As a result, risks associated with use of LANs include:
- Loss of data and program integrity through unauthorized changes
- Lack of current data protection through inability to maintain version control
- Exposure to external activity through limited user verification and potential public network access from dial-in connections
- Virus and worm infection
- Improper disclosure of data because of general access rather than need-to-know access provisions
- Violating software licenses by using unlicensed or excessive numbers of software copies
- Illegal access by impersonating or masquerading as a legitimate LAN user
- Internal user's sniffing (obtaining seemingly unimportant information from the network that can be used to launch an attack such as network address information)
- Internal user's spoofing (reconfiguring a network address to pretend to be a different address)
- Destruction of the logging and auditing data

The LAN security provisions available depend on the software product, product version and implementation. Commonly available network security administrative capabilities include:
- Declaring ownership of programs, files and storage
- Limiting access to a read-only basis
- Implementing record and file locking to prevent simultaneous update
- Enforcing user ID/password sign-on procedures, including the rules relating to password length, format and change frequency
- Using switches to implement port security policies rather than hubs or non-manageable switches. This will prevent unauthorized hosts, with unknown MAC addresses, to connect to the LAN.
- Encrypting local traffic using IPSec (IP security) protocol

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

To gain a full understanding of the LAN, the IS auditor should identify and document the following:
- LAN topology and network design
- LAN administrator/LAN owner
- Functions performed by the LAN administrator/owner
- Distinct groups of LAN users
- Computer applications used on the LAN
- Procedures and standards relating to network design, support, naming conventions and data security

LAN Risks and Issues

The administrative and control functions available with network software might be limited. Software vendors and network users have recognized the need to provide diagnostic capabilities to identify the cause of problems when the network goes down or functions in an unusual manner. The use of logon IDs and passwords with associated administration facilities is only becoming standard now.

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

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

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

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

Dial-up Access Controls

It is possible to break LAN security through the dial-in route. Without dial-up access controls, a caller can dial in and try passwords until they gain access. Once in, they can hide pieces of software, pass through WAN links to other systems, and generally create havoc.

To minimize the risk of unauthorized dial-in access, remote users should never store their passwords in plaintext login scripts on notebooks or desktops. Furthermore, portable PCs should be protected by physical keys and/or basic input/output system (BIOS)-based passwords to limit access to data if stolen.

A dial-back modem may be used to prevent access by guessing passwords. When a call is answered by the modem, the caller must enter a code. The modem then hangs up the connection, looks up a corresponding phone number that has been authorized for dial-in access, and calls the number back if it is authenticated. However, several things may go wrong with this method. First, a hacker can record the caller's code and use it later, if the hacker can be at the target location, turn on call forwarding or otherwise divert the call. Some dial-back modems do not listen for dial tone when they call back. If the hacker stays on the line, dialing occurs but has no effect. Then the hacker can start trying passwords until they achieve entry. There are solutions to this issue. Packet-sized authenticating and encrypting modems with random password generation can be used by authenticating the user's personal identification number (PIN). Other methods include the use of one-time password generator devices held by the user. These generate unique passwords that can be authenticated by the host. Alternatively, dial-back modems are available that are connected to two individual telephone lines: one is used for incoming calls and the second is used to call back the user on the known telephone number. These are generally referred to as twin-line dial-back modems.

5.4.2 CLIENT-SERVER SECURITY

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

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

Client-server Risks and Issues

Since the early 1990s, client-server technology has become one of the predominant ways many organizations have processed production data, and developed and delivered mission-critical products and services. Client-server technology enables business units to develop and deliver products and services to market much quicker traditional legacy methods. The trade-off is that controls over these systems typically are substandard to those associated with traditional mainframe systems. However, there are higher risks that can severely impact a company's business, if controls are not in place to prevent or detect them.

The areas of risk and concern in a client-server environment are listed below:

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

Note: The IS auditor should be familiar with risks and exposures related to network infrastructure. The CISA candidate will not be tested on risks of specific technical platforms or infrastructures.

5.4.3 WIRELESS SECURITY THREATS AND RISK MITIGATION

The classification of security threats may be segmented into nine categories:

- Errors and omissions
- Fraud and theft committed by authorized or unauthorized users of the system
- Employee sabotage
- Loss of physical and infrastructure support
- Malicious hackers
- Industrial espionage
- Malicious code
- Foreign government espionage
- Threats to personal privacy

All of these represent potential threats in wireless networks as well. However, the more immediate concerns for wireless communications are device theft, denial of service, malicious hackers, malicious code, theft of service, and industrial and foreign espionage.

Theft is likely to occur with wireless devices because of their portability. Authorized and unauthorized users of the system may commit fraud and theft; however, authorized users are more likely to carry out such acts. Since users of a system may know what resources a system has and the system's security flaws, it is easier for them to commit fraud and theft.

Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications.

Malicious code involves viruses, worms, Trojan horses, logic bombs or other unwanted software that is intended to damage files or bring down a system. Theft of service occurs when an unauthorized user gains access to the network and consumes network resources. In wireless networks, the unauthorized access threat stems from the relative ease with which eavesdropping can occur on radio transmissions.

Ensuring confidentiality, integrity, authenticity and availability are the prime objectives in wireless networks.

Security requirements include the following:

- **Authenticity**—A third party must be able to verify that the content of a message has not been changed in transit.
- **Nonrepudiation**—The origin or the receipt of a specific message must be verifiable by a third party.
- **Accountability**—The actions of an entity must be uniquely traceable to that entity.
- **Network availability**—The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.

Risks in wireless networks are equal to the sum of the risk of operating a wired network plus the new risks introduced by weaknesses in wireless protocols. To mitigate these risks, an

organization must adopt security measures and practices that help bring their risks to a manageable level.

To date, the list below includes some of the more salient threats and vulnerabilities of wireless systems:
- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Weaknesses in wireless protocols increase the threat of disclosure of sensitive information. Many wireless networks are either not secure or use outdated encryption algorithms.
- Malicious entities may gain unauthorized access to an agency's computer or voice (IP telephony) network through wireless connections, potentially bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and is transmitted between two wireless devices may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and track their physical movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other agencies for the purposes of launching attacks and concealing their activity.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.
- Malicious entities may use a third-party, untrusted wireless network service to gain access to the network resources.

Currently, there are many ways that malicious entities may gain access to wireless devices. Those related to WLANs include, but are not limited to, war driving, war walking and war chalking as described in exhibit 5.8.

On the wireless personal area network (WPAN) side, one of the important risks is the man-in-the-middle attack as described in exhibit 5.8.

The other problem with WPANs is the uncontrolled propagation of radio waves; for example, the radio traffic on Bluetooth connections can be passively intercepted and recorded using Bluetooth protocol sniffers such as Red Fang, Bluesniff and others. If the device addresses are known, then even if the devices are currently in nondiscoverable mode, it is possible to synchronize to the frequency hopping sequence. All the layers of the Bluetooth protocol stack can be examined and analyzed offline. If encryption is not used, then it is possible to extract and monitor the transmitted user data. Use of an antenna with a strong directional characteristic and electronics capable of amplifying Bluetooth signals can make passive listening attacks possible from a greater distance than the functional range. Transmitting power control is optional and is not supported by every Bluetooth device.

The growing prevalence of people using Bluetooth-enabled equipment is likely to follow the trend of Wi-Fi war driving, in which people try to identify inadequately secured networks by driving around with a laptop.

5.4.4 INTERNET THREATS AND SECURITY

The nature of the Internet makes it vulnerable to attack. The Internet is a global TCP/IP-based system that enables public and private heterogeneous networks to communicate with one another. Estimates claim that there are over 300 million computers connected via the Internet. Originally designed to allow for the freest possible exchange of information, it is widely used today for commercial purposes. This poses significant security problems for organizations when protecting their information assets. For example, hackers and virus writers try to attack the Internet and computers connected to the Internet. Some want to invade others' privacy and attempt to crack into databases of sensitive information or sniff information as it travels across Internet routes. Consequently, it becomes more important for IS auditors to understand the risks and security factors that are needed to ensure that proper controls are in place when a company connects to the Internet.

The Internet Protocol is designed solely for the addressing and routing of data packets across a network. It does not guarantee or provide evidence on the delivery of messages; there is no verification of an address; the sender will not know if the message reaches its destination at the time it is required; the receiver does not know if the message came from the address specified as the return address in the packet. Other protocols correct some of these drawbacks.

Network Security Threats

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

Passive Attacks

Examples of passive attacks that gather network information include network analysis, eavesdropping and traffic analysis as explained in exhibit 5.8.

Active Attacks

Once enough network information has been gathered, the intruder will launch an actual attack against a targeted system to either gain complete control over that system or enough control to cause certain threats to be realized. This may include obtaining unauthorized access to modify data or programs, causing a denial of service, escalating privileges, accessing other systems, and

obtaining sensitive information for personal gain. These types of penetrations or intrusions are known as active attacks. They affect the integrity, availability and authentication attributes of network security. Common forms of active attacks may include the following (explained in exhibit 5.8):

- Brute-force attack
- Masquerading
- Packet replay
- Phishing
- Message modification
- Unauthorized access through the Internet or World Wide Web
- Denial of service (DoS)
- Dial-in penetration attacks
- E-mail bombing and spamming
- E-mail spoofing

Causal Factors for Internet Attacks

Generally, Internet attacks of both a passive and active nature occur for a number of reasons including:

- Availability of tools and techniques on the Internet or as commercially available software that an intruder can download easily. For example, to scan ports, an intruder can easily obtain network scanners such as strobe, netcat, jakal, nmap or Asmodeous (Windows). Additionally, password cracking programs such as John the Ripper and LophtCrack are available free or at a minimal cost.
- Lack of security awareness and training among an organization's employees
- Exploitation of known security vulnerabilities in network- and host-based systems. Many organizations fail to properly configure their systems and to apply security patches or fixes when vulnerabilities are discovered. Most problems can be reduced significantly by keeping network- and host-based systems properly configured and up to date.
- Inadequate security over firewalls and host-based operating systems allowing intruders to view internal addresses and use network services indiscriminately

With careful consideration when designing and developing network security controls and supporting processes, an organization can effectively prevent and detect most intrusive attacks on their networks. In this situation, it becomes important for IS auditors to understand the risks and security factors that are needed to ensure proper controls are in place when a company connects to the Internet. There are several areas of control risks that must be evaluated by the IS auditor to determine the adequacy of Internet security controls.

Internet Security Controls

To establish effective Internet security controls, an organization must develop controls within an information systems security framework from which Internet security controls can be implemented and supported. Generally, the process for establishing such a framework entails defining, through corporate policies and procedures, the rules the organization will follow to control Internet usage. For example, one set of rules should address appropriate use of Internet resources with rules that might reserve Internet privileges for those with a business need, define what information resources should be available for outside users, and define trusted and untrusted networks within and outside the organization.

Another set of rules should address the classification of the sensitivity or criticality of corporate information resources. This will help to determine what information will be available for use on the Internet and the level of security to be used for corporate resources of a sensitive or critical nature on the Internet.

From an evaluation of these issues, an organization will be able to develop guidelines specific to their situations for defining the level of security controls related to the confidentiality, integrity and availability of information resources (i.e., business applications) on the Internet. For example, operating system security hardening guidelines can be developed which define how the operating system should be configured, detail which Internet services should be blocked from use or exploitation by external untrusted users, and define how the system will be protected by firewalls. Additionally, supporting processes over these controls should be defined including:

- Risk assessments performed periodically over the development and redesign of Internet-based web applications
- Security awareness and training for employees, tailored to their levels of responsibilities
- Firewall standards and security to develop and implement firewall architectures
- Intrusion detection standards and security to develop and implement IDS architectures
- Remote access for coordinating and centrally controlling dial-up access on the Internet via corporate resources
- Incident handling and response for detection, response, containment and recovery
- Configuration management for controlling the security baseline when changes do occur
- Encryption techniques applied to protect information assets passing over the Internet
- A common desktop environment to control, in an automated fashion, what is displayed on a user's desktop
- Monitoring Internet activities for unauthorized usage and notification to end users of security incidents via CERT bulletins or alerts

In summary, Internet usage is drastically changing the way business is done and is creating opportunities for organizations to compete in what has become a global virtual market. To compete and survive in this new marketplace, organizations have to go through a paradigm shift in the way they regard security. Security, as it relates to the Internet, will have to be considered an enabler for success and treated as an essential business tool.

Firewall Security Systems

Every time a corporation connects its internal computer network to the Internet, it faces potential danger. Because of the Internet's openness, every corporate network connected to it is vulnerable to attack. Hackers on the Internet could theoretically break into the corporate network and do harm in a number of ways: steal or damage important data, damage individual computers or the entire network, use the corporate computer's resources, or use the corporate network and resources as a way of posing as a corporate employee. Companies should build firewalls as one means of perimeter security for their networks. Likewise, this same principle holds true for sensitive or critical systems that need to be protected from untrusted users inside the corporate network (internal hackers). Firewalls are defined as a device installed at the point where

network connections enter a site; they apply rules to control the type of networking traffic flowing in and out. Most commercial firewalls are built to handle the most commonly used Internet protocols.

To be effective, firewalls should allow individuals on the corporate network to access the Internet and, at the same time, stop hackers or others on the Internet from gaining access to the corporate network to cause damage. Generally, most organizations will follow a deny-all philosophy, which means that access to a given resource will be denied unless a user can provide a specific business reason or need for access to the information resource. The converse of this access philosophy, not widely accepted, is the accept-all philosophy under which everyone is allowed access unless someone can provide a reason for denying access.

Firewall General Features

Firewalls are hardware and software combinations that are built using routers, servers and a variety of software. They should control the most vulnerable point between a corporate network and the Internet, and they can be as simple or complex as the corporate information security policy demands. There are many different types of firewalls, but most enable organizations to:

- Block access to particular sites on the Internet
- Limit traffic on an organization's public services segment to relevant addresses and ports
- Prevent certain users from accessing certain servers or services
- Monitor communications between an internal and an external network
- Monitor and record all communications between an internal network and the outside world to investigate network penetrations or detect internal subversion
- Encrypt packets that are sent between different physical locations within an organization by creating a VPN over the Internet (i.e., IP security [IPSec], VPN tunnels)

The capabilities of some firewalls can be extended so they can also provide for protection against viruses and attacks directed to exploit known operating system vulnerabilities.

Firewall Types

Generally, the types of firewalls available today fall into three categories:

- Router packet filtering
- Application firewall systems
- Stateful inspection

These firewalls are discussed in the following sections.

ROUTER PACKET FILTERING FIREWALLS

The simplest and earliest kinds of firewalls (i.e., first generation of firewalls) were packet filtering-based firewalls deployed between the private network and the Internet. In packet filtering, a screening router examines the header of every packet of data traveling between the Internet and the corporate network. Packet headers have information in them, including the IP address of the sender and receiver, and the authorized port numbers (application or service) allowed to use the information transmitted. Based on that information, the router knows what kind of Internet service, such as web-based or or FTP, is being used to send the data as well as the identities of the sender and receiver of the data. Using that information, the router can prevent certain packets from being sent between the Internet and the corporate network. For example, the router could block any traffic except for e-mail or traffic to and from suspicious destinations.

The advantages of this type of firewall are its simplicity and generally stable performance since the filtering rules are performed at the network layer. Its simplicity is also a disadvantage, because it is vulnerable to attacks from improperly configured filters and attacks tunneled over permitted services. Since the direct exchange of packets is permitted between outside systems and inside systems, the potential for an attack is determined by the total number of hosts and services to which the packet filtering router permits traffic. Also, if a single packet filtering router is compromised, every system on the private network may be compromised and organizations with many routers may face difficulties in designing, coding and maintaining the rule base. This means that each host directly accessible from the Internet needs to support sophisticated user authentication and needs to be regularly examined by the network administrator for signs of attack.

Some of the more common attacks against packet filter firewalls are:

- **IP spoofing**—The attacker fakes the IP address of either an internal network host or a trusted network host so that the packet being sent will pass the rule base of the firewall. This allows for penetration of the system perimeter. If the spoofing uses an internal IP address, the firewall can be configured to drop the packet on the basis of packet flow direction analysis. However, if the attacker has access to a secure or trusted external IP address and spoofs on that address, the firewall architecture is defenseless.
- **Source routing specification**—It is possible to define the routing that an IP packet must take when it traverses from the source host to the destination host, across the Internet. In this process, it is possible to define the route so it bypasses the firewall. Only those that know of the IP address, subnet mask and default gateway settings at the firewall routing station can do this. A clear defense against this attack is to examine each packet and, if the source routing specification is enabled, drop that packet. However, if the topology permits a route, skipping the choke point, this countermeasure will not be effective.
- **Miniature fragment attack**—Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall in the hope that only the first of the sequence of fragmented packets would be examined and the others would pass without review. This is true if the default setting is to pass residual packets. This can be countered by configuring the firewall to drop all packets where IP fragmentation is enabled or offset to value 1.

APPLICATION FIREWALL SYSTEMS

There are two types of application firewall systems. They are referred to as application- and circuit-level firewall systems and provide greater protection capabilities than packet filtering routers. Packet filtering routers allow the direct flow of packets between internal and external systems. Application and circuit gateway firewall systems allow information to flow between systems but do not allow the direct exchange of packets. The primary risk of allowing packet exchange between internal and

external systems is that the host applications residing on the protected network's systems must be secure against any threat posed by the allowed packets.

The two types of application firewall systems sit atop hardened (tightly secured) operating systems, such as Windows NT and UNIX, and work at the application level of the Open Systems Interconnection (OSI) model. The application-level gateway firewall is a system that analyzes packets through a set of proxies—one for each service (e.g., Hypertext Transmission Protocol [HTTP] proxy for web traffic, FTP proxy). This kind of work could reduce network performance. Circuit-level firewalls are more efficient and also operate at the application level—where Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) sessions are validated, typically through a single, general-purpose proxy before opening a connection. Commercially, circuit-level firewalls are quite rare.

Both application firewall systems employ the concept of bastion hosting in that they handle all incoming requests from the Internet to the corporate network, such as FTP or web requests. Bastion hosts are heavily fortified against attack. By having only a single host handling incoming requests, it is easier to maintain security and track attacks. Therefore, in the event of a break-in, only the firewall system has been compromised, not the entire network. In this way, none of the computers or hosts on the corporate network can be contacted directly for requests from the Internet, providing an effective level or layer of security.

Additionally, application-based firewall systems are set up as proxy servers to act on the behalf of someone inside an organization's private network. Rather than relying on a generic packet filtering tool to manage the flow of Internet services through the firewall, a special-purpose code called a proxy server is incorporated into the firewall system. For example, when someone inside the corporate network wants to access a server on the Internet, a request from the computer is sent to the proxy server, the proxy server contacts the server on the Internet, and the proxy server then sends the information from the Internet server to the computer inside the corporate network. By acting as a go-between, proxy servers can maintain security by examining a service's (e.g., FTP, Telnet) program code and modifying and securing it to eliminate known vulnerabilities. The proxy server can also log all traffic between the Internet and the network.

The application-level firewall implementation of proxy server functions is based on providing a separate proxy for each application service (e.g., FTP, Telnet, HTTP). This differs from circuit-level firewalls, which do not need a special proxy for each application-level service. In other words, one proxy server is used for all services.

Advantages of these types of firewalls are that they provide security for commonly used protocols and generally hide the internal network from outside untrusted networks. For example, a feature available on these types of firewall systems is the network address translation (NAT) capability. This capability takes private internal network addresses (unusable on the Internet) and maps them to a table of public IP addresses, assigned to the organization, which can be used across the Internet.

Disadvantages are poor performance and scalability as Internet usage grows. To offset this problem, the concept of load balancing is applicable in cases where a redundant fail-over firewall system may be used.

STATEFUL INSPECTION FIREWALLS

A stateful inspection firewall keeps track of the destination IP address of each packet that leaves the organization's internal network. Whenever the response to a packet is received, its record is referenced to ascertain and ensure that the incoming message is in response to the request that went out from the organization. This is done by mapping the source IP address of an incoming packet with the list of destination IP addresses that is maintained and updated. This approach prevents any attack initiated and originated by an outsider.

The advantages of this approach over application firewall systems is that stateful inspection firewalls control the flow of IP traffic by matching information contained in the headers of connection-oriented or connectionless IP packets at the transport layer, against a set of rules specified by the firewall administrator. This provides a greater degree of efficiency when compared to typical CPU-intensive, full-time application firewall systems' proxy servers, which may perform extensive processing on each data packet at the application level.

The disadvantages include that stateful inspection firewalls can be relatively complex to administer compared to the other two types of firewalls.

Examples of Firewall Implementations

Firewall implementations can take advantage of the functionality available in a variety of firewall designs to provide a robust layered approach in protecting an organization's information assets. Commonly used implementations available today include:

- **Screened-host firewall**—Utilizing a packet filtering router and a bastion host, this approach implements basic network layer security (packet filtering) and application server security (proxy services). An intruder in this configuration has to penetrate two separate systems before the security of the private network can be compromised. This firewall system is configured with the bastion host connected to the private network with a packet filtering router between the Internet and the bastion host. Router filtering rules allow inbound traffic to access only the bastion host, which blocks access to internal systems. Since the inside hosts reside on the same network as the bastion host, the security policy of the organization determines whether inside systems are permitted direct access to the Internet, or whether they are required to use the proxy services on the bastion host.
- **Dual-homed firewall**—A firewall system that has two or more network interfaces, each of which is connected to a different network. In a firewall configuration, a dual-homed firewall usually acts to block or filter some or all of the traffic trying to pass between the networks. A dual-homed firewall system is a more restrictive form of a screened-host firewall system, in which a dual-homed bastion host is configured with one interface established for information servers and another for private network host computers.
- **Demilitarized zone (DMZ) or screened-subnet firewall**—Utilizing two packet filtering routers and a bastion host,

this approach creates the most secure firewall system since it supports network- and application-level security while defining a separate DMZ network. The DMZ functions as a small, isolated network for an organization's public servers, bastion host information servers and modem pools. Typically, DMZs are configured to limit access from the Internet and the organization's private network. Incoming traffic access is restricted into the DMZ network by the outside router and protects the organization against certain attacks by limiting the services available for use. Consequently, external systems can access only the bastion host (and its proxying service capabilities to internal systems) and possibly information servers in the DMZ. The inside router provides a second line of defense, managing DMZ access to the private network, while accepting only traffic originating from the bastion host. For outbound traffic, the inside router manages private network access to the DMZ network. It permits internal systems to access only the bastion host and information servers in the DMZ. The filtering rules on the outside router require the use of proxy services by accepting only outbound traffic on the bastion host. The key benefits of this system are that an intruder must penetrate three separate devices, private network addresses are not disclosed to the Internet, and internal systems do not have direct access to the Internet.

Firewall Issues

Problems faced by organizations that have implemented firewalls include:

- A false sense of security may exist where management feels that no further security checks and controls are needed on the internal network (i.e., the majority of incidents are caused by insiders, who are not controlled by firewalls).
- The circumvention of firewalls through the use of modems may connect users directly to ISPs. Management should provide assurance that the use of modems when a firewall exists is strictly controlled or prohibited altogether.
- Misconfigured firewalls may allow unknown and dangerous services to pass through freely.
- What constitutes a firewall may be misunderstood (e.g., companies claiming to have a firewall merely have a screening router).
- Monitoring activities may not occur on a regular basis (i.e., log settings not appropriately applied and reviewed).
- Firewall policies may not be maintained regularly.
- Most firewalls operate at the network layer; therefore, they do not stop any application-based or input-based attacks. Examples of such attacks include Structured Query Language (SQL) injection and buffer-overflow attacks. Newer-generation firewalls are able to inspect traffic at the application layer and stop some of these attacks.

Firewall Platforms

Firewalls may be implemented using hardware or software platforms. When implemented in hardware, it will provide good performance with minimal system overhead. Although hardware-based firewall platforms are faster, they are not as flexible or scalable as software-based firewalls. Software-based firewalls are generally slower with significant systems overhead; however, they are flexible with additional services. They may include content and virus checking, before traffic is passed to users.

It is generally better to use appliances, rather than normal servers, for the firewall. Appliances are normally installed with hardened operating systems. When server-based firewalls are used, operating systems in servers are often vulnerable to attacks. When the attacks on operating systems succeed, the firewall would be compromised. Appliance-type firewalls are, generally, significantly faster to set up and recover.

Intrusion Detection Systems

Another element to securing networks complementing firewall implementations is an IDS. An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies. It protects a company's IS resources from external as well as internal misuse.

An IDS operates continuously on the system, running in the background and notifying administrators when it detects a perceived threat. Broad categories of IDSs include:

- **Network-based IDSs**—They identify attacks within the monitored network and issue a warning to the operator. If a network-based IDS is placed between the Internet and the firewall, it will detect all the attack attempts, whether or not they enter the firewall. If the IDS is placed between a firewall and the corporate network, it will detect those attacks that enter the firewall (it will detect intruders). The IDS is not a substitute for a firewall, but it complements the function of a firewall.
- **Host-based IDSs**—They are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack. They can detect the modification of executable programs, detect the deletion of files and issue a warning when an attempt is made to use a privileged command.

Components of an IDS are:

- Sensors that are responsible for collecting data. The data can be in the form of network packets, log files, system call traces, etc.
- Analyzers that receive input from sensors and determine intrusive activity
- An administration console
- A user interface

Types of IDSs include:

- **Signature-based**—These IDS systems protect against detected intrusion patterns. The intrusive patterns they can identify are stored in the form of signatures.
- **Statistical-based**—These systems need a comprehensive definition of the known and expected behavior of systems.
- **Neural networks**—An IDS with this feature monitors the general patterns of activity and traffic on the network, and creates a database. This is similar to the statistical model but with added self-learning functionality.

Signature-based IDSs will not be able to detect all types of intrusions due to the limitations of the detection rules. On the other hand, statistical-based systems may report many events outside of the defined normal activity but which are normal activities on the network. A combination of signature- and statistical-based models provides better protection.

FEATURES
The features available in an IDS include:
- Intrusion detection
- Gathering evidence on intrusive activity
- Automated response (i.e., termination of connection, alarm messaging)
- Security policy
- Interface with system tools
- Security policy management

LIMITATIONS
An IDS cannot help with the following weaknesses:
- Weaknesses in the policy definition
- Application-level vulnerabilities
- Back doors into applications
- Weaknesses in identification and authentication schemes

In contrast to IDSs, which rely on signature files to identify an attack as (or after) it happens, an intrusion prevention system (IPS) predicts an attack before it can take effect. It does this by monitoring key areas of a computer system, and looks for "bad behavior" such as worms, Trojans, spyware, malware and hackers. It complements firewall, antivirus and antispyware tools to provide complete protection from emerging threats. It is able to block new (zero-day) threats that bypass traditional security measures since it is not reliant on identifying and distributing threat signatures or patches. The above is taken from ISACA Guideline G33 General Considerations on the Use of the Internet, Section 3.5.2.

Intrusion Prevention Systems
Intrusion prevention systems (IPSs) are closely related to IDSs and are designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks. If a malicious program contains commands that, when executed, cause a system to delete all of the files in a system directory, an IPS needs to prevent this from happening. The intrusion prevention approach appears to be effective in limiting damage or disruption to systems that are attacked. However, as with an IDS, the IPS must be properly configured and tuned to be effective. Threshold settings that are too high or low will lead to limited effectiveness of the IPS. Additionally, some concerns have been raised that IPSs may in themselves constitute a threat since a clever attacker could send commands to a large number of hosts protected by an IPS in order to cause them to become dysfunctional. Such a situation would be a potentially catastrophic outcome in today's typical corporate computing environment in which continuity of service is so critical.

Honeypots and Honeynets
A honeypot is a software application that pretends to be an unfortunate server on the Internet and is not set up to actively protect against break-ins. Rather, it acts as a decoy system that lures hackers and, therefore, is attractive to hackers. The more a honeypot is targeted by an intruder, the more valuable it becomes. Although honeypots are technically related to intrusion detection systems and firewalls, they have no real production value as an active sentinel of networks.

There are two basic types of honeypots:
- **High-interaction**—Essentially give hackers a real environment to attack
- **Low-interaction**—Emulate production environments and, therefore, provide more limited information

A honeynet is multiple honeypots networked together to simulate a larger network installation, as part of an architecture to let hackers break into the false network while allowing investigators to watch their every move by a combination of surveillance technologies.

An IDS triggers a virtual alarm whenever an attacker breaches security of any networked computers. A stealthy keystroke logger watches everything the intruder types. A separate firewall cuts off the machines from the Internet anytime an intruder tries to attack another system from the honeynet.

All traffic on honeypots or honeynets are assumed to be suspicious because the systems are not meant for internal use and the information collected about these attacks are used proactively to update vulnerabilities on a company's live network.

Eventually, the honeynet—the concept expanded from the honeypot—could become an important part of network security.

If a honeypot is designed to be accessible from the Internet, there is a risk that external monitoring services that create lists of untrusted sites may report the organization's system as vulnerable, without knowing that the vulnerabilities belong to the honeypot and not to the system itself. Such independent reviews made public can affect the organization's reputation. Therefore, prior to implementing a honeypot in the network, careful judgment should be exercised.

5.4.5 ENCRYPTION
Encryption is the process of converting a plaintext message into a secure-coded form of text, called ciphertext, which cannot be understood without converting back, via decryption (the reverse process), to plaintext. This is done via a mathematical function and a special encryption/decryption password called the key. In many countries, encryption is subject to governmental laws and regulations.

Encryption generally is used to:
- Protect data in transit over networks from unauthorized interception and manipulation
- Protect information stored on computers from unauthorized viewing and manipulation
- Deter and detect accidental or intentional alterations of data
- Verify authenticity of a transaction or document

Encryption is limited in that it cannot prevent the loss or modification of data, and it is possible to compromise encryption programs if encryption keys are not protected adequately. Therefore, encryption should be regarded as an essential, but incomplete, form of access control that should be incorporated into an organization's overall computer security program.

Key Elements of Encryption Systems

Key elements of encryption systems include:

- **Encryption algorithm**—A mathematically based function or calculation that encrypts/decrypts data
- **Encryption keys**—A piece of information that is used within an encryption algorithm (calculation) to make the encryption or decryption process unique. Similar to passwords, a user needs to use the correct key to access or decipher a message. The wrong key will decipher the message into an unreadable form.
- **Key length**—A predetermined length for the key. The longer the key, the more difficult it is to compromise in a brute-force attack where all possible key combinations are tried.

Effective encryption systems depend upon algorithm strength, secrecy and difficulty of compromising a key, the nonexistence of back doors by which an encrypted file can be decrypted without knowing the key, the inability to decrypt an entire ciphertext message if the way a portion of it decrypts is known (called a known-text attack), and the properties of the plaintext known by a perpetrator.

There are two types of cryptographic systems: the symmetric and the asymmetric key systems. Symmetric key systems use single, secret, bidirectional (encrypt/decrypt) keys. Asymmetric key systems use pairs of unidirectional (only encrypt or decrypt), complementary keys, one of which is usually secret and the other publicly known. Public key systems are asymmetric encryption systems.

Most encrypted transactions over the Internet use a combination of private/public keys, secret keys, hash functions (fixed values derived mathematically from a text message) and digital certificates to achieve confidentiality, message integrity, authentication and nonrepudiation by either sender or recipient (also known as a PKI). This encryption process allows data to be stored and transported with reduced exposure so a company's corporate data are secure as they move across the Internet or other networks.

Symmetric Key Cryptographic Systems

Symmetric key cryptographic systems are based on a symmetric encryption algorithm, which uses a secret key to encrypt the plaintext to the ciphertext and the same key to decrypt the ciphertext to the corresponding plaintext. In this case, the key is said to be symmetric because the encryption key is the same as the decryption key.

The most common symmetric key cryptographic system is the Data Encryption Standard (DES). DES is based on a public algorithm that operates on plaintext in blocks (strings or groups) of bits. This type of algorithm is known as a block cipher. DES uses blocks of 64 bits. A key of 56 bits is used for the encryption and decryption of plaintext. An additional 8 bits are used for parity checking. Any 56-bit number can be used as a key and there are 72,057,594,037,927,936 possible keys in the key space.

DES is no longer considered a strong cryptographic solution since its entire key space can be brute-forced (every possible key tried) by large computer systems within a relatively short period of time. In this regard, private key cryptographic spaces of symmetric keys are susceptible to compromise. DES is being replaced with AES, a public algorithm that supports keys from 128 bits to 256 bits in size.

There are two main advantages to symmetric key cryptosystems such as DES or AES. The first is that the user has to remember/know only one key for both encryption and decryption. The second is that symmetric key cryptosystems are generally less complicated and, therefore, use up less processing power than asymmetric techniques. This makes symmetric key cryptosystems ideally suited for bulk data encryption. The major disadvantage of this approach is how to get the keys into the hands of those with whom you want to exchange data, particularly in e-commerce environments where customers are unknown, untrusted entities. Also, a symmetric key cannot be used to sign electronic documents or messages due to the fact that the mechanism is based on a shared secret.

Public (Asymmetric) Key Cryptographic Systems

Public key cryptographic systems developed for key distribution solve the problem of getting single symmetric keys into the hands of two people who do not know each other, but who want to exchange information in a secure manner. Based on an asymmetric encryption process, two keys work together as a pair. One key is used to encrypt data, the other is used to decrypt data. Either key can be used to encrypt or decrypt, but once the key has been used to encrypt data, only its partner can be used to decrypt the data (even the key that was used to encrypt the data cannot be used to decrypt it).

The keys are asymmetric in that they are inversely related to each other. Based on mathematical integer factorization, the idea of implementation of the original asymmetric keys is to generate a single product from two large prime numbers, where it is impractical to factor the number and recover the two factors. This integer factorization process forms the basis for public key cryptography (i.e., function easy to compute in one direction, but very difficult or impractical in the other). The system involves modular arithmetic, exponentiation, and large prime numbers thousands of bits long. Asymmetric keys are often used for short messages such as encrypting DES symmetric keys or creating digital signatures. If asymmetric keys were used to encrypt bulk data (long messages), the process would be very slow; this is the reason they are used to encrypt short messages such as digests or signatures.

A common form of asymmetric encryption is RSA. RSA is a public key cryptosystem for encryption and authentication; it was invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA stands for the initials of their last names).

It works as follows: take two large primes randomly generated, p and q, and find their product n = pq; n is called the modulus. Choose a number, e, less than n and relatively prime to (p minus 1)(q minus 1), which means that e and (p minus 1)(q minus 1) have no common factors except 1. Find another number, d, such that (ed minus 1) is divisible by (p minus 1)(q minus 1). The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is (n, d). The factors p and q may be kept with the private key, or destroyed.

It is extremely unlikely that one could obtain the private key d from the public key (n, e). If one could factor n into p and q, however, then one could obtain the private key d. Thus, the security of RSA is related to the assumption that factoring is difficult.

With asymmetric encryption, one key—the secret or private key—is known only to one person; the other key—the public key—is known by many people. In other words, a message that has been sent encrypted by the secret (private) key of the sender can be deciphered by anyone with the corresponding public key. In this way, if the public key deciphers the message satisfactorily, one can be sure of the origin of the message because only the sender (owner of the correspondent private key) could have encrypted the message. This forms the basis of authentication and nonrepudiation (i.e., the sender cannot later claim that he/she did not generate the message). A message that has been sent encrypted using the public key of the receiver can be generated by anyone, but can only be read by the receiver. This is one basis of confidentiality. In theory, a message that has been encrypted twice, first, by the sender's secret key and, second, by the receiver's public key, achieves both authentication and confidentiality objectives, but it is not commonly used because it could generate performance issues.

Elliptical Curve Cryptography

A variant and more efficient form of public key cryptography (how to manage more security out of minimum resources) gaining prominence is the elliptical curve cryptography (ECC). ECCs work well on networked computers requiring strong cryptography but have some limitations such as bandwidth and processing power. This is even more important with devices such as smart cards, wireless phones and other mobile devices.

As explained earlier, under public key cryptography, a person makes one key publicly available and holds a second, private key. A message is encrypted with the public key, sent and decrypted with the private key. Such systems depend mostly on long key sizes and complex mathematical problems to ensure security. But now cryptographers are looking to a mathematical system known as an elliptical curve to solve the efficiency riddle. It is believed that ECC demands less computational power and, therefore, offers more security per bit. For example, an ECC with a 160-bit key offers the same security as an RSA-based system with a 1,024-bit key.

Quantum Cryptography

Quantum cryptography is the next generation of cryptography that may solve some of the existing problems associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. Initial commercial usage has already started now that the laboratory research phase has been completed. Quantum cryptography is based on a practical application of the characteristics of the smallest "grains" of light, the photons, and on the physical laws governing their generation, propagation and detection.

Advanced Encryption Standard

AES has replaced the DES as the cryptographic algorithm standard. Due to its short key length, the former standard for symmetric encryption—DES—reached the end of its life cycle. Secure applications need a new standard for symmetric encryption.

In 1997, NIST announced the initiation of the AES development effort and made a formal call for algorithms. On 2 October 2000, NIST announced that it had selected Rijndael to propose the algorithm for the AES. This algorithm was developed by Dr. Joan Daemen and Dr. Vincent Rijmen. Because AES was to replace DES, it was easy to see that a lot of existing and future applications and protocols would use this algorithm for secure information exchange.

Rijndael is a symmetric block cipher with variable block and key length. For AES the block length was fixed to 128 bits and three different key sizes (128, 192 and 256 bits) were specified. Therefore, AES-128, AES-192 and AES-256 are three different versions of AES. The cipher is based on round operations. Each round has a 128-bit round key and the result of the previous round as input. The round keys can be precomputed or generated out of the input key. Due to its regular structure, it can be implemented efficiently in hardware. Decryption is computed by applying inverse functions of the round operations. The sequence of operations for the round function differs from encryption which often results in separated encryption and decryption circuits. Computational performance of software implementations often differ between encryption and decryption because the inverse operations in the round function are more complex than the respective operation for encryption.

Digital Signatures

A digital signature is an electronic identification of a person or entity created by using a public key algorithm and intended to verify to a recipient the integrity of the data and the identity of the sender. To verify the integrity of the data, a cryptographic hashing algorithm is computed against the entire message or electronic document, which generates a small fixed string message, in general, usually about 128 bits in length. This process, also referred to as a digital signature algorithm, creates a message digest (i.e., smaller extrapolated version of the original message).

Common types of message digest algorithms are SHA1, MD2, MD4 and MD5. These algorithms are one-way functions unlike private and public key encryption algorithms. The process of creating message digests cannot be reversed. They are meant for digital signature applications where a large electronic document or string of characters, such as word processor text, a spreadsheet, a database record, the content of a hard disk or a jpg image, has to be compressed in a secure manner before being signed with the private key. All digest algorithms take a message of arbitrary length and produce a 128-bit message digest. While the structures of these algorithms are somewhat similar, the design of MD2 is quite different from that of MD4 and MD5. MD2 was optimized for 8-bit machines, whereas MD4 and MD5 were created for 32-bit machines. Descriptions and source code for the three algorithms can be found as Internet RFCs 1319-1321.

Note: The IS auditor needs to be familiar with how a digital signature functions to protect data. The specific types of message digest algorithms are not tested on the CISA exam.

The next step, which verifies the identity of the sender, is to encrypt the message digest using the sender's private key, which "signs" the document with the sender's digital signature for message authenticity. To decipher, the receiver would use the sender's public key, proving that the message could only have come from the sender. This process of sender authentication is known as nonrepudiation because the sender cannot later claim that they did not generate the message.

Once decrypted, the receiver will recompute the hash using the same hashing algorithm on the electronic document and compare the results with what was sent, to ensure the integrity of the message. Therefore, digital signature is a cryptographic method that ensures:

- **Data integrity**—Any change to the plaintext message would result in the recipient failing to compute the same message hash.
- **Authentication**—The recipient can ensure that the message has been sent by the claimed sender since only the claimed sender has the secret key.
- **Nonrepudiation**—The claimed sender cannot later deny generating and sending the message.

Replay protection is not ensured by signing an electronic document using a cryptographic technique. A timestamp is used to date a document and the document hash could be used to uniquely identify or number the document. The timestamp or the hashing of the document could provide replay protection or warranties.

However, digital signatures and public key encryption are vulnerable to man-in-the-middle attacks wherein the sender's digital signature private key and public key may be faked. To protect against such attacks, an independent sender authentication authority has been designed. The public key infrastructure performs the function of independently authenticating the validity of senders' digital signatures and public keys.

Digital Envelope

A digital envelope is used to send encrypted information, using symmetric keys, and the relevant key session along with it. It is a secure method to send electronic documents without compromising the data integrity, authentication and nonrepudiation, which were obtained with the use of asymmetric keys.

The (original plaintext) message to be sent can be encrypted by using either an asymmetric key or a symmetric key. The disadvantage in using an asymmetric key is that it takes much longer to encrypt/decrypt than a symmetric key, with the resultant performance reduction explained in the section on public key cryptographic systems. If a message is short, the time taken is not an issue. When using an asymmetric key with a longer message, memory requirements are much greater and, consequently, the message takes longer to receive, which is one of the reasons it is not generally used.

A digital envelope mechanism works as follows: the symmetric key, which is used to encrypt the message (e.g., plaintext alone or plaintext plus signature), can be referred to as the session key. If the session key is sent to the receiver in cleartext, anyone can access the session key in transit and confidentiality can easily be compromised. Therefore, it is critical that the session key be encrypted before sending it to the receiver. The session key is encrypted using the receiver's public key.

The encrypted message and the encrypted session key are sent to the receiver who, in turn, opens the session key with the receiver's private key (to ensure authentication of sender and integrity of session key). The session key is then applied to the message to get it in plaintext. The process of encrypting the bulk data using symmetric key cryptography and encrypting the symmetric key with a public key algorithm is referred to as a digital envelope.

Public Key Infrastructure

If an individual wants to send messages or electronic documents and sign them with a digital signature using a public key cryptographic system, how does the individual distribute the public key in a secure way? If the public key is distributed electronically, then it could be intercepted and changed. To prevent this from occurring, a framework needs to be established to issue, maintain and revoke public key certificates by a trusted party. This framework is known as a PKI.

PKI allows users to interact with other users and applications, and obtain and verify identities and keys from trusted sources. The actual implementation of PKI varies according to specific requirements. Key elements of the infrastructure are as follows:

- **Digital certificates**—A digital credential is composed of a public key and identifying information about the owner of the public key. The purpose of digital certificates is to associate a public key with the individual's identity. These certificates are electronic documents, digitally signed by some trusted entity with its private key (transparent to users), that contains information about the individual and his/her public key.

  The process involves proving the sender's authenticity. When a person digitally signs a document, that person attaches a digital certificate issued by a trusted entity. The receiver of the message and accompanying digital certificate relies on the public key of the trusted third-party certificate authority (that is included with the digital certificate or obtained separately) to authenticate the message. The receiver can link the message to a person, not simply to a public key, because of their trust in this third party.

  The status and values of a current user's certificate should include a distinguishing username, an actual public key, the algorithm used to compute the digital signature inside the certificate and a certificate validity period.
- **Certificate authority**—A CA is an authority in a network that issues and manages security credentials and public keys for message signature verification or encryption. The CA attests, to the authenticity of the owner (entity or individual) of a public key. The process involves a CA who makes a decision to issue a certificate based on evidence or knowledge obtained in verifying the identity of the recipient. As part of a PKI, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Upon verifying the identity of the recipient, the CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will verify the certificate signature with the CA's public key (e.g., commercial CAs such as Verisign

issue certificates through web browsers). The ideal CA is authoritative (someone that the user trusts) for the name or key space it represents. A certificate always includes the owner's public key, expiration date and the owner's information.

Types of CAs may include:
- Organizationally empowered, which have authoritative control over those individuals in their name space
- Liability empowered, for example, choosing commercially available options (such as Verisign, Certco., Cybertrust, etc.) in obtaining a digital certificate

The CA is responsible for managing the certificate throughout its life cycle. Key elements or subcomponents of the CA structure include the certification practice statement (CPS), RAs and certificate revocation lists (CRLs).

- **Registration authority**—An RA is an authority in a network that verifies user requests for a digital certificate and tells the CA to issue it. An optional entity separate from a CA, an RA would be used by a CA with a very large customer base. CAs use RAs to delegate some of the administrative functions associated with recording or verifying some or all of the information needed by a CA to issue certificates or CRLs and to perform other certificate management functions. However, with this arrangement, the CA still retains sole responsibility for signing either digital certificates or CRLs. RAs are part of a PKI. The digital certificate contains a public key that is used to encrypt messages and verify digital signatures. If an RA is not present in the PKI structure established, the CA is assumed to have the same set of capabilities as those defined for an RA.

  The administrative functions that a particular RA implements will vary based on the needs of the CA, but must support the principle of establishing or verifying the identity of the subscriber. These functions may include the following:
  - Verifying information supplied by the subject (personal authentication functions)
  - Verifying the right of the subject to requested certificate attributes
  - Verifying that the subject actually possesses the private key being registered and that it matches the public key requested for a certificate. This is generally referred to as proof of possession (POP).
  - Reporting key compromise or termination cases where revocation is required
  - Assigning names for identification purposes
  - Generating shared secrets for use during the initialization and certificate pick-up phases of registration
  - Initiating the registration process with the CA on behalf of the subject end entity
  - Initiating the key recovery processing
  - Distributing the physical tokens (such as smart cards) containing the private keys
- **Certificate revocation list**—The CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. The CRL details digital certificates that are no longer valid because they were revoked by the CA. The time gap between two updates is critical and is also a risk in digital certificates verification.
- **Certification practice statement**—CPS is a detailed set of rules governing the certificate authority's operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA in terms of the controls that an organization observes, the method it uses to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used.

Applications of Cryptographic Systems

The use of cryptosystems by applications, for example, in e-mail and Internet transactions generally involves a combination of private/public key pairs, secret keys, hash functions and digital certificates. The purpose of applying these combinations is to achieve confidentiality, message integrity or nonrepudiation by either the sender or recipient. The process generally involves the sender hashing the message into a message digest or prehash code for message integrity, which is encrypted using the sender's private key for authenticity, integrity and nonrepudiation (i.e., digital signature). Using his/her secret key, the sender then will encrypt the message. Afterward, the secret key is encrypted with the recipient's public key, which has been validated through the recipient's digital certificate and provides message confidentiality.

The process on the receiving end reverses what has been done by the sender. The recipient uses his/her private key to decrypt the sender's secret key. He/she uses this secret key to decrypt the message, to expose it. If the prehash code has been encrypted with the sender's private key, the recipient verifies its authenticity using the public key contained in the sender's digital certificate and decrypts the prehash code, which provides the nonrepudiation to the recipient of the sender's message. For integrity purposes, the recipient calculates a posthash code, which should equal the prehash code.

Specific examples of this method or related variants are described below:

- **Secure Sockets Layer (SSL) and Transport Layer Security (TLS)**—These are cryptographic protocols which provide secure communications on the Internet. There are only slight differences between SSL 3.0 (the latest version) and TLS 1.0, but they are not interchangeable. For general concepts, both are called SSL. SSL is a session- or connection-layered protocol widely used on the Internet for communication between browsers and web servers, where any amount of data is securely transmitted while a session is established.

  SSL provides end point authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated while the client remains unauthenticated. Mutual authentication requires PKI deployment to clients. The protocols allow client-server applications to communicate in a way designed to prevent eavesdropping, tampering and message forgery.

  SSL involves a number of basic phases:
  - Peer negotiation for algorithm support
  - Public-key, encryption-based key exchange and certificate-based authentication
  - Symmetric cipher-based traffic encryption

During the first phase, the client and server negotiate which cryptographic algorithms will be used. Current implementations support the following choices:
– For public-key cryptography: RSA, Diffie-Hellman, DSA or Fortezza
– For symmetric ciphers: RC2, RC4, IDEA, DES, Triple DES or AES
– For one-way hash functions: MD5 or SHA-1 or SHA-256

SSL runs on layers beneath application protocols such as HTTP, SMTP and Network News Transfer Protocol (NNTP) and above the TCP transport protocol, which forms part of the TCP/IP suite. While SSL can add security to any protocol that uses TCP, it is most commonly used with HTTP to form Secured Hypertext Transmission Protocol (HTTPS). HTTPS serves to secure World Wide Web pages for applications such as electronic commerce. HTTPS uses public key certificates to verify the identity of endpoints.

SSL uses a hybrid of hashed, private and public key cryptographic processes to secure transactions over the Internet through a PKI. This provides the necessary confidentiality, integrity, authenticity and nonrepudiation features needed for e-commerce transactions over the Internet. SSL can be characterized as a two-way SSL process, for example for B-to-B e-commerce activities. It also is commonly associated as a one-way consumer process, whereby a retail customer over an Internet retail virtual store can verify, through a CA, the authenticity of an e-store's public key, which can then subsequently be used to negotiate a secure transaction.

The SSL provides for:
– Confidentiality
– Integrity
– Authentication, e.g., between client and server
– Nonrepudiation

The SSL handshake protocol is based on the application layer but provides for the security of the communication sessions, too. It negotiates the security parameters for each communication section. Multiple connections can belong to one SSL session and the parties participating in one session can take part in multiple simultaneous sessions.

- **Secure Hypertext Transfer Protocol (S/HTTP)**—As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing an SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than as a session-oriented protocol.
- **IPSec**—IPSec is used for communication among two or more hosts, two or more subnets, or hosts and subnets.

This IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods. For the transport method, the data portion of each packet referred to as the encapsulation security payload (ESP) is encrypted, achieving confidentiality over the process. In the tunnel mode, the ESP payload and its header are encrypted. To achieve nonrepudiation, an additional authentication header (AH) is applied.
In establishing IPSec sessions in either mode, security associations (SAs) are established. SAs define which security parameters should be applied between the communicating parties as encryption algorithms, keys, initialization vectors, life span of keys, etc. Within either the ESP or AH header, respectively, an SA is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is a unique identifier that enables the sending host to reference the security parameters to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and those of the cryptographic keys.

- **SSH**—A client-server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data, including passwords, binary files and administrative commands, transmitted between systems on a network. SSH is typically implemented between two parties by validating each other's credentials via digital certificates. SSH is useful in securing Telnet and FTP services, and is implemented at the application layer, as opposed to operating at the network layer (IPSec implementation).
- **Secure Multipurpose Internet Mail Extensions (S/MIME)**—A standard secure e-mail protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of a message's contents, including attachments
- **Secure Electronic Transactions (SET)**—SET is a protocol developed jointly by VISA and Master Card to secure payment transactions among all parties involved in credit card transactions on behalf of cardholders and merchants. As an open system specification, SET is an application-oriented protocol that uses trusted third parties' encryption and digital signature processes, via a PKI infrastructure of trusted third-party institutions, to address confidentiality of information, integrity of data, cardholder authentication, merchant authentication and interoperability.

Encryption Risks and Password Protection

The security of encryption methods relies mainly on the secrecy of keys. In general, the more a key is used, the more vulnerable it is to compromise. For example, password cracking tools for today's microcomputers can brute-force every possible key combination for a cryptographic hashing algorithm with a 40-bit key in a matter of a few hours.

The randomness of key generation is also a significant factor in the ability to compromise a key. When passwords are tied into key generation, the strength of the encryption algorithm is diminished, particularly when common words are used. This significantly lessens the key space combinations to search for the key (e.g., an eight-character password is comparable to a 32-bit

key). Therefore, a 128-bit encryption algorithm's capabilities are diminished when encrypting keys based on passwords, and the passwords lack randomness. Therefore, it is important that effective password syntax rules are applied, and easily guessed passwords are prohibited.

5.4.6 VIRUSES

The term virus is a generic term applied to a variety of malicious computer programs that send out requests to the operating system of the host system under attack to append the virus to other programs. In this way, viruses are self-propagating to other programs. They can be relatively benign (e.g., web application defacement) or malicious (e.g., deleting files, corrupting programs or causing a denial of service). Generally, viruses attack four parts of the computer:

- Executable program files
- The file-directory system, which tracks the location of all the computer's files
- Boot and system areas, which are needed to start the computer
- Data files

Another variant of a virus frequently encountered is a worm, which, unlike a virus, does not physically attach itself to another program. To propagate itself to the host systems, a worm typically exploits security weaknesses in operating systems' configurations. These problems are particularly severe in today's highly decentralized client-server environments.

Today, viruses or worms are transmitted easily from the Internet by downloading files to computers' web browsers. Viruses are also transmitted as attachments to e-mail, so that when word processing software opens the attachment, the system becomes infected if it is not using scanning software to review unopened attachments. Other methods of infection occur from files received through online services, computer bulletin board systems, LANs and even shrink-wrapped software that the user may buy from a retail store.

Virus and Worm Controls

To effectively reduce the risk of computer viruses and worms infiltrating an organization, a comprehensive and dynamic antivirus program needs to be established. There are two major ways to prevent and detect viruses and worms that infect computers and network systems. The first is by having sound policies and procedures in place (preventive controls) and the second is by technical means (detective controls), including antivirus software. Neither is effective without the other.

Management Procedural Controls

Some of the policy and procedure controls that should be in place are:

- Build any system from original, clean master copies. Boot only from original media whose write protection has always been in place, if applicable.
- Allow no disk or other kind of media, such as miniature hard/flash drives which simply plug into the USB port, to be used until it has been scanned on a stand-alone machine that is used for no other purpose and is not connected to the network.
- Update virus software scanning definitions/signatures frequently.
- Write-protect all diskettes.
- Have vendors run demonstrations on their machines.
- Enforce a rule of not using shareware without first scanning the shareware thoroughly for a virus.
- Scan before any new software is installed since commercial software occasionally is supplied with a Trojan horse (viruses or worms).
- Insist that field technicians scan their disks on a test machine before they use any of their disks on the system.
- Ensure the network administrator uses workstation and server antivirus software.
- Ensure all servers are equipped with an activated current release of the virus-detection software.
- Consider encrypting files and then decrypting them before execution.
- Ensure bridge, router and gateway updates are authentic.
- Because backups are a vital element of an antivirus strategy, ensure a sound and effective backup plan is in place. This plan should account for scanning selected backup files for virus infection once a virus has been detected.
- Educate users so they will heed these policies and procedures. For example, many viruses and worms today are propagated in the form of e-mail attachments where the attachment, such as an executable Visual Basic script, infects the user's system upon opening the attachment. The hacker relies upon social engineering tactics in getting the user to open the attachment (e.g., "Love" viruses).
- Review antivirus policies and procedures at least once a year.
- Prepare a virus eradication procedure and identify a contact person.

Technical Controls

Technical methods of preventing viruses can be implemented through hardware and software means. The following are hardware tactics that can reduce the risk of infection:

- Use boot virus protection (i.e., built-in, firmware-based virus protection).
- Use remote booting (e.g., diskless workstations).
- Use a hardware-based password.
- Use write-protected tabs on diskettes.
- Ensure that insecure protocols are blocked by the firewall from external segments and the Internet.

However, antivirus software is, by far, the most common antivirus tool and is considered the most effective means of protecting networks and host-based computer systems against viruses. Antivirus software is both a preventive and a detective control. Unless updated periodically, antivirus software will not be an effective tool against viruses.

Antivirus software contains a number of components that address the detection of viruses via scanning technologies from different angles. There are different types of antivirus software:

- **Scanners**—Look for sequences of bits called signatures that are typical of virus programs. The two primary types are:
  - **Virus masks or signatures**—Antivirus scanners check files, sectors and system memory for known and new (unknown to scanner) viruses, on the basis of virus masks or signatures. Virus masks or signatures are specific code strings that are recognized as belonging to a virus. For polymorphic viruses, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

– **Heuristic scanners**—Analyzes the instructions in the code being scanned and decides on the basis of statistical probability whether it could contain malicious code. Heuristic scanning results could indicate that a virus may be present, i.e., possibly infected. Heuristic scanners tend to generate a high level of false-positive errors (i.e., they indicate that a virus may be present when, in fact, no virus is present).

  Scanners examine memory, disk-boot sectors, executables, data files and command files for bit patterns that match a known virus. Scanners, therefore, need to be updated periodically to remain effective.

- **Active monitors**—Interpret DOS and read-only memory (ROM) BIOS calls, looking for virus-like actions. Active monitors can be problematic because they cannot distinguish between a user request and a program or virus request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.
- **Integrity CRC checkers**—Compute a binary number on a known virus-free program that is then stored in a database file. The number is called a cyclical redundancy check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the files as compared to the database and reports possible infection if changes have occurred. A match means no infection; a mismatch means a change in the program has occurred. A change in the program could mean a virus within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred, i.e., it is often too late to save files. Also, CRC checkers can only detect subsequent changes to files, because they assume files are virus free in the first place. Therefore, they are ineffective against new files that are virus-infected and that are not recorded in the database. Integrity checkers take advantage of the fact that executable programs and boot sectors do not change often, if at all.
- **Behavior blockers**—Focus on detecting potentially abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect a virus at an early stage. Most hardware-based antivirus mechanisms are based on this concept.
- **Immunizers**—Defend against viruses by appending sections of themselves to files—somewhat in the same way that file viruses append themselves. Immunizers continuously check the file for changes and report changes as possible viral behavior. Other types of immunizers are focused to a specific virus and work by giving the virus the impression that the virus has already infected the computer. This method is not always practical since it is not possible to immunize files against all known viruses.

Once a virus has been detected by antivirus software, an eradication program can be used to wipe the virus from the hard disk. Sometimes eradication programs can kill the virus without having to delete the infected program or data file, while other times those infected files must be deleted. Still, other programs, sometimes called inoculators, do not allow a program to be run if it contains a virus.

Antivirus Software Implementation Strategies

Organizations have to develop virus implementation strategies to effectively control and prevent the spread of viruses throughout their IS infrastructure. An important means of controlling the spread of viruses is to detect the virus at its point of entry—before it has the opportunity to cause damage. This includes everything from networks, server platforms and end-user workstations.

The user server or workstation level could include screening of software and data as they enter the machine, where antivirus programs can be set to perform:

- Scheduled virus scans (daily, weekly, etc.)
- Manual/on-demand scans, where the virus scan is requested by the user
- Continuous/on-the-fly scanning, where files are scanned as they are processed

At the corporate network level, in cases of interconnected networks, virus scanning software is used as an integral part of firewall technologies, referred to as virus walls. Virus walls scan incoming traffic with the intent of detecting and removing viruses before they enter the protected network. Virus walls normally work at the following levels:

- SMTP protection, to scan inbound and outbound SMTP traffic for viruses in coordination with the mail server
- HTTP protection, to prevent virus-infected files from being downloaded and to offer protection against malicious Java and ActiveX programs
- FTP protection, to prevent infected files from being downloaded

Virus walls most often are updated automatically with new virus signatures by their vendors on a scheduled basis or on an as-needed basis when dangerous, new virus strains emerge. Virus walls also provide facilities to log virus incidents and deal with the incident in accordance with preset rules. The presence of virus walls does not preclude the necessity for virus-detection software to be installed on computers within a network because the virus wall only addresses one channel through which viruses enter the network. Virus-detection software should be loaded on all computers within the network. Virus signature files should be kept updated. The facility of automatic "live update" has become fairly popular and allows organizations to update the virus scanner signature files as soon as updates are available.

For virus scanners to be acceptable and viable, they should have the following features:

- Reliability and quality in the detection of viruses
- Memory resident, which is a continuous checking facility
- Efficiency, such as a reasonable working speed and usage of resources

5.4.7 VOICE-OVER IP

IP telephony, also known as Internet telephony, is the technology that makes it possible to have a voice conversation over the Internet or over any dedicated IP network instead of dedicated voice transmission lines. The protocols used to carry the signal over the IP network are commonly referred to as Voice-over IP (VoIP). VoIP is a technology where voice traffic is carried on top of existing data infrastructure. Sounds are digitized into IP packets and transferred through the network layer before being

decoded back into the original voice. VoIP has significantly reduced long-distance costs in a number of large organizations.

VoIP allows the elimination of circuit switching and the associated waste of bandwidth. Instead, packet switching is used, where IP packets with voice data are sent over the network only when data needs to be sent.

It has advantages over traditional telephony:
- Unlike traditional telephony, VoIP innovation progresses at market rates rather than at the rates of the multilateral committee process of the International Telecommunications Union (ITU)
- Lower costs per call or even free calls, especially for long-distance calls
- Lower infrastructure costs. Once IP infrastructure is installed, no or little additional telephony infrastructure is needed.

VoIP introduces security risks and opportunities. VoIP has a different architecture than traditional circuit-based telephony, and these differences result in significant security issues.

VoIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units and mobile units. In addition to end-user equipment, VoIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls and protocols. Most of these components have counterparts used in data networks, but the performance demands of VoIP mean that ordinary network software and hardware must be supplemented with special VoIP components.

When designing a VoIP system, the backup has to be considered. While telecom companies usually operate under the requirement to have 99.9999 percent uptime, data traffic normally has less reliability. For this reason, the backup has to be designed to ensure that communication will not be interrupted should undesirable events occur on the data backbone. Bandwidth capacity should be baselined to determine the current levels of data traffic and adjust the necessary additional bandwidth for voice traffic. Quality of service will need to be defined so that voice traffic will be given priority over data traffic. Other considerations are laws and regulations. Certain countries may ban the use of VoIP.

VoIP Security Issues

With the introduction of VoIP, the need for security is more important because it is needed to protect two assets—the data and the voice.

Protecting the security of conversations in VoIP is vital now. In a conventional office telephone system, security is a more valid assumption. Intercepting conversations requires physical access to telephone lines or compromise of the office PBX. Only particularly security-sensitive organizations bother to encrypt voice traffic over traditional telephone lines. It cannot be said for Internet-based connections.

In VoIP, packets are sent over the network from a user's computer or VoIP phone to similar equipment on the other end. Packets may pass through several intermediate systems that are not under the control of the user's ISP. The current Internet architecture does not provide the same physical wire security as the phone lines. The key to securing VoIP is to use the security mechanisms such as those deployed in data networks (e.g., firewalls, encryption) to emulate the security level currently used by public switched telephone network (PSTN) network users.

The main concern with VoIP solutions is that while, in the case of traditional telephones, if the system is disrupted, then different sites of the organization could still be reached via telephone. With VoIP, a computer system disruption also terminates the telephone since both are supported by the same devices. In this case, only mobile phones will function. Thus, a backup communications facility should be planned for if the availability of communications is vital to the organization. This would be the case with branches of financial institutions.

Another issue might arise with the fact that IP telephones and their supporting equipment require the same care and maintenance as computer systems do.

Thus, operating system patches and virus signature updates must be promptly applied to prevent a potential system outage. To enhance the protection of the telephone system and data traffic, the VoIP infrastructure should be segregated using virtual local area networks (VLANs). Any connections between these two infrastructures should be protected using firewalls that can interpret VoIP protocols.

In many cases, session border controllers (SBCs) are utilized to provide security features for VoIP traffic similar to that provided by firewalls. SBCs can be configured to filter specific VoIP protocols, monitor for DoS attacks, and provide network address and protocol translation features.

5.4.8 PRIVATE BRANCH EXCHANGE

A private branch exchange (PBX) is a sophisticated computer-based switch that can be thought of as essentially a small, in-house phone company for the organization that operates it. Protection of the PBX is, thus, a high priority. Failure to secure a PBX can result in exposing the organization to toll fraud, theft of proprietary or confidential information, loss of revenue, or legal entanglements.

PBXs have been a part of organizations' communication infrastructures since the early 1920s, originally using analog technology. PBXs of today use digital technology; digital signals are converted to analog for outside calls on the local loop using Plain Old Telephone Service (POTS), which refers to the standard telephone service that most homes use.

Digital PBXs are widespread throughout industry and public organizations, having replaced their analog predecessors. The advent of software-based PBXs has provided a wealth of communications capabilities within these switches. Today, even the most basic PBX systems have a wide range of capabilities that were previously available only in large-scale switches. These new features have opened up many new opportunities for an intruder to attempt to exploit the PBX, particularly by usage of these features for a purpose that was never intended.

Attributes of today's PBXs include:
- More than two telephone trunk (multiple phone) lines that terminate at the PBX
- The use of digital phones that permit integrated voice/data workstations
- Scalable computer-based PBX systems with memory that manages the switching of the calls within the PBX
- Distributed architecture with multiple switches in a hierarchical or meshed configuration with distributed intelligence providing enhanced reliability
- Nonblocking configurations where all attached devices can be engaged in calls simultaneously
- The network of lines within the PBX
- An operator console or switchboard for a human operator

One of the principal purposes of a PBX is to save the cost of requiring a line for each user to the telephone company's central office. Also, it is easier to call someone within a PBX because only three or four digits need to be dialed.

PBX Risks

PBX environments involve many security risks, presented by people both internal and external to the organization. If a PBX is not correctly configured, back doors can be easily established for unauthorized purposes. The threats to PBX telephone systems are many, depending on the goals of these attackers, and include:
- **Theft of service**—Toll fraud, probably the most common of motives for attackers
- **Disclosure of information**—Data disclosed without authorization, either by deliberate action or by accident. Examples include eavesdropping on conversations and unauthorized access to routing and address data.
- **Data modification**—Data altered in some meaningful way by reordering, deleting or modifying it. For example, an intruder may change billing information or modify system tables to gain additional services.
- **Unauthorized access**—Actions that permit an unauthorized user to gain access to system resources or privileges
- **Denial of service**—Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.
- **Traffic analysis**—A form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences, e.g., from the source and destination numbers or frequency and length of the messages. For example, an intruder observes a high volume of calls between a company's legal department and patent office, and concludes that a patent is being filed.

PBXs are sophisticated computer systems, and many of the threats and vulnerabilities associated with operating systems are shared by PBXs. But there are two important ways in which PBX security is different from conventional OS security:
- **External access/control**—As with larger telephone switches, PBXs typically require remote maintenance by the vendor. Instead of relying on local administrators to make OS updates and patches, organizations normally have updates installed remotely by the switch manufacturer. This, of course, requires remote maintenance ports and access to the switch by a potentially large pool of outside parties.
- **Feature richness**—The wide variety of features available on PBXs, particularly administrative features and conference functions, provide the possibility of unexpected attacks. A feature may be used by an attacker in a manner that was not intended by its designers. Features may also interact in unpredictable ways, leading to system compromise, even if each component of the system conforms to its security requirements and the system is operated and administered correctly.

Some additional control weaknesses include:
- Uncontrolled definition of direct inward dial (DID) lines, which would allow an external party to request a dial tone locally, enabling that person to make unauthorized long-distance phone calls
- Lack of system access controls over long-distance phone calls (e.g., default system vendor passwords unchanged, 24/7 availability of PBX lines)
- Lack of blocking controls for long-distance phone calls to particular numbers (e.g., hot numbers, cellular numbers, etc.)
- Lack of control over the numbers destined for fax machines and modems
- Not activating the option to register calls, which enables the use of call-tracking logs

Although most features are common from PBX to PBX, the implementation of these features may vary and the degree of vulnerability, if any, will depend on how each feature is implemented. For example, many PBX vendors have proprietary designs for the Digital Signaling Protocol between the PBX and the user instruments.

Knowing the design implementation will aid in determining if an intruder or an insider have an easy way to exploit weaknesses or normal functions.

PBX Audit

When planning a PBX audit, the type of skills, the number of auditors and the length of time required to perform the audit cannot be determined without a preliminary assessment of the PBX system, since these depend on the size and complexity of the chosen PBX. The type of perceived threat and the seriousness of any discovered vulnerabilities must be decided by the auditor. Consequently, any corrective actions must also be determined based on the cost of the loss compared with the cost of the corrective action.

A list of critical items of PBX structure, usage and setup will be given, together with specific risks and applicable controls.

PBX System Features

Many features sometimes available to the system may be used by phreakers (security crackers) or intruders for illegal purposes, including:
- Eavesdropping on conversations, without the other parties being aware of it
- Eavesdropping on conference calls
- Illegally forwarding calls from specific instruments to remote numbers

Exhibit 5.10—PBX System Features and Risks		
System Feature	**Description**	**Risk**
Automatic call distribution	Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on hold until one becomes available	Tapping and control of traffic
Call forwarding	Allows specifying an alternate number to which calls will be forwarded based on certain conditions	User tracking
Account codes	Used to: • Track calls made by certain people or for certain projects for appropriate billing • Dial-in system access (user dials from outside and gains access to the normal features of the PBX) • Changing the user class of service so a user can access a different set of features (i.e., the override feature)	Fraud, user tracking, nonauthorized features
Access codes	Key for access to specific features from the part of users with simple instruments, i.e., traditional analog phones	Nonauthorized features
Silent monitoring	Silently monitors other calls	Eavesdropping
Conferencing	Allows for conversation among several users	Eavesdropping, by adding unwanted/unknown parties to a conference
Override (Intrude)	Provides for the possibility to break into a busy line to inform another user of an important message	Eavesdropping
Autoanswer	Allows an instrument to automatically go when called—usually gives an audible or visible warning which can easily be turned off.	Gaining information not normally available, for various purposes (i.e., eavesdropping through the automatic answering of an instrument in a conference room)
Tenanting	Limits system user access to only those users who belong to the same tenant group—useful when one company leases out part of its buildings to other companies and tenants share an attendant, trunk lines, etc.	Illegal usage, fraud, eavesdropping
Voice mail	Stores messages centrally and—by using a password—allows for retrieval from inside or outside lines	Disclosure or destruction of all messages of a user when that user's password is known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines
Privacy release	Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.	Eavesdropping
Nonbusy extensions	Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook	Eavesdropping a conference in progress
Diagnostics	Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics.	Fraud and illegal usage
Camp-on or call waiting	When activated, sends a visual or audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call-waiting party.	Making the called individual a party to a conference without knowing it
Dedicated connections	Connections made through the PBX without using the normal dialing sequence. It can be used to create hot-lines between devices, i.e., one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility.	Eavesdropping on a line

- Forwarding a user's instrument to an unused or disabled number, thereby making it unreachable by external calls

PBX System Attacks

PBX system features and capabilities may present significant vulnerabilities. This occurs because, with such a large number of features available, it becomes difficult for the manufacturer to consider all individual risks and the potential problems caused by the manner in which different features may interact. This may result in vulnerabilities that allow an intruder unwanted access to the PBX and its instruments. See **exhibit 5.10**, showing PBX system features and corresponding risks.

Protecting against all of the risks is not easy. Knowing that a given vulnerability, in fact, exists is already a vital indication. A conservative approach of enabling only the needed features is advisable. Following are some controls to minimize PBX system attacks:

- Where possible, configure and secure separate and dedicated administrative ports.
- Control the definition of DID lines to avoid an external party requesting a dial tone locally, disabling that person's ability to make unauthorized long-distance phone calls.
- Establish system access controls over long-distance phone calls (e.g., change default system vendor passwords, limit the 24/7 availability of PBX lines).
- Block controls for long-distance phone calls to particular numbers (e.g., hot numbers, cellular numbers).
- Establish control over the numbers destined for fax machines and modems.
- Activate the option to register calls, enabling the use of call-tracking logs.

Hardware Wiretapping

A PBX's susceptibility to tapping depends on the methods used for communication between the PBX and its attached devices. This communication may include voice, data and signaling information. The signaling information is typically composed of commands to the devices (e.g., turn on indicators, microphones and speakers) and status from the devices (e.g., hook status and keys pressed). Communications methods use analog voice with or without separate control signals, analog voice with inclusive control signals, and digital voice with inclusive control signals.

Tapping or intrusion in the control sequences is possible using various appropriate hardware technologies, which often include device modification.

The following measures provide controls to minimize risks:

- Physical security of the PBX facilities
- Usage of appropriate antitamper devices on critical hardware components

Hardware Conferencing

When implemented in hardware, the conferencing feature may employ a circuit card known as a conference bridge or a signal processor chip. This allows multiple lines to be bridged to create a conference where all parties can both speak and listen. Some PBXs have a mute feature where all parties can hear, but only certain parties can speak. An intruder could try to obtain a connection to the bridge where the conference could be overheard. A hardware modification to the bridge itself may make it possible to cause the output of the bridge available to a specific port. As in device modifications, some additional steps must be taken to receive this information. This may include modifying the database to make the intruder a permanent member of the bridge so any conference on that bridge could be overheard.

The following measures provide controls to minimize risks:

- Establish a strong physical security to prevent unauthorized access to telephone closets and to the PBX facilities. Whenever possible, the PBX should be kept in a locked room with restricted access.
- Lock critical hardware with antitamper devices.

Remote Access

Remote access is frequently an unavoidable necessity of maintenance, but it can represent a serious vulnerability. The maintenance features may be accessible via a remote terminal with a modem, a system console or other device or over an outside dial-in line. This allows for systems to be located over a large area (perhaps around the world) and have one central location from which maintenance can be performed. Often it is necessary for the switch manufacturer to have remote access to the switch, to install software upgrades or to restart a switch that has experienced service degradation. Dial-back modem usage is a basic precaution, but does not offer full protection. When possible, remote access should be left closed and should be opened only upon need or upon a verified request from the organization that performs the maintenance. It is easy for attackers to contact the switch manufacturer on the pretext of needing help with a particular type of switch, obtain the names of the manufacturer's remote maintenance personnel, and then masquerade as these personnel to obtain access to the victim's switch.

The following measures provide controls to minimize risks:

- A dial-back scheme
- Careful scrutiny and proper authentication of requests to open the remote control

Maintenance

A common maintenance feature is maintenance out of service (MOS). This feature allows maintenance personnel to place a line out of service for maintenance. It is typically used when a problem is detected with a line or when it is desired to disable a line. However, if a line is placed into MOS while it is in operation, the PBX may terminate its signaling communication with the instrument and leave the instrument's voice channel connection active, even after the telephone device is placed on-hook. If the MOS feature were to function in this manner, the potential exists for someone to use the MOS feature to establish a live microphone connection to a user's location without the user's knowledge and, thereby, eavesdrop on the area surrounding the user's telephone.

Another common maintenance feature is the ability to connect two lines together to transmit data from one line to the other and verify whether or not the second line receives the data properly. This feature would allow someone with maintenance access to connect a user's instrument to an instrument at another location

to eavesdrop on the area surrounding the user's telephone without the user's knowledge.

Also, the PBX may support some maintenance features that are not normally accessible to the owner/operator of the PBX for several reasons. These types of utilities vary greatly from one PBX to another, so a general approach to finding them cannot be detailed. Some suggested courses of action to verify the existence of such features are listed below:

- Ask the manufacturer or maintenance company if any such features exist.
- Attempt to learn about undocumented usernames/passwords.
- Attempt to search the system's programmable read-only memory (PROM) or disks for evidence of such features.
- View the system load files with a binary editor to determine whether this reveals the names of undocumented commands among a list of known maintenance commands, which can be recognized in the binaries.
- Verify the existence of alarm features.
- Enable and review usage and intervention logs.

Special Manufacturer's Features

These types of features would most likely be accessible via undocumented username/password access to the maintenance and/or administrative tools. Some possible undocumented features and their associated risks are listed below:

- **Database upload/download utility**—Such a utility allows the manufacturer to download the database from a system that is malfunctioning and examine it at their location to try to determine the cause of the malfunction. It would also allow the manufacturer to upload a new database to a PBX in the event that the database became so corrupted that the system became inoperable. Compromise of such a utility could allow an adversary to download a system's database, insert a Trojan horse or otherwise modify it to allow special features to be made available to the adversary, and upload the modified database back into the system.
- **Database examine/modify utility**—Such a utility allows the manufacturer to remotely examine and modify a system's database to repair damage caused by incorrect configuration, design bugs or tampering. This utility could also provide an intruder with the ability to modify the database to gain access to special features.
- **Software debugger/update utility**—This type of utility gives the manufacturer the ability to remotely debug a malfunctioning system. It also allows the manufacturer to remotely update systems with bug fixes and software upgrades. Such a utility could also grant an adversary the same abilities. This is perhaps the most dangerous vulnerability because access to the software would give an adversary virtually unlimited access to the PBX and its associated instruments.

Manufacturer's Development and Test Features

There may be features that were added to the system during its development phase that were forgotten and not removed when production versions were released. There also may be hidden features that were added by a person on the development team with the intent of creating a back door into the customer's systems. The test features are probably easy to access for ease of development and have few restrictions to reduce development time.

Potential forms of attack include:

- Undocumented username/passwords
- Entering out-of-range values in database fields
- Dialing undocumented access codes on instruments
- Pressing certain key sequences on instruments

The following measures provide controls to minimize risks:

- Establish strong authentication of external technicians.
- Keep maintenance terminals in a locked, restricted area.
- Turn off maintenance features when not needed, if possible.

Software Loading and Update Tampering

When software is initially loaded onto a PBX and when any software updates/patches are loaded, the PBX is particularly vulnerable to software tampering. A software update sent to a PBX administrator could be intercepted by an adversary. The update could be modified to allow special access or special features to the adversary. The modified update would then be sent to the PBX administrator who would install the update and unknowingly give the adversary unwanted access to the PBX.

A control for software loading and updates would be strong modification—tamper detection based on cryptography used in software packages. Conventional error detection codes, such as checksums or cyclic redundancy checks (CRCs), are not sufficient to ensure tamper detection.

Crash-restart Attacks

System crashes may indicate a DoS vulnerability. The means by which a system may be crashed vary significantly from one system to another. The following list suggests a few features and conditions that can sometimes trigger a system crash:

- Call forwarding
- Voice mail
- Physical removal of hardware or media from the PBX
- Use of administrative/maintenance terminal functions
- Direct modification of the system or the database. This may be possible if the media can be read by utilities typically found on a PC or workstation.
- Normal system shutdown procedures

These approaches should be tested as possible ways of exposing the weaknesses discussed in the remainder of this section. One possible additional weakness is that a crash may interrupt the control flow and leave microphones open, so an intruder could overhear what is said after the crash. A further danger is that, in some cases, embedded logons and passwords are restored upon rebooting the system, making it possible for a remote operator to complete the remote restart. However, this also makes it possible for an attacker to gain administrator privileges on a system by crashing the system, then applying a known embedded logon ID/password combination.

Controls for these types of attacks include:

- Crash-restart vulnerability tests and preventing or forbidding, if possible, the triggering of events
- Restart procedures that eliminate the vulnerability from loss of control. This may require doing a cold start (i.e., complete shutdown, power-off, and restart) in the event of a system crash.

- If embedded passwords are found, patching the load module to replace them. Authorized manufacturer personnel can be given the new password, if needed.
- A PBX firewall to enhance the protection of the PBX. In recent years, specialized firewalls have been developed specifically for the protection of PBX systems.

Passwords

Most PBXs grant administrative access to the system database through a system console or a generic dumb terminal. Username/password combinations are often used to protect the system from unwanted changes to the database. If remote access to the maintenance features is available, it is usually restricted by some form of password protection. There may be a single fixed maintenance account, multiple fixed maintenance accounts or general user-defined maintenance accounts. The documentation provided with the PBX should state what type of maintenance access is available. The documentation should also indicate how passwords function. Dangers from improper definition and usage of passwords are the loss of control and confidentiality, illegal usage and tampering of the database.

Controls for passwords include:
- Passwords resistant to cracking by automated tools. A password generator that creates random passwords can go a long way in defeating password crackers.
- Monitoring of multilevel password rights
- Setting an appropriate time-out period for logins

5.5 AUDITING INFORMATION SECURITY MANAGEMENT FRAMEWORK

Auditing the information security framework of an organization involves the audit of logical access, the use of techniques for testing security and the use of investigation techniques.

5.5.1 AUDITING INFORMATION SECURITY MANAGEMENT FRAMEWORK

The information security management framework should be reviewed per the basic elements in an information security framework.

Reviewing Written Policies, Procedures and Standards

Policies and procedures provide the framework and guidelines for maintaining proper operation and control. The IS auditor should review the policies and procedures to determine if they set the tone for proper security and provide a means for assigning responsibility for maintaining a secure computer processing environment.

Logical Access Security Policies

These policies should encourage limiting logical access on a need-to-know basis. They should reasonably assess the exposure to the identified concerns.

Formal Security Awareness and Training

Effective security will always be dependent on people. As a result, security can only be effective if employees know what is expected of them and what their responsibilities are. They should know why various security measures, such as locked doors and use of logon IDs, are in place and the repercussions of violating security.

Promoting security awareness is a preventive control. Through this process, employees become aware of their responsibilities for maintaining good physical and logical security. This can also be a detective measure, because it encourages people to identify and report possible security violations.

Training should start with the new employee orientation or induction process. Ongoing awareness can be provided in company newsletters through visible and consistent security enforcement and short reminders during staff meetings. The security administrator should direct the program. To determine the effectiveness of the program, the IS auditor should interview a sample of employees to determine their overall awareness.

Data Ownership

Data ownership refers to the classification of data elements and the allocation of responsibility for ensuring that they are kept confidential, complete and accurate. A key point of ownership is that, by assigning responsibility for protecting computer data to particular employees, accountability is established. The IS auditor can use this information to determine if proper ownership has been assigned and whether the data owner is aware of the assignment. The IS auditor should also review a sample of job descriptions to ensure that responsibilities and duties are consistent with the information security policy. The auditor should review the classification of data and evaluate their appropriateness, as they relate to the area under review.

Data Owners

These people are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rules for the data for which they are responsible.

Data Custodians

These people are responsible for storing and safeguarding the data, and include IS personnel such as systems analysts and computer operators.

Security Administrator

Security administrators are responsible for providing adequate physical and logical security for IS programs, data and equipment. (The physical security may be handled by someone else, not always by the security administrator.) Normally, the information security policy will provide the basic guidelines under which the security administrator will operate.

New IT Users
New IT users (employees or third parties) and, in general, all new users assigned PCs or other IT resources should sign a document containing the main IT security obligations that they are thereby engaged to know and observe. These are:
- Reading and agreeing to follow security policies
- Keeping logon IDs and passwords secret
- Creating quality passwords according to policy
- Locking their terminal screens when not in use
- Reporting suspected violations of security
- Maintaining good physical security by keeping doors locked, safeguarding access keys, not disclosing access door lock combinations and questioning unfamiliar people
- Conforming to applicable laws and regulations
- Use of IT resources only for authorized business purposes

Data Users
Data users, including the internal and the external user community, are the actual users of the computerized data. Their levels of access into the computer should be authorized by the data owners, and restricted and monitored by the security administrator. Their responsibilities regarding security are to be vigilant regarding the monitoring of unauthorized people in the work areas and comply with general security guidelines and policies.

Documented Authorizations
Data access should be identified and authorized in writing. The IS auditor can review a sample of these authorizations to determine if the proper level of written authority was provided. If the facility practices data ownership, only the data owners provide written authority.

Terminated Employee Access
Termination of employment can occur in the following circumstances:
- On the request of the employee (voluntary resignation from service)
- Scheduled (on retirement or completion of contract)
- Involuntary (forced by management in special circumstances)

In case of involuntary termination of employment, the logical and physical access rights of employees to the IT infrastructure should either be withdrawn completely or highly restricted, as early as possible, before the employee becomes aware of the termination or its likelihood. This ensures that terminated employees cannot continue to access potentially confidential or damaging information from the IT resources or perform any action that would result in damage of any kind to the IT infrastructure, applications and data. Similar procedures should be in place to terminate access for third parties upon terminating their activities with the organization.

When it is necessary for employees to continue to have access, such access must be monitored carefully and continuously and should take place with senior management's knowledge and authorization.

In case of voluntary or scheduled termination of employment, it is management's prerogative to decide whether access is restricted or withdrawn. This depends on:
- The specific circumstances associated with each case
- The sensitivity of the employee's access to the IT infrastructure and resources
- The requirements of the organization's information security policies, standards and procedures

Security Baselines
A baseline security plan is meant to be used as a first step to IT security. The baseline plan should be followed with a full security evaluation and plan. **Exhibit 5.11** illustrates baseline security topics and their associated recommendations.

Exhibit 5.12 depicts a checklist for a baseline security evaluation.

Access Standards
Access standards should be reviewed by the IS auditor to ensure they meet organizational objectives for separating duties, prevent fraud or error, and meet policy requirements for minimizing the risk of unauthorized access.

Standards for security may be defined:
- At a generic level (e.g., all passwords must be at least five characters long)
- For specific machines (e.g., all UNIX machines can be configured to enforce password changes)
- For specific application systems (e.g., sales ledger clerks can access menus that allow entry of sales invoices, but may not access menus that allow check authorization)

5.5.2 AUDITING LOGICAL ACCESS
When evaluating logical access controls the IS auditor should:
- Obtain a general understanding of the security risks facing information processing, through a review of relevant documentation, inquiry, observation, risk assessment and evaluation techniques
- Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness by reviewing appropriate hardware and software security features and identifying any deficiencies or redundancies
- Test controls over access paths to determine whether they are functioning and effective by applying appropriate audit techniques
- Evaluate the access control environment to determine if the control objectives are achieved by analyzing test results and other audit evidence
- Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standards or practices and procedures used by other organizations

Familiarization With the IT Environment
This is the first step of the audit and involves obtaining a clear understanding of the technical, managerial and security environment of the IS processing facility. This typically includes interviews, physical walk-throughs, review of documents and risk assessments.

Exhibit 5.11—IT Security Baseline Recommendations		
Topics	**Objective**	**Recommendations**
Inventory	Establish and maintain an inventory	Users are expected to follow standards for managing computers connected to the network, and have registered network addresses. The operating system and owner should be included along with the data provided.
Antivirus	Install antivirus software with automatic updating	Antivirus software with an automatic DAT file should be updated at regular intervals—no less than weekly.
Passwords	Recognize the importance of passwords	Users must use only strong passwords. The IT department should provide password guidance. Departmental accounts are created for workgroups to prevent/avoid password sharing.
Patching	Make it automatic—less work for you, less chance for compromise	Each machine should be configured to patch automatically for operating system and basic software patching. A process should be set up that works for the department and minimizes disruptions at inconvenient times. Workstations should be more automated to enable system administrators the time to give servers the attention required to minimize the impact on services offered.
Minimizing services offered by systems	Eliminate unnecessary services—reducing security risk and saving time in the long run	To improve basic security and minimize effort to maintain systems, workstations should offer only needed services. Many operating systems are installed with services turned on. By removing services, a workstation's chances of being compromised are reduced and security risks are minimized.
Addressing vulnerabilities	Eliminate many vulnerabilities with good system administration	System compromises can be time-consuming and damage credibility and the business's integrity. Information from enterprisewide scans helps to identify vulnerabilities on each system and provide a baseline for comparison when system integrity is in question.
Backups	Allow easy recovery from user mistakes and hardware failure with backups	Backups should be made offsite for increased security.

Exhibit 5.12—Baseline Security Evaluation Checklist	
Topics	**Evaluation Questions**
Environment/inventory	• What types of data are maintained by the enterprise (i.e., financial, statistical, graphical)? • In what form are they maintained (i.e., spreadsheets, databases, etc.)? • Is there any critical or confidential information maintained or handled? If so, how is it protected? • Are there any specific requirements for handling data (legal or regulatory requirements) • Have you identified machines that store or require access to confidential information? • What type of operating systems exist? • How many subnets exist? • How many workstations/servers exist? • In how many locations is there IT infrastructure? • Has the wireless infrastructure been deployed? How is it secured? • Is staff instructed on how to lock workstations when they step away? • Are users aware that unexpected e-mail attachments should not be opened? • Is staff aware that many compromises are due to social engineering and the sharing of information? • Does the enterprise have a network diagram that includes IP addresses, room numbers and responsible parties? • Has the enterprise limited and secured physical and remote access to network services? • Is corporate hardware upgraded at regular intervals? • Does the enterprise have a current documented inventory of hardware and software? • Is all corporate software licensed? • Is license documentation available (licenses, purchase orders) if a software audit is required?

Assessing and Documenting the Access Paths

The access path is the logical route an end user takes to access computerized information. This starts with a terminal/workstation and typically ends with the data being accessed. Along the way, numerous hardware and software components are encountered. The IS auditor should evaluate each component for proper implementation and physical and logical access security.

Special consideration should be given to the:
- Origination and authorization of the data
- Validity and correctness of the input data
- Maintenance of the affected operating systems (patching, hardening and closing the unnecessarily open ports)
- Examples of attacks from the Internet, in the case of web-based applications where control measures are not defined and enforced are: SQL injection (passing input containing SQL commands to a database behind the web page), cross-site scripting (exploiting applications so that they provide malicious input to another application in the form of an executable script), path traversal (exploiting unchecked input to reach files on the server in such a way that circumvents the access rights management), etc.

The typical sequence of the components is as follows:
- A PC, which is part of the LAN, is used by an end user to sign on. The PC should be physically secure and the logon ID/password used for sign-on should be subject to the restrictions identified previously in this chapter in the Features of Password and Password Syntax Rules sections.
  - The operating system running on the PC should be patched according to the suggestions of the supplier of the operating system and the virus defense must also be updated. Out-of-date operating system versions and out-of-date virus defenses can be exploited by attackers. In the case of the Unix/Linux operating system, the system must be hardened—deleting the unnecessary services (e.g., those connected with remote procedure calls, sending mail, or network management) and library routines. The parameter settings and configuration of the operating system must also be investigated. The ports that are not used should be closed.
  - One or more servers from which the applications to be used are invoked. The operating system running on the servers should be patched according to the recommendations of the supplier of the operating system and the virus defense must also be updated. Out-of-date operating system versions and out-of-date virus defenses can be exploited by attackers. In the case of the Unix/Linux operating system, the system must be hardened—deleting unnecessary services (e.g., those connected with remote procedure calls, sending mail, or network management) and library routines. The parameter settings and configuration of the operating system must also be investigated. The ports that are not used should be closed.
  - The development of the application systems must be disciplined. The auditor should evaluate the control objectives, referring to the origination and authorization of the applications data, and should evaluate the control measures used in data input and processing (see "recommended set of application control objectives" in COBIT 4.0 and 4.1). Omitting these control objectives and measures makes the applications vulnerable to attacks either from within or from the outside, especially from the Internet. Firewalls do not protect applications against the types of attacks that come with the HTTP communication that is usually permitted on the applications.
- The telecommunications software (LAN server or terminal emulator if connecting to a mainframe) intercepts the logon to direct it to the appropriate telecommunication link. The telecommunication software can restrict PCs to specific data or application software. A key audit issue with telecommunication software is to ensure that all applications have been defined within the software and that the various optional telecommunication control and processing features used are appropriate and approved by management. This analysis typically requires the assistance of a system software analyst.
- The transaction processing software may be the next component in the access path. This software routes transactions to the appropriate application software. Key audit issues include ensuring proper identification/authentication of the user (logon ID and password) and authorization of the user to gain access to the application. This analysis is performed by reviewing internal tables that reside in the transaction processing software or in separate security software. Access to these should be restricted to the security administrator.
- The application software then is encountered and should process transactions in accordance with program logic. Audit issues include restricting access to the production software library to only the implementation coordinator.
- The DBMS directs access to the computerized information. Audit issues include ensuring that all data elements are identified in the data dictionary, that access to the data dictionary is restricted to the database administrator (DBA) and that all data elements are subject to logical access control. The application data now can be accessed.
- The access control software can wrap logical access security around all of the above components. This is done via internal security tables. Audit issues include ensuring all of the above components are defined to the access control software, providing access rules that define who can access what on a need-to-know basis and restricting security table access to the security administrator.

Interviewing Systems Personnel

To control and maintain the various components of the access path, as well as the operating system and computer mainframe, technical experts often are required. These people can be a valuable source of information to the IS auditor when gaining an understanding of security. To determine who these people are, the IS auditor should meet with the IS manager and review organizational charts and job descriptions. Key people include the security administrator, network control manager and systems software manager.

The security administrator should be asked to identify the responsibilities and functions of the position. If the answers provided to this question do not support sound control practices or do not adhere to the written job description, the IS auditor should compensate by expanding the scope of the testing of access controls. Also, the IS auditor should determine whether the security administrator is aware of the logical accesses that must be protected, has the motivation and means to actively monitor logons to account for employee changes, and is knowledgeable in how to maintain and monitor access.

A sample of end users should be interviewed to assess their awareness of management policies regarding logical security and confidentiality.

Reviewing Reports From Access Control Software

The reporting features of access control software provide the security administrator with the opportunity to monitor adherence to security policies. By reviewing a sample of security reports, the IS auditor can determine if enough information is provided to support an investigation and if the security administrator is performing an effective review of the report.

Unsuccessful access attempts should be reported and should identify the time, terminal, logon, and file or data element for which access was attempted.

Reviewing Application Systems Operations Manual

An application systems manual should contain documentation on the programs that generally are used throughout a data processing installation to support the development, implementation, operations and use of application systems. This manual should include information about the platform the application can run on, DBMSs, compilers, interpreters, telecommunication monitors and other applications that can run with the application.

5.5.3 TECHNIQUES FOR TESTING SECURITY

Auditors can use different techniques for testing security. Some methods are described in the following subsections.

Terminal Cards and Keys

The IS auditor can take a sample of these cards or keys and attempt to gain access beyond that which is authorized. Also, the IS auditor will want to know if the security administrator followed up on any unsuccessful attempted violations.

Terminal Identification

The IS auditor can work with the network manager to get a listing of terminal addresses and locations. This list can then be used to inventory the terminals, looking for incorrectly logged, missing or additional terminals. The IS auditor should also select a sample of terminals to ensure that they are identified in the network diagram.

Logon IDs and Passwords

To test confidentiality, the IS auditor could attempt to guess the password of a sample of employees' logon IDs (though this is not necessarily a test). This should be done discreetly to avoid upsetting employees. The IS auditor should tour end-user and programmer work areas looking for passwords taped to the side of terminals, the inside of desk drawers or located in card files. Another source of confidential information is the wastebasket. The IS auditor might consider going through the office wastebasket looking for confidential information and passwords. Users could be asked to give their password to the IS auditor. However, unless specifically authorized for a particular situation and supported by the security policy, no user should ever disclose his/her password. Another way to test password strength is to analyze global configuration settings for password strength in the system application and compare this with the organization's security policy.

To test encryption, the IS auditor should work with the security administrator to attempt to view the internal password table. If viewing is possible, the contents should be unreadable. Being able to view encrypted passwords can still be dangerous. On some systems, although the passwords are impossible to decipher, if an individual can obtain the encryption program, they can encrypt common passwords and look for matches. This was a method used to break into UNIX computers prior to the development of shadow password files. Application logs should also be reviewed to ensure that passwords and logon IDs are not recorded in a clear form.

To test access authorization, the IS auditor should review a sample of access authorization documents to determine if proper authority has been provided and if the authorization was granted on a need-to-know basis. Conversely, the IS auditor should get a computer-generated report of computer access rules, take a sample to determine if the access is on a need-to-know basis, and attempt to match the sample of these rules to authorizing documents. If no written authorization is found, this indicates a breakdown in control and may warrant further review to determine the exposures and implications.

Account settings for minimizing authorized access should be available from most access control software or from the operating system. To verify that these settings actually are working, the IS auditor can perform the following manual tests:

- To test periodic change requirements, the IS auditor can draw on his/her experiences using the system and interview a sample of users to determine if they are forced to change their password after the prescribed time interval.
- To test for disabling or deleting of inactive logon IDs and passwords, the IS auditor should obtain a computer-generated list of active logon IDs. On a sample basis, the IS auditor should match this list to current employees, looking for logon IDs assigned to employees or consultants who are no longer with the company.
- To test for password syntax, the IS auditor should attempt to create passwords in a format that is invalid, such as too short, too long, repeated from the previous password, incorrect mix of alpha or numeric characters, or the use of inappropriate characters.
- To test for automatic logoff of unattended terminals, the IS auditor should log on to a number of terminals. The IS auditor then simply waits for the terminals to disconnect after the established time interval. Before beginning this test, the IS auditor should verify with the security administrator that this automatic logoff feature applies to all terminals.
- To test for automatic deactivation of terminals after unsuccessful access attempts, the IS auditor should attempt to log on, purposefully entering the wrong password a number of times. The logon ID should deactivate after the established number of invalid passwords has been entered. The IS auditor will be interested in how the security administrator reactivates the logon ID. If a simple telephone call to the security administrator with no verification of identification results in reactivation, then this function is not controlled properly.
- To test for masking of passwords on terminals, the IS auditor should log on to a terminal and observe if the password is displayed when entered.

Controls Over Production Resources

Computer access controls should extend beyond application data and transactions. There are numerous high-level utilities, macro or job control libraries, control libraries, and system software parameters for which access control should be particularly strong. Access to these libraries would provide the ability to bypass other access controls.

The IS auditor should work with the system software analyst and operations manager to determine if access is on a need-to-know basis for all sensitive production resources. Working with the security administrator, the IS auditor should determine who can access these resources and what can be done with this access.

Logging and Reporting of Computer Access Violations

To test the reporting of access violations, the IS auditor should attempt to access computer transactions or data for which access is not authorized. The attempts should be unsuccessful and identified on security reports. This test should be coordinated with the data owner and security administrator to avoid violation of security regulations.

Follow-up Access Violations

To test the effectiveness and timeliness of the security administrator and data owner's responses to reported violation attempts, the IS auditor should select a sample of security reports and look for evidence of follow-up and investigation of access violations. If such evidence cannot be found, the IS auditor should conduct further interviews to determine why this situation exists.

Bypassing Security and Compensating Controls

This is a technical area of review. As a result, the IS auditor should work with the system software analyst, network manager, operations manager and security administrator to determine ways to bypass security. This typically includes bypass label processing, special system maintenance logon IDs, operating system exits, installation utilities and input/output (I/O) devices. Working with the security administrator, the IS auditor should determine who can access these resources and what can be done with this access. The IS auditor should determine if access is on a need-to-know/have basis or if compensating detective controls exist.

Since many of these bypassing security features can be exploited by technically sophisticated intruders, the IS auditor should also ensure that:

- All uses of these features are logged, reported and investigated by the security administrator or system software manager
- Unnecessary bypass security features are deactivated
- If possible, the bypass security features are subject to additional logical access controls

Review Access Controls and Password Administration

Access controls and password administration are reviewed to determine that:

- Procedures exist for adding individuals to the list of those authorized to have access to computer resources, changing their access capabilities and deleting them from the list
- Procedures exist to ensure that individual passwords are not inadvertently disclosed
- Passwords issued are of an adequate length, cannot be easily guessed and do not contain repeating characters
- Passwords are periodically changed
- User organizations periodically validate the access capabilities currently provided to individuals in their department
- Procedures provide for the suspension of user identification codes (logon IDs or accounts) or the disabling of terminal, microcomputer or data entry device activity—after a particular number of security procedure violations

5.5.4 INVESTIGATION TECHNIQUES

Investigation techniques include the investigation of computer crime and the protection of evidence and chain of custody, among others.

Investigation of Computer Crime

Computer crimes are not reported in most cases simply because they are not detected. In many cases where computer crimes are detected, companies hesitate to report them since they generate a large amount of negative publicity that can affect their business. In such cases, the management of the affected company seeks to simply plug the loopholes used for the crime and move on. In addition, in many countries current laws are directed toward protecting physical property. It is very difficult to use such laws against computer crime. Even in jurisdictions where the laws have been updated, the investigation procedures are not always widely known and the necessary hardware and software tools are not always available to collect the digital evidence.

In the aftermath of a computer crime, it is very important that proper procedures are used to collect evidence from the crime scene. If data and evidence is not collected in the proper manner, it could be damaged and, even if the perpetrator is eventually identified, prosecution will not be successful in the absence of undamaged evidence. Therefore, after a computer crime, the environment and evidence must be left unaltered and specialist law enforcement officials must be called in. If the incident is to be handled in-house, the company must have a suitably qualified and experienced incident response team.

Protection of Evidence and Chain of Custody

The evidence of a computer crime exists in the form of log files, file time stamps, contents of memory, etc. Rebooting the system or accessing files could result in such evidence being lost, corrupted or overwritten. Therefore, one of the first steps taken should be copying one or more images of the attacked system. Memory content should also be dumped to a file before rebooting the system. Any further analysis must be performed on an image of the system and on copies of the memory dumped—not on the original system in question.

In addition to protecting the evidence, it is also important to preserve the chain of custody. Chain of custody is a term that refers to documenting, in detail, how evidence is handled and maintained, including its ownership, transfer and modification. This is necessary to satisfy legal requirements that mandate a high level of confidence regarding the integrity of evidence.

5.6 AUDITING NETWORK INFRASTRUCTURE SECURITY

When performing an audit of the network infrastructure, the IS auditor should:

- Review network diagrams (campus LAN networks, WANS, metropolitan area networks [MANs]) that identify the organizations internetworking infrastructure, which would include gateways, firewalls, routers, switches, hubs, access servers, modems, etc. This information is important because the IS auditor will want to evaluate these links to determine whether proper physical and logical access controls are in effect and to inventory the various terminal connections to ensure that the diagram is accurate.
- Identify the network design implemented, including the IP strategy used, segmentation of routers and switches for campus environments, and WAN configurations and protocols
- Determine that applicable security policies, standards, procedures and guidance on network management and usage exist and have been distributed to staff, network management and administration. He/she should also ensure that staff members have been trained in their duties and responsibilities.
- Identify who is responsible for security and operation of Internet connections, and evaluate whether they have sufficient knowledge and experience to undertake this role
- Determine whether consideration has been given to the legal problems arising from use of the Internet. (Considerations should include liability arising from inaccurate web pages; legislation regarding sale or advertising of regulated products, such as financial services; implications of selling/buying in different countries; and the state of application of standard contract terms to electronic trading.)
- If the service is outsourced, review service level agreements (SLAs) to ensure that they include provisions for security in addition to availability and quality of service
- Review network administrator procedures to ensure that hardware and software components are upgraded in response to new vulnerabilities

5.6.1 AUDITING REMOTE ACCESS

Remote use of information resources dramatically improves business productivity, but generates control issues and security concerns. In this regard, IS auditors should determine that all remote access capabilities used by an organization provide for effective security of the organization's information resources. Remote access security controls should be documented and implemented for authorized users operating outside of the trusted network environment.

In reviewing existing remote access architectures, IS auditors should assess remote access points of entry in addressing how many (known/unknown) exist and whether greater centralized control of remote access points is needed. IS auditors should also review access points for appropriate controls, such as in the use of VPNs, authentication mechanisms, encryption, firewalls and IDSs.

As part of this review, the IS auditor should also test dial-up access controls. To test for dial-up access authorization, the IS auditor should dial the computer from a number of authorized and unauthorized telephone lines. If controls are adequate, successful connection will occur with the authorized numbers only. The IS auditor should test the logical controls invoked after authorized connections to the computer are achieved by using the successful dial-up connections to attempt to gain unauthorized file access. Performance of this test should be coordinated through the security administrator to avoid violating security regulations.

In reviewing future remote access initiatives, IS auditors should first determine whether design and development of remote access approaches are based on a cost-effective, risk-based solution taking into account business requirements. This includes assessing the types of remote environments applicable, the integrity and availability of telecommunication services, and required measures to take in protecting the corporate infrastructure.

Auditing Internet Points of Presence

When auditing an organization's presence on the Internet, the IS auditor should review the use of the Internet to ensure that a business case has been demonstrated for the following possible uses:

- E-mail (i.e., communications to/from business partners, customers and the general public)
- Marketing (e.g., mechanism for communicating customer values such as online home shopping catalogue)
- Sales channel/electronic commerce (e.g., electronic ordering of goods/services, purchasing of goods from home shopping catalogue using credit cards, or electronic transmission of standard electronic data interchange (EDI)-formatted order messages by business partners)
- Channel of delivery for goods/services (such as online bookstores, and Internet banking)
- Information gathering (e.g., staff browsing the web for information)

Network Penetration Tests

Combinations of procedures, whereby an IS auditor uses the same techniques as a hacker, are called penetration tests, intrusion tests or ethical hacking. This is an effective method of identifying the real-time risks to an information processing environment. During penetration testing, an auditor attempts to circumvent the security features of a system and exploits the vulnerabilities to gain access that would otherwise be unauthorized.

Scope can vary based on the terms and conditions of the client and requirements. However, from an audit risk perspective, the following should be mentioned clearly in the audit scope:

- Precise IP addresses/ranges to be tested
- Host restricted (i.e., hosts not to be tested)
- Acceptable testing techniques (i.e., social engineering, DoS/distributed denial of service [DDoS], sql injections, etc.)
- Acceptance of proposed methodology from management
- Timing of attack simulation (i.e., business hours, off hours, etc)
- IP addresses of the source of attack simulation (to identify between approved simulated attack and actual attack)
- Point of contact for both the penetration tester/auditor and the targeted system owner/administrator

- Handling of information collected by the penetration tester/auditor (i.e., nondisclosure agreement [NDA] or reference to standard rules of engagement)
- Warning notification from penetration tester/auditor, before the simulation begins to avoid false alarms to law enforcement bodies

The different phases of penetration testing appear in **exhibit 5.13** and the corresponding procedures in **exhibit 5.14**.

Penetration testing is intended to mimic an experienced hacker attacking a live site. It should only be performed by experienced and qualified professionals who are aware of the risks of undertaking such work and can limit the damage resulting from a successful break-in to a live site (e.g., avoidance of DoS attacks). It is a simulation of a real attack and maybe restricted by the law, an organization's policy and federal regulations; therefore, it is imperative to obtain management's consent in writing before finalization of the test/engagement scope.

There are several types of penetration tests depending upon the scope, objective and nature of the test. Generally accepted and common types of penetration tests are:

- **External testing**—Refers to attacks and control circumvention attempts on the target's network perimeter from outside the target's system, i.e., usually the Internet
- **Internal testing**—Refers to attacks and control circumvention attempts on the target from within the perimeter. The objective is to identify what would occur if the external network perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on the network.
- **Blind testing**—Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such testing is expensive, since penetration testers have to research the target and profile it based on publicly available information only.
- **Double blind testing**—It is an extension of blind testing, since the administrator and security staff at the target are also not aware of the test. Such testing can effectively evaluate the incident handling and response capability of the target.
- **Targeted testing**—Refers to attacks and control circumvention attempts on the target, while both the target's IT team and penetration testers are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they may also be provided with a limited-privilege user account to be used as a starting point to identify privilege-escalation possibilities in the system.

Although management may sponsor the activities of penetration testing, some of the risks of these activities include:

- Penetration testing does not provide assurance that all vulnerabilities are discovered and may fail to discover significant vulnerabilities.
- Miscommunication may result in the test objectives not being achieved.
- Testing activities may inadvertently trigger escalation procedures that may not have been appropriately planned.
- Sensitive information may be disclosed, heightening the target's exposure level.
- Without proper background and qualification checks of penetration testers, the penetration tester may damage the information assets or misuse the information gained for personal benefits.

Additionally, these techniques are becoming more popular for testing the reliability of firewall access controls. The IS auditor should be extremely careful if attempting to break into a live production system since, if successful, the IS auditor may cause the system to fail. Permission for the use of such techniques should always be obtained from top-level senior management. Permission from top-level senior management is also required to determine what other tests can be performed without informing the staff who are responsible for the monitoring and reporting of security violations (if any are aware that the attack will take places, they are likely to be more vigilant than normal).

Exhibit 5.13—Penetration Testing Phases

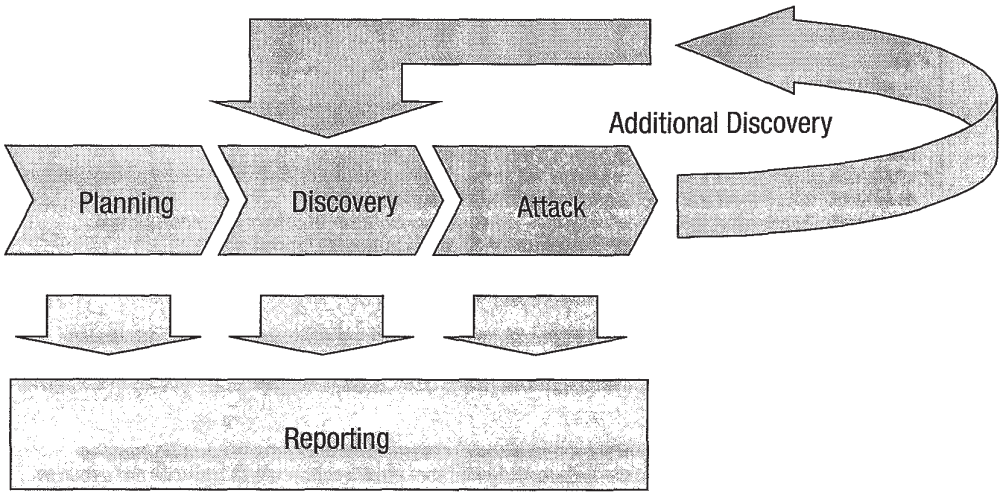


Exhibit 5.14—Penetration Testing Phases and Procedures	
Phase	**Procedures**
Planning	• Rules of engagement • Management approval/finalization • Adopted testing methodology • Intrusive or nonintrusive testing • Goals/objectives identified and agreed upon • Timelines/deadlines agreed upon • Milestones identified • Assignment time tracking technique understood and communicated • Deliverables agreed upon • Tools collected/installed/tested in a test environment
Reconnaissance/ discovery	• Network mapping • DNS interrogation • WHOIS queries (from InterNIC) • Searching target's web site for information • Searching target's related data on search engines • Searching resume/curriculum vitae of target's current and formal employees (reveals system related details) • Packet capture/sniffing (during internal testing only) • Host detection (Internet control message protocol [ICMP], DNS, WHOIS, PingSweep, TCP/UDP Sweep, etc.) • Service detection (port scanning, stealth scanning, error/banner detection, etc.) • Network topology detection (Internet control message protocol [ICMP], firewalking, etc.) • OS detection (TCP stack analysis, etc.) • Web site mapping • Web page analysis • Unused pages/scripts • Broken links • Hidden links/files accessible • Application logic/use • Points of input error page banner grabbing • Vulnerability classification (based on information collected in previous steps, vulnerabilities are searched on available search engines or custom-built repositories) Some of the attack techniques are as follows: • Directory browsing • Show code • Error injection • Type and bound checks on input
Attacks	• Special character injection (metacharacters, escape characters, etc.) • Cookie/session IDs analysis • Authentication circumvention • Long input • System functions (shell escapes, etc) • Logic alteration (SQL query injection, etc) • Cookie/session IDs manipulation • Internet service exploits (bind, mdac, unicode, apache-http, statd, sadmind, etc.) • Operating system exploits • Network exploits (SYN flooding, ICMP redirects, DNS poisoning etc.) Furthermore, once an attack is successful, it typically follows these subprocedures of an attack phase: • Privilege escalation—If only a user-level access was gained previously, then the tester will attempt to obtain super-level access (i.e., root on UNIX/Linux and administrator on NT/Windows 2000 and above) • Information gathering from inside—The attacker will probe further systems on the network efficiently utilizing the compromised system as a launch pad and thereby attempt to gain access to trusted/high-risk systems • Installation of further attack tools inside the system—Attacker may require installation of additional tools and penetration testing software to gain further access to the resources, trusted or high-risk systems This phase simultaneously occurs with the rest of the three phases. In the planning phase, rules of engagement, written consent and test plans are developed, discussed and reported. In the discovery phase, written logs are kept and periodic reports on the status of assignment are reported to management, as appropriate. Following the attack phase, the vulnerabilities and weaknesses discovered are reported with risk rating based on probability derived from ease of exploitation and impact derived from attack results or official advisories and resources from the vendor. In addition, the recommendations contain steps to mitigate the risks and to effectively rectify the weaknesses.

Full Network Assessment Reviews

Upon completion of penetration testing, comprehensive review of all network system vulnerabilities should occur to determine whether threats to confidentiality, integrity and availability have been identified. The following reviews should occur:

- Security policy and procedures should be reviewed to determine best practices are in place.
- The network and firewall configuration should be evaluated to ensure that they have been designed to support the security of the services being provided (e.g., screening routers, dual/multihomed host, screened subnet, demilitarized zone proxy servers).
- The logical access controls should be evaluated to ensure that they support separation of duties (e.g., development vs. operation, security administration vs. audit).
- The following should be determined:
  - Intrusion detection software is in place.
  - Filtering is being performed.
  - Encryption is being used (consider VPNs/tunneling, digital signatures for e-mail, etc).
  - Strong forms of authentication are being used (consider use of smart cards, biometrics, etc., for authentication to firewalls, to internal software/hardware within the network, and to external hardware/software).
  - The firewalls have been configured properly (consider removal of all unnecessary software, addition of security and auditing software, removal of unnecessary logon IDs, disabling of unused services).
  - The application- or circuit-level gateways in use are running proxy servers for all legitimate services (e.g., teletype network [Telnet], HTTP, FTP).
  - Virus scanning is being used.
  - Periodic penetration testing is being completed.
  - Audit logging is undertaken for all key systems (e.g., firewalls, application gateways, routers, etc.) and audit logs are copied to secure file systems (consider direct writing of audit logs to write once CD-WORM).
  - The security administrators are reviewing the latest CERT, Computer Incident Advisory Capability (CIAC) and SysAdmin, Audit, Network, Security (SANS) Institute's reports for Internet security breaches.

Development and Authorization of Network Changes

Network configuration changes to update telecommunications lines, terminals, modems and other network devices should be authorized in writing by management and implemented in a timely manner. The IS auditor can test this change control by:

- Sampling recent change requests, looking for appropriate authorization and matching the request to the actual network device
- Matching recent network changes, such as new telecommunication lines, to added terminals and authorized change requests

As an added control, the IS auditor should determine who can access the network change software. This access should be restricted to senior network administrators.

Specific development and change control procedures should be in place for network components' hardware and software. Procedures should cover:

- Firewalls
- Routers
- Switches
- Application gateways
- DNS/network topology
- Client software
- Network management software
- Web server hardware and configuration
- Application software
- Web pages

Unauthorized Changes

One of the most important objectives of change control procedures is to prevent or detect unauthorized changes to software, configurations or parameters, and data. Unauthorized changes include any changes to software or configurations/parameters that occur without conforming to change control procedures. They include situations where changes are made to software code without authorization, in addition to legitimate changes made in accordance with change control procedures. Controls to prevent unauthorized changes to software and software configurations include:

- Segregation of duties between software development, software administration and computer operations
- Restricting the software development team's access to the development environment only
- Restricting access to the software source codes

Controls to detect unauthorized changes to software include software code comparison utilities. Unauthorized changes to configurations/parameters can be detected through logging and monitoring system administrator activities.

Changes to data normally are controlled through the applications. Application access control mechanisms and built in application controls normally prevent unauthorized access to data. These controls can be circumvented by direct access to data. For this reason, direct access to data (specifically "write" or "change" access) should be restricted and monitored.

Computer Forensics

By definition, computer forensics is the "process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law)," according to D. Rodney McKemmish in his book *Computer and Intrusion Forensics*. An IS auditor may be required or asked to be involved in a forensic analysis in progress to provide expert opinion or to ensure the correct interpretation of information gathered.

Computer forensics includes activities that involve the exploration and application of methods to gather, process, interpret and use digital evidence that help to substantiate whether an incident happened such as:

- Providing validation that an attack actually occurred
- Gathering digital evidence that can later be used in judicial proceedings

Any electronic document or data can be used as digital evidence, provided there is sufficient manual or electronic proof that the contents of digital evidence are in their original state and have not been tampered with or modified during the process of collection and analysis.

It is very important to preserve evidence in any situation. Most organizations are not well equipped to deal with intrusions and electronic crimes from an operational and procedural perspective, and they respond to it only when the intrusion has occurred and the risk is realized. The evidence loses its integrity and value in legal proceedings if it has not been preserved and subject to a documented chain of custody. This happens when the incident is inappropriately managed and responded to in an *ad hoc* manner.

For evidence to be admissible in a court of law, the chain of custody needs to be maintained professionally. The chain of evidence essentially contains information regarding:
- Who had access to the evidence (chronological manner)
- The procedures followed in working with the evidence (such as disk duplication, virtual memory dump)
- Proving that the analysis is based on copies that are identical to the original evidence (could be documentation, checksums, timestamps)

It is important to use industry-specified best practices, proven tools and due diligence to provide reasonable assurance of the quality of evidence.

It is also important to demonstrate integrity and reliability of evidence for it to be acceptable to law enforcement authorities.

There are four major considerations in the chain of events in regards to evidence in computer forensics:
- **Identify**—Refers to the identification of information that is available and might form the evidence of an incident.
- **Preserve**—Refers to the practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain-of-custody so that it can be established in a court of law.
- **Analyze**—Involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. Interpreting the data requires an in-depth knowledge of how different pieces of evidence may fit together. The analysis should be performed using an image of media and not the original.
- **Present**—Involves a presentation to the various audiences such as management, attorneys, court, etc. Acceptance of the evidence depends upon the manner of presentation (as it should be convincing), qualifications of the presenter, and credibility of the process used to preserve and analyze the evidence.

The IS auditor should give consideration to key elements of computer forensics during audit planning. These key elements are described in the following subsections.

DATA PROTECTION
To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocols to inform appropriate parties that electronic evidence will be sought and to not destroy it by any means.

Infrastructure and processes for incident response and handling should be in place to permit an effective response and forensic investigation if an event or incident occurs.

DATA ACQUISITION
All information and data required should be transferred into a controlled location; this includes all types of electronic media such as as fixed disk drives and removable media. Each device must be checked to ensure that it is write-protected. This may be achieved by using a device known as a write-blocker.

It is also possible to get data and information from witnesses or related parties by recorded statements.

By volatile data, investigators can determine what is currently happening on a system. This kind of data includes open ports, open files, active processes, user logons and other data present in RAM. This information is lost when the computer is shut down.

IMAGING
The imaging is a process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

With appropriate tools, it is sometimes possible to recover destroyed information (erased even by reformatting) from the disk's surface.

EXTRACTION
This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made.

The extraction process could include different sources such as system logs, firewall logs, IDS logs, audit trails and network management information.

INTERROGATION
Interrogation is used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data.

INGESTION/NORMALIZATION
This process converts the information extracted to a format that can be understood by investigators. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tools.

It is possible to create relationships from data by extrapolation, using techniques such as fusion, correlation, graphing, mapping or time lining, which could be used in the construction of the investigation's hypothesis.

REPORTING

The information obtained from computer forensics has limited value when it is not collected and reported in the proper way.

When an IS auditor writes the report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusions were made from this analysis.

The report should achieve the following goals (taken from Mandia, Kevin; Matt Pepe; Chris Prosise; *Incident Response & Computer Forensics, 2nd Edition,* McGraw Hill/Osborne, USA, 2003):

- Accurately describe the details of an incident
- Be understandable to decision-makers
- Be able to withstand a barrage of legal scrutiny
- Be unambiguous and not open to misinterpretation
- Be easily referenced
- Contain all information required to explain conclusions reached
- Offer valid conclusions, opinions or recommendations when needed
- Be created in a timely manner

The report should also identify the organization, sample reports and restrictions on circulation (if any) and include any reservations or qualifications that the IS auditor has with respect to the assignment.

5.7 ENVIRONMENTAL EXPOSURES AND CONTROLS

5.7.1 ENVIRONMENTAL ISSUES AND EXPOSURES

Environmental exposures are due primarily to naturally occurring events such as lightning storms, earthquakes, volcanic eruptions, hurricanes, tornados and other types of extreme weather conditions. The result of such conditions can lead to many types of problems. One particular area of concern is power failures of computer and supporting environmental systems. Generally, power failures can be grouped into four distinct categories, based on the duration and relative severity of the failure:

- **Total failure (blackout)**—A complete loss of electrical power, which may span from a single building to an entire geographical area and is often caused by weather conditions (e.g., storm, earthquake) or the inability of an electrical utility company to meet user demands (e.g., during summer months)
- **Severely reduced voltage (brownout)**—The failure of an electrical utility company to supply power within an acceptable range (i.e., 108-125 volts AC in the US). Such failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.
- **Sags, spikes and surges**—Temporary and rapid decreases (sags) or increases (spikes and surges) in voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices (e.g., hard disks or memory chips).
- **Electromagnetic interference (EMI)**—Caused by electrical storms or noisy electrical equipment (e.g., motors, fluorescent lighting, radio transmitters). This interference may cause computer systems to hang or crash as well as damages similar to those caused by sags, spikes and surges.

Short-term interruptions, such as sags, spikes and surges, which last from a few millionths to a few thousandths of a second, can be prevented by using properly placed surge protectors. Intermediate-term interruptions, which last from a few seconds to 30 minutes, can be controlled by UPS devices. Finally, long-term interruptions, which last from a few hours to several days, require the use of alternate power generators. These generators may be portable devices or part of the building's infrastructure and are powered by alternative sources of energy such as diesel, gasoline or propane.

Another area of concern deals with water damage/flooding. This is a concern even with facilities located on upper floors of high-rise buildings since water damage typically occurs from broken water pipes.

Other concerns, outside of natural threats, are man-made. They include terrorist threats/attacks, vandalism, electrical shock and equipment failure.

Some questions that organizations must address related to environmental issues and exposures include the following:

- Is the power supply to the computer equipment properly controlled to ensure that power remains within the manufacturer's specifications?
- Are the air conditioning, humidity and ventilation control systems for the computer equipment adequate to maintain temperatures within manufacturers' specifications?
- Is the computer equipment protected from the effects of static electricity, using an antistatic rug or antistatic spray?
- Is the computer equipment kept free of dust, smoke and other particulate matter such as food?
- Do policies exist that prohibit the consumption of food, beverage and tobacco products near computer equipment?
- Are backup media protected from damage due to temperature extremes, the effects of magnetic fields and water damage?

5.7.2 CONTROLS FOR ENVIRONMENTAL EXPOSURES

Environmental exposures should be afforded the same level of protection as physical and logical exposures. Environmental controls are described in the following subsections.

Alarm Control Panels

An alarm control panel should ideally be:

- Separated from burglar or security systems located on the premises
- Accessible to fire department personnel at all times
- Located in a weatherproof box
- In accordance with temperature requirements set by the manufacturer
- Situated in a controlled room to prevent access by unauthorized personnel
- Allocated power from a dedicated and separate circuit
- Able to control or disable separate zones within the facilities
- In adherence with local and national regulations and approved by local authorities

Water Detectors

In the computer room, water detectors should be placed under raised floors and near drain holes, even if the computer room is on a high floor (remember water leaks). Any unattended equipment storage facilities should also have water detectors. When activated, the detectors should produce an audible alarm that can be heard by security and control personnel. The location of the water detectors should be marked on the raised computer room floor for easy identification and access. On hearing the alarm, specific individuals should be responsible for investigating the cause and initiating remedial action; other staff should be made aware by security and control personnel that there is a risk of electric shock.

Handheld Fire Extinguishers

Fire extinguishers should be in strategic locations throughout the facility. They should be tagged for inspection and inspected at least annually.

Manual Fire Alarms

Hand-pull fire alarms should be placed strategically throughout the facility. These are normally located near exit doors to ensure personnel safety. The resulting audible alarm should be linked to a monitored guard station.

Smoke Detectors

Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised computer room floor. The detectors should produce an audible alarm when activated and be linked to a monitored station (preferably by the fire department). The location of the smoke detectors above the ceiling tiles and below the raised floor should be marked on the tiling for easy identification and access. Smoke detectors should supplement, not replace, fire suppression systems.

Fire Suppression Systems

These systems are designed to automatically activate immediately after detection of high heat, typically generated by fire. Like smoke detectors, the system should produce an audible alarm when activated and be linked to a central guard station that is regularly monitored. The system should also be inspected and tested annually. Testing intervals should comply with industry and insurance standards and guidelines. Ideally, the system should automatically trigger other mechanisms to localize the fire. This includes closing fire doors, notifying the fire department, closing off ventilation ducts and shutting down nonessential electrical equipment. In addition, the system should be segmented so a fire in one part of a large facility does not activate the entire system.

Broadly speaking, there are two methods for applying an extinguishing agent: total flooding and local application.

Systems working under a *total flooding* principle apply an extinguishing agent to a three-dimensional enclosed space in order to achieve a concentration of the agent (volume percent of the agent in air) adequate to extinguish the fire. These types of systems may be operated automatically by detection and related controls or manually by the operation of a system actuator.

Systems working under a *local application* principle apply an extinguishing agent directly onto a fire (usually a two- dimensional area), or into the three-dimensional region immediately surrounding the substance or object on fire. The main difference between local application and total flooding designs is the absence of physical barriers enclosing the fire space in the local application design.

In the context of automatic extinguishing systems, local application does normally not refer to the use of manually operated wheeled or portable fire extinguishers, although the nature of the agent delivery is similar.

The medium for fire suppression varies, but is usually one of the following:

- Water-based systems are typically referred to as sprinkler systems. These systems are effective but are also unpopular because they damage equipment and property. The system can be dry-pipe or charged (water is always in the system piping). A charged system is more reliable but has the disadvantage of exposing the facility to expensive water damage if the pipes leak or break.
- Dry-pipe sprinkling systems do not have water in the pipes until an electronic fire alarm activates the water pumps to send water into the system. This is opposed to a fully charged water pipe system. Dry-pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment from above. Since water and electricity do not mix, these systems must be combined with an automatic switch to shut down the electricity supply to the area protected.
- Halon systems release pressurized Halon gases that remove oxygen from the air, thus starving the fire. Halon was popular because it is an inert gas and does not damage equipment like water does. There should be an audible alarm and brief delay before discharge to permit personnel time to evacuate the area or to override and disconnect the system. Because Halon adversely affects the ozone layer, it was banned in the Montreal (Canada) protocol of 1987, which stopped Halon production as of 1 January 1994. The Halon substitute is FM-200, which is the most effective alternative.
- FM-200TM: Also called heptafluoropropane, HFC-227 or HFC-227ea (ISO name), is a colorless odorless gaseous halocarbon. It is commonly used as a gaseous fire suppression agent. The HFC-227 fire suppression agent was the first nonozone-depleting replacement for Halon 1301. In addition, HFC-227 leaves no residue on valuable equipment after discharge. Trade names include FE-227 (DuPont), FM-200 (Chemtura) and Solkaflam 227 (Solvay Fluor). This agent suppresses fire by discharging as a gas onto the surface of combusting materials. Large amounts of heat energy are absorbed from the surface of the burning material, lowering its temperature below the ignition point. FM-200 fire suppression systems have low atmospheric lifetimes, global warming and ozone depletion potentials.
- Argonite is the brand name (a registered trademark owned by Ginge-Kerr) for a mixture of 50% argon (Ar) and 50% nitrogen (N2). It is an inert gas used in gaseous fire suppression systems for extinguishing fires where damage to equipment is to be avoided. Although argon is nontoxic, it does not satisfy the body's need for oxygen and is a simple asphyxiant. People have suffocated by breathing argon by mistake

Unlike carbon dioxide (CO2) fire suppression systems, which are unable to sustain human life, FM-200 and Argonite systems are environmentally friendly. They provide an effective, safe method of fire suppression, and unlike charged sprinkler systems, they do not suffer from the disadvantage of exposing the expensive information processing facility (IPF) to water damage during the firefighting or if the pipe leaks or breaks.

- CO2 systems release pressurized carbon dioxide gas into the area protected to replace the oxygen required for combustion. Unlike Halon and its later replacements, however, CO2 is unable to sustain human life. Therefore, in most countries, it is illegal for such systems to be set to automatic release if any human may be in the area. Because of this, these systems are usually discharged manually, introducing an additional delay in combating the fire.

Strategically Locating the Computer Room

To reduce the risk of flooding, the computer room should not be located in the basement or top floor. If located in a multistory building, studies show that the best location for the computer room—the location which reduces the risk of fire, smoke and water damage—is on the middle floors (e.g., third, fourth, fifth or sixth floor). Adjacent water or gas pipes should be avoided except in the case of fire suppression systems. Care should be taken to avoid locating computer rooms adjacent to areas where functions carrying a high risk are carried out, such as paper storage. The activity of neighboring organizations should be considered when establishing a computer facility. Locations adjacent to, or on the final path to, an airport or a chemical works where explosive gases may be present, for example, should be avoided.

Regular Inspection by Fire Department

To ensure that all fire detection systems comply with building codes, the fire department should inspect the system and facilities annually. Also, the fire department should be notified of the location of the computer room, so it can be prepared with equipment appropriate for electrical fires.

Fireproof Walls, Floors and Ceilings of the Computer Room

Walls surrounding the information processing facility should contain or block fire from spreading. The surrounding walls should have at least a two-hour fire resistance rating.

Electrical Surge Protectors

These electrical devices reduce the risk of damage to equipment due to power spikes. Voltage regulators measure the incoming electrical current and either increase or decrease the charge to ensure a consistent current. Such protectors are typically built into the UPS system.

Uninterruptible Power Supply/Generator

A UPS system consists of a battery or gasoline (petrol)-powered generator that interfaces with the electrical power entering the facility and the electrical power entering the computer. The system typically cleanses the power to ensure that wattage into the computer is consistent. Should a power failure occur, the UPS continues providing electrical power from the generator to the computer for a certain length of time. Depending on the sophistication of the UPS, electrical power could continue to flow for days or for just a few minutes to permit an orderly computer shutdown. A UPS system can be built into a computer or can be an external piece of equipment.

Emergency Power-off Switch

There may be a need to immediately shut off power to the computer and peripheral devices such as during a computer room fire or emergency evacuation. Two emergency power-off switches should serve this purpose—one in the computer room, the other near, but outside, the computer room.

Switches should be clearly labeled and easily accessible, for this purpose, and yet they should still be secure from unauthorized people. The switches should be shielded to prevent accidental activation.

Power Leads From Two Substations

Electrical power lines that feed into the facility are exposed to many environmental hazards—water, fire, lightning, cutting due to careless digging, etc. To reduce the risk of a power failure due to these events that, for the most part, are beyond the control of the organization, redundant power lines should feed into the facility. In this way, interruption of one power line does not adversely affect electrical supply.

Wiring Placed in Electrical Panels and Conduit

Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised computer room floor.

Inhibited Activities Within the IPF

Food, drink and tobacco use can cause fires, the buildup of contaminants or damage to sensitive equipment (especially in the case of liquids). They should be prohibited from the information processing facility (IPF). This prohibition should be overt, for example, a sign on the entryway.

Fire-resistant Office Materials

Wastebaskets, curtains, desks, cabinets and other general office materials in the IPF should be fire-resistant. Cleaning fluids for desktops, console screens and other office furniture/fixtures should not be flammable.

Documented and Tested Emergency Evacuation Plans

Evacuation plans should emphasize human safety, but should not leave IPFs physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation, if time permits.

5.7.3 AUDITING ENVIRONMENTAL CONTROLS

The testing procedures noted in the following subsections should also be applied to any offsite storage and processing facilities.

Water and Smoke Detectors

The computer room should be visited for the visual verification of the presence of water and smoke detectors. Whether the power supply to these detectors is sufficient should be determined,

especially in instances of battery-operated devices. Also, the locations of the devices should be placed to give early warning of a fire, such as immediately above the computer equipment they are protecting, and should be clearly marked and visible.

Handheld Fire Extinguishers
Handheld fire extinguishers should be in strategic highly visible locations throughout the facility and should be inspected annually.

Fire Suppression Systems
Fire suppression systems are expensive to test and, therefore, the IS auditor's ability to determine operability is limited. IS auditors may need to limit their tests to reviewing documentation to ensure that the system has been inspected and tested within the last year. The exact testing interval should comply with industry and insurance standards and guidelines.

Regular Inspection by Fire Department
The person responsible for fire equipment maintenance should be contacted and asked if a local fire department inspector or insurance evaluator has been recently invited to tour and inspect the facilities. If so, a copy of the report should be obtained, and how to address the noted deficiencies should be determined.

Fireproof Walls, Floors and Ceilings of the Computer Room
With the assistance of building management, the documentation that identifies the fire rating of the walls surrounding the IPF should be located. These walls should have at least a two-hour fire resistance rating.

Electrical Surge Protectors
The presence of electrical surge protectors on sensitive and expensive computer equipment should be visually observed.

Power Leads From Two Substations
With the assistance of building management, documentation concerning the use and placement of redundant power lines into the IPF should be located.

Fully Documented and Tested Business Continuity Plan
See the content area, business continuity and disaster recovery in chapter 6, for a description of testing the business continuity plans.

Wiring Placed in Electrical Panels and Conduit
Wiring in the IPF should be placed in fire-resistant panels and conduit.

UPS/Generator
The most recent test date should be determined and the test reports should be reviewed.

Documented and Tested Emergency Evacuation Plans
A copy of the emergency evacuation plan should be obtained. It should be examined to determine whether it describes how to leave the IPFs in an organized manner that does not leave the facilities physically insecure. A sample of IS employees should be interviewed to determine if they are familiar with the documented plan. The emergency evacuation plans should be posted throughout the facilities.

Humidity/Temperature Control
The IPF should be visited on regular intervals to determine whether temperature and humidity are adequate.

5.8 PHYSICAL ACCESS EXPOSURES AND CONTROLS

Physical exposures could result in financial loss, legal repercussions, loss of credibility or loss of competitive edge. They primarily originate from natural and man-made hazards, and can expose the business to unauthorized access and unavailability of the business information.

5.8.1 PHYSICAL ACCESS ISSUES AND EXPOSURES
Physical access issues are a major concern in security. Exposures and possible perpetrators are described in the following subsections.

Physical Access Exposures
Exposures that exist from accidental or intentional violation of these access paths include:
- Unauthorized entry
- Damage, vandalism or theft to equipment or documents
- Copying or viewing of sensitive or copyrighted information
- Alteration of sensitive equipment and information
- Public disclosure of sensitive information
- Abuse of data processing resources
- Blackmail
- Embezzlement

Possible Perpetrators
Possible perpetrators include employees with authorized or unauthorized access who are:
- Disgruntled (upset by or concerned about some action by the organization or its management)
- On strike
- Threatened by disciplinary action or dismissal
- Addicted to a substance or gambling
- Experiencing financial or emotional problems
- Notified of their termination

Other possible perpetrators could include:
- Former employees
- Interested or informed outsiders such as competitors, thieves, organized crime and hackers
- An accidental ignorant, for example, someone who unknowingly perpetrates a violation (e.g., an employee or outsider)

The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.

Other questions and concerns to consider include the following:
- Are hardware facilities reasonably protected against forced entry?
- Are keys to the computer facilities adequately controlled to reduce the risk of unauthorized access?
- Are computer terminals locked or otherwise secured to prevent removal of boards, chips and the computer itself?
- Are authorized equipment passes required before computer equipment can be removed from its normal secure surroundings?

From an IS perspective, facilities to be protected include:
- Programming area
- Computer room
- Operator consoles and terminals
- Tape library, tapes, disks and all magnetic media
- Storage rooms and supplies
- Offsite backup file storage facility
- Input/output control room
- Communications closets
- Telecommunications equipment (including radios, satellites, wiring, modems and external network connections)
- Microcomputers and personal computers (PCs)
- Power sources
- Disposal sites
- Minicomputer establishments
- Dedicated telephones/telephone lines
- Control units and front-end processors
- Portable equipment (handheld scanners and coding devices, bar code readers, laptop computers and notebooks, printers, pocket LAN adapters and others)
- Onsite and remote printers
- Local area networks

Additionally, system, infrastructure or software application documentation should be protected against unauthorized access.

For these safeguards to be effective, they must extend beyond the computer facility to include any vulnerable access points within the entire organization and at organizational boundaries/interfaces with external organizations. This may include remote locations and rented, leased or shared facilities. Additionally, the IS auditor may require assurances that similar controls exist within service providers or other third parties, if they are potentially vulnerable access points to sensitive information within the organization.

5.8.2 PHYSICAL ACCESS CONTROLS

Physical access controls are designed to protect the organization from unauthorized access. These controls should limit access to only those individuals authorized by management. This authorization may be explicit, as in a door lock for which management has authorized you to have a key, or implicit, as in a job description that implies a need to access sensitive reports and documents. Examples of some of the more common access controls are:
- **Bolting door locks**—These locks require the traditional metal key to gain entry. The key should be stamped "do not duplicate" and should be stored and issued under strict management control.
- **Combination door locks (cipher locks)**—This system uses a numeric key pad or dial to gain entry. The combination should be changed at regular intervals or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces the risk of the combination being known by unauthorized people.
- **Electronic door locks**—This system uses a magnetic or embedded chip-based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by the sensor device that then activates the door locking mechanism. Electronic door locks have the following advantages over bolting and combination locks:
  - Through the special internal code, cards can be assigned to an identifiable individual.
  - Through the special internal code and sensor devices, access can be restricted based on the individual's unique access needs. Restrictions can be assigned to particular doors or to particular hours of the day.
  - They are difficult to duplicate.
  - Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. Silent or audible alarms can be automatically activated, if unauthorized entry is attempted. Issuing, accounting for and retrieving the card keys is an administrative process that should be carefully controlled. The card key is an important item to retrieve when an employee leaves the firm. An example of a common technique used for card entry is the swipe card. A swipe card is a physical control technique that uses a plastic card with a magnetic strip containing encoded data to provide access to restricted or secure locations. The encoded data can be read by a slotted electronic device. After a card has been swiped, the application attached to the slotted electronic device prevents unauthorized physical access to those sensitive locations, as well as logs all card users that try to gain access to the secure location.
- **Biometric door locks**—An individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.
- **Manual logging**—All visitors should be required to sign a visitor's log indicating their name, company representative, reason for visiting, person to see and date and time of entry and departure. Logging typically is at the front reception desk and entrance to the computer room. Before gaining access, visitors should also be required to provide verification of identification such as a driver's license, business card or vendor identification tag.
- **Electronic logging**—This is a feature of electronic and biometric security systems. All access can be logged, with unsuccessful attempts being highlighted.
- **Identification badges (photo IDs)**—Badges should be worn and displayed by all personnel. Visitor badges should be a different color from employee badges for easy identification. Sophisticated photo IDs can also be utilized as electronic card keys. Issuing, accounting for and retrieving the badges is an administrative process that must be carefully controlled.
- **Video (CCTV) cameras**—Cameras should be located at strategic points and monitored by security guards. Sophisticated video cameras can be activated by motion. The video surveillance recording should be retained for possible future playback.
- **Security guards**—Guards are very useful if supplemented by video cameras and locked doors. Guards supplied by an external agency should be bonded to protect the organization from loss.

- **Controlled visitor access**—All visitors should be escorted by a responsible employee. Visitors include friends, maintenance personnel, computer vendors, consultants (unless long-term, in which case special guest access may be provided) and external auditors.
- **Bonded personnel**—All service contract personnel, such as cleaning people and offsite storage services, should be bonded. This does not improve physical security but limits the financial exposure of the organization.
- **Deadman doors**—This system, which uses two doors, is typically found in entries to facilities such as computer rooms and document stations. For the second door to operate, the first entry door must close and lock, with only one person permitted in the holding area. This reduces the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry.
- **Not advertising the location of sensitive facilities**—Facilities such as computer rooms should not be visible or identifiable from the outside, that is, no windows or directional signs. The building or department directory should discreetly identify only the general location of the information processing facility.
- **Computer workstation locks**—These lock the device to the desk, prevent the computer from being turned on or disengage keyboard recognition, thus preventing use. Another available feature is locks that prevent turning on a PC workstation until a key lock is unlocked by a turn key or card key.
- **Controlled single entry point**—A controlled entry point monitored by a receptionist should be used by all incoming personnel. Multiple entry points increase the risk of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.
- **Alarm system**—An alarm system should be linked to inactive entry points, motion detectors, and the reverse flow of enter- or exit-only doors. Security personnel should be able to hear the alarm when activated.
- **Secured report/document distribution cart**—Secured carts, such as mail carts, should be covered and locked and should not be left unattended.
- **Windows**—Ideally the computer room should not have externally facing windows: where these are present, they should be constructed of reinforced glass and, if on the ground floor of the building, further protected for example, by bars.

5.8.3 AUDITING PHYSICAL ACCESS

Touring the computer site is useful to gain an overall understanding and perception of the installation being reviewed. This tour provides the opportunity to begin reviewing physical access restrictions (e.g., control over employees, visitors, intruders and vendors).

The computer site (i.e., computer room, programmers' area, tape library, printer stations and management offices) and any offsite storage facilities should be included in this tour.

Much of the testing of physical safeguards can be achieved by visually observing the previously noted safeguards. Documents to assist with this effort include emergency evacuation procedures, inspection tags (recent inspection?), fire suppression system test results (successful? recently tested?) and key lock logs (all keys accounted for and not outstanding to former employees or consultants?).

Testing should extend beyond the IPF/computer room to include the following related facilities:
- Location of all operator consoles
- Printer rooms
- Computer storage rooms (this includes equipment, paper and supply rooms)
- UPS/generator
- Location of all communications equipment identified on the network diagram
- Tape library
- Offsite backup storage facility

To complete a thorough testing, the IS auditor should look above the ceiling panels and below the raised floor in the computer operations center, observing smoke and water detectors, general cleanliness, and walls that extend all the way to the real ceiling (not just the fake/suspended ceiling). For a ground-floor computer room, the auditor may also consider walking around the outside of the room, viewing the location of any windows, examining emergency exit doors for evidence that they are routinely used (such as the presence of cigarette stubs or litter) and examining the air conditioning units. The auditor should also consider whether any additional threats exist close to the room, such as storage of dangerous or flammable material.

The following paths of physical entry should be evaluated for proper security:
- All entry doors
- Emergency exit doors
- Glass windows and walls
- Movable walls and modular cubicles
- Above suspended ceilings and beneath raised floors
- Ventilation systems
- Over a curtain, fake wall

5.9 MOBILE COMPUTING

In today's mobile computing environment, it is not unusual to keep sensitive data on PCs and diskettes, particularly laptops, where it is more difficult to implement logical and physical access controls. Protecting laptop data confidentiality requires a layered security approach at both physical and logical access levels, as well as a laptop security policy and safe practices guidelines. In particular, the following controls will reduce the risk of disclosure of sensitive data stored on a laptop:
- Engrave or brand a serial number and company name and logo on to a laptop using an electric engraver or tamper resistant tags.
- Use a cable locking system or a locking system with a motion detector that sounds an audible alarm.
- Back up business critical or sensitive data on a regular basis, both at work (using shared folders on the company's file server) and while traveling (using flash drives or online backup solutions).
- Encrypt data using well-known encryption software that is based on public domain algorithms and is not proprietary. The decision what to encrypt can be left to the user, by creating designated volumes in which encrypted files are stored and processed. An alternative approach encrypts the entire hard drive, leaving nothing to the discretion of the user.

- Allocate passwords to individual files to prevent them from being opened by an unauthorized person, that is, one not in possession of the password. This facility should be used with great caution since, should the password be forgotten, or the person who created it leave the organization, the data would be unavailable because the password cannot be circumvented.
- Establish a theft response team and develop procedures to follow when a laptop is stolen. These procedures should include identifying the stolen laptop, reporting the loss of the laptop to local authorities, assessing the importance or criticality of the compromised data and determining if clients or other third parties are affected by the theft.

As laptops are often used for the remote logging into the computer systems of the organization, special care should be taken to defend against malicious code. The best solution is to centralize virus signature updates and the handling of patches to the operating system.

Laptop security can be hardened by using two-factor authentication. This can be achieved using biometric readers, or devices that are possessed by the user.

5.10 CASE STUDIES

The following case studies are included as a learning tool to reinforce the concepts introduced in this chapter. Exam candidates should note that the CISA exam does not currently use this format for testing.

5.10.1 CASE STUDY A

Case Study A Scenario

Management is currently considering ways in which to enhance the physical security and protection of its data center. The IS auditor has been asked to assist in this process by evaluating the current environment and making recommendations for improvement. The data center consists of 15,000 square feet (1,395 square meters) of raised flooring on the ground floor of the corporate headquarters building. A total of 22 operations personnel require regular access. Currently, access to the data center is obtained using a proximity card, which is assigned to each authorized individual. There are three entrances to the data center, each of which utilizes a card reader and has a camera monitoring the entrance. These cameras feed their signals to a monitor at the building reception desk, which cycles through these images along with views from other cameras inside and outside the building. Two of the doors to the data center also have key locks that bypass the electronic system so that a proximity card is not required for entry. Use of proximity cards is written to an electronic log. This log is retained for 45 days. During the review, the IS auditor noted that 64 proximity cards are currently active and issued to various personnel. The data center has no exterior windows, although one wall is glass and overlooks the entry foyer and reception area for the building.

Case Study A Questions	
A1.	Which of the following risks would be mitigated by supplementing the proximity card system with a biometric scanner to provide two-factor authentication? A. Piggybacking or tailgating B. Sharing access cards C. Failure to log access D. Copying of keys
A2.	Which of the following access mechanisms would present the greatest difficulty in terms of user acceptance? A. Hand geometry recognition B. Fingerprints C. Retina scanning D. Voice recognition
See answers and explanations to the practice questions at the end of the chapter (page 360).	

5.10.2 CASE STUDY B

Case Study B Scenario

A company needed to enable remote access to one of its servers for remote maintenance purposes. Firewall policy did not allow any external access to the internal systems. Therefore, it was decided to install a modem on that server and to activate the remote access service to permit dial-up access. As a control, a policy has been implemented to manually power on the modem only when the third party was requesting access to the server and powered off by the company's system administrator when the access is no longer needed. As more and more systems are being maintained remotely, the company is asking an IS auditor to evaluate the current risks of the existing solution and to propose the best strategy for addressing future connectivity requirements.

Dase Study B Questions	
B1.	What test is **MOST** important for the IS auditor to perform as part of the review of dial-up access controls? A. Dial the server from authorized and unauthorized telephone lines B. Determine bandwidth requirements of remote maintenance and the maximum line capacity C. Check if the availability of the line is guaranteed to allow remote access any time D. Check if call back is not used and the cost of calls is charged to the third party
B2.	What is the **MOST** significant risk that the IS auditor should evaluate regarding the existing remote access practice? A. Modem is not powered on/off whenever is needed B. A nondisclosure agreement was not signed by the third party C. Data exchanged over the line is not encrypted D. Firewall controls are bypassed
B3.	Which of the following recommendations is **MOST** likely to reduce the current level of remote access risks? A. Maintain an access log with the date and time when the modem was powered on/off B. Encrypt the traffic over the telephone line C. Migrate the dial-up access to an Internet VPN solution D. Update firewall policies and implement an IDS system
B4.	What control should be implemented to prevent an attack on the internal network being initiated though an Internet VPN connection? A. Firewall rules are periodically reviewed B. All VPNs terminate at a single concentrator C. An IDS capable to analyze encrypted traffic is implemented D. Antivirus software is installed on all production servers
See answers and explanations to the practice questions at the end of the chapter (page 360).	

5.10.3 CASE STUDY C

Case Study C Scenario

"My Music" is a company dedicated to the production and distribution of video clips specializing in jazz music. Born in the Internet era, the company has actively supported the use of notebook computers by its staff so they can use them when traveling and when working from home. Through the Internet they can access the company databases and provide online information to customers. This decision has resulted in an increase in productivity and high morale among employees who are allowed to work up to two days a week from home. Based on written procedures and a training course, employees learn security procedures to avoid the risk of unauthorized access to company data. Employees' access to the company data includes using logon IDs and passwords to the application server through a VPN. Initial passwords are assigned by the security administrator. When the employee logs on for the first time, the system forces a password change to improve confidentiality.

Management is currently considering ways to improve security protection for remote access by employees. The IS auditor has been asked to assist in this process by evaluating the current environment and making recommendations for improvement.

Case Study C Questions	
C1.	Which of the following levels provides a higher degree of protection in applying access control software to avoid unauthorized access risks? A. Network and operating system level B. Application level C. Database level D. Log file level
C2.	When an employee notifies the company that he/she has forgotten his/her password, what should be done **FIRST** by the security administrator? A. Allow the system to randomly generate a new password B. Verify the user's identification through a challenge/response system C. Provide the employee with the default password and explain that it should be changed as soon as possible D. Ask the employee to move to the administrator terminal to generate a new password in order to assure confidentiality
See answers and explanations to the practice questions at the end of the chapter (page 360).	

5.10.4 CASE STUDY D

Case Study D Scenario

A major financial institution has just implemented a centralized banking solution (CBS) in one of its branches. It has a secondary concern to look after marketing of the bank. Employees of a separate legal entity work on the bank premises, but they have no access to the bank's solution software. Employees of other branches get training on this solution from this branch and for training purposes temporary access credentials are also given to such employees. IS auditors observed that employees of the separate legal entity also access the CBS software through the branch employees access credentials. IS auditors also observed that there are numerous active IDs of employees who got training from the branch and have since been transferred to their original branch.

Case Study D Questions	
D1.	Which of the following should IS auditors recommend to effectively eliminate such password sharing? A. Assimilation of security need to keep password secret B. Stringent rules prohibiting sharing of password C. Use of smart card along with strong password D. Use of smart card along with employee's terminal ID
D2.	Which of the following **BEST** addresses user ID management of trainee employees? A. Unused user ID shall be automatically deleted periodically B. To integrate access rights with human resource process C. Password of unused but active user ID shall be suspended D. Active user ID register shall checked frequently

See answers and explanations to the practice questions at the end of the chapter (page 360).

5.11 ANSWERS TO CASE STUDY QUESTIONS

ANSWERS TO CASE STUDY A QUESTIONS

A1. **B** Two-factor authentication involving the use of biometrics would effectively prevent the sharing of access cards since these cards would be ineffective without the corresponding biometric. Piggybacking or tailgating would not be mitigated since traffic flow would remain unchanged. Since two entrances utilize key locks that override the electronic entry system, individuals entering using keys would not be logged by the electronic system, and keys could still potentially be copied.

A2. **C** Although the highest in terms of accuracy, many individuals feel uncomfortable with the idea of having a device scan the inside of their eye. So, even though retina scanning may be highest in terms of effectiveness from a control perspective, its lack of user acceptance may make it inappropriate for applications where customer acceptance is of prime importance. Fingerprints, hand geometry and voice recognition are all less invasive and, therefore, not as subject to adverse negative reaction by users. The objective of this area is to ensure that the CISA candidate understands and can provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.

ANSWERS TO CASE STUDY B QUESTIONS

B1. **A** Dial-up access should be possible only from authorized telephone lines as a preventive control for unauthorized access when logon credentials are compromised or misused by third-party personnel. Initiating the connection by the server to an authorized phone number using the call back feature would be one implementation of this requirement. Options B, C and D address performance issues and not access control issues.

B2. **D** The company's security infrastructure relies on controls implemented on the firewall. The fact that someone from the outside can connect directly to an internal system, bypassing firewall rules, could expose the internal network to the third party, thereby facilitating unauthorized access. Choices A, B and C are risks to be considered by the IS auditor, but concern only the server being maintained remotely, and not the entire internal system.

B3. **C** Using an Internet VPN solution will eliminate the vulnerabilities of the dial-up access such as lack of encryption and bypassing firewall controls. Option A and B will address punctual issues and Option D will have no effect since security infrastructure controls are bypassed by the direct dial-up access.

B4. **C** An IDS should be able to analyze the encrypted traffic of the VPN connection to determine potential attacks. A firewall rules review and ending all VPNs in a single concentrator will prevent unauthorized connections to the internal network, but this will not prevent an attack occurring through an authorized VPN connection. Antivirus software will prevent contamination by computer viruses, but the internal system is still vulnerable to many other threats.

ANSWERS TO CASE STUDY C QUESTIONS

C1. **A** The greatest degree of protection in applying access control software against internal and external users' unauthorized access is at the network and platform/operating system levels. These systems are also referred to as general support systems, and they make up the primary infrastructure on which applications and database systems will reside.

C2. **B** When an employee notifies that he/she has forgotten his/her password, the security administrator should start a password process generation procedure only after verifying the user's identification using a challenge/response system or similar procedure. To verify, it is advised that the security administrator should return the user's call after verifying his/her extension or calling his/her supervisor for verification.

ANSWERS TO CASE STUDY D QUESTIONS

D1. **A** Assimilation of security need to keep password secret can only effectively refrain such password sharing and such assimilation is possible only through continuous and conscientious security awareness and education programs. Without assimilation of security need stringent rules prohibiting sharing of password cannot effectively stop password sharing. Use of smart card along with strong password and use of smart card along with employee's terminal ID do not deter password sharing.

D2. **B** Integration of access rights with human resource process is the best way to address user ID management. Automatic periodic deletion of unused user ID, suspension of password of unused but active user ID and frequently checking active user ID register are not the best way since vulnerability persists during the period in which user IDs remain active.