Exam CISSP®

CISSP®

# Mega Guide

## Prepare With Confidence

This PrepLogic Mega Guide was written by certified subject matter experts and published authors to provide you accurate, in-depth exam coverage. All exam objectives are covered in detail, giving you the knowledge and confidence you need to pass your exam.

PrepLogic

*Be Prepared. Be Confident. Get Certified.*

Christopher Parker - Managing Editor

PrepLogic, Inc. • 1300 N. Westshore Boulevard, Suite # 125 • Tampa, Florida 33607
Phone: (813) 769-0920 (800) 418-6789 • Fax: (813) 769-0926 • Website: www.preplogic.com

# CISSP® Mega Guide

Product ID: 010015
Production Date: December 1, 2009

## Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

## Volume, Corporate, and Educational Sales

PrepLogic offers favorable discounts on all products when ordered in quantity. For more information, please contact PrepLogic directly:

**1-800-418-6789**
**solutions@preplogic.com**

# Information Security and Risk Management

## Core information security goals

There are three main goals of any information security program that are encapsulated by the CIA Triad:

- Confidentiality – Ensures that private information remains protected from unauthorized disclosure. Confidentiality is often enforced through the use of access controls, encryption, classification policies, and user training.
- Integrity – Ensures that data isn't modified in an unintended manner, either through accidental modification by authorized individuals, or malicious modification by any individual (authorized or unauthorized). Integrity is often enforced through the use of cryptographic hashes and checksums.
- Availability – Ensures that data is always available for the use of authorized individuals. Availability is often enforced through the use of redundant systems, system backups, disaster recovery/business continuity plans, and prevention of denial of service attacks.

## Security Policies Management

Security policies consist of broad statements about the organization's commitment to information security and the goals of the program. A security policy is used to set a common set of expectations to communicate management's goals and objectives. Security standards, guidelines, procedures, and baselines are used to support the implementation of policy. There are a number of different types of security policy including organizational, functional, and system-specific policies.

- *Security standards* – Provide specific technical requirements for security mechanisms. This includes the hardware and software security devices which are selected to control the organization's security risks.
- *Security guidelines* – Are the optional controls which are used to enable the individual to make judgments about their security actions.
- *Security procedures* – Provide step-by-step instructions for performing specific security-related tasks. The procedure will define how a policy is implemented and who is responsible for accomplishing it.
- *Security baseline* – Sets up the specific rules which are needed to implement security controls. Any exceptions to the baseline of a specific system should have both a technical review and a business case supporting it.

There are a number of best practices which are recommended when formulating security policies. There are a number of different factors which go into the writing of a policy; these guidelines should be used to create a good security policy:

- Clearly define policy creation practice
- Write policies that will survive for at least 2 years
- Always use directive wording
- Avoid technical implementation details
- Keep length to a minimum
- Provide navigation from the defined policy to the supporting procedure, standards, guideline, and baseline documents
- Thoroughly review before publishing
- Always conduct a management review
- Avoid techno babble
- Adjust policy as needed
- Develop sanctions for policy non-compliance

## Audit Frameworks

There have been a number of different audit frameworks which have been created to support the auditing of security controls and policies. These are used to assist the design of a security program. These different frameworks are shown below:

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO).
    - Formed to sponsor the National Commission on Fraudulent Financial Reporting
        - Studies factors that lead to fraudulent financial reporting and produces recommendations to follow.
    - Identifies five areas of internal control necessary to meet the financial reporting and disclosure requirements
        - Control Environment
        - Risk Assessment
        - Control Activities
        - Information and Communication
        - Monitoring

- The IT Infrastructure Library (ITIL)
    - Set of 34 books published by the British Government between 1989 and 1992
    - Sets up a framework of best practices, including change, release and configuration management; incident and problem management; capacity and availability management; and IT financial management.
- Control Objectives for Information and related Technology (COBIT)
    - Published by the IT Governance Institute
    - Contains a set of 34 high-level processes
- ISO 17799/BS 7799
    - Originally developed by the U.K. Department of Trade and Industry Code of Practice for information security
    - Became BS 7799 in 1995
    - Part 1 of BS 7799 was published as ISO 17799:2000
    - Revised in 2005 to become ISO 17799:2005
        - Contains 134 detailed information security controls based on 11 areas:
            - Information security policy
            - Organizing information security
            - Asset management
            - Human management
            - Physical and environmental security
            - Communications and operations management
            - Access Control
            - Information systems acquisition, development, and maintenance.
            - Business continuity management
            - Compliance

## Information security best practices

There are a number of best practices which can be followed to limit the potential of individuals causing security threats. While these can be hard to implement for some smaller businesses that do not have the staff resources it is recommended that the ones that are possible be implemented.

- Job Rotation – The rotation of job responsibilities limits the ability of individuals to gain through collusion. Job rotation also allows the uncovering of any abnormal activities performed by the previous job owner.
- Separation of Duties – No one individual should have the capability to execute all of the steps of a process.
- Least Privilege – This involves only providing the access absolutely needed for an individual to perform their duties.
- Mandatory Vacations – Mandating a consecutive day vacation allows the duties of an individual to pass to someone else temporarily which can point out any irregularities in their activities.
- Job Position Sensitivity – The access and duties of specific individuals should be measured based on the sensitivity of the position.

## Information security officer responsibilities

The following is a brief list of the main duties of the information security officer in a company. The person in this position is responsible for ensuring the security of all company information assets.

- Communicates risks to executive management – The information security officer is responsible for performing risk analyses and communicating these risks to the executives of the company.
- Budget for information security activities – The information security officer responsible for preparation of budget to manage companywide information security programs.
- Ensuring the development of security standards, guidelines, procedures, and baselines – The information security officer is responsible for making sure that these different items are completed and well documented, however it does not mean that the officer is responsible for writing them.
- Develop and provide Security Awareness Program – The information security officer is responsible for leading an Information Security awareness campaign.
- Understanding fundamental business objectives – The information security officer is responsible for understanding the company's objectives in order to best plan for the security implications inside the company.
- Maintain awareness of emerging threats and vulnerabilities – The information security officer is responsible for staying current on potential future threats and vulnerabilities.
- Evaluate security incidents and response – The information security officer is responsible for operating Computer Incident Response Teams (CIRT) to deal with security incidents as they come up within the company. The CIRTs should include a group of individuals who have a wide range of expertise including management, technical, infrastructure, and communications.
- Develop Security Compliance Program – The information security officer is responsible for developing and maintaining an active security compliance program which keeps a close eye on policy adherence.

- Developing and Maintaining security metrics program – The information security officer is responsible for keeping a number of both long- and short-term security metrics which can be used to optimize company operations.
- Participate in management meetings – The information security officer is responsible for being involved with management in making all planning decisions.
- Ensure compliance with government regulations – The information security officer is responsible for keeping track of all existing and future government regulation changes.
- Assisting Internal and External auditors – The information security officer is responsible for helping both internal and external auditors in reviewing the company's security controls.
- Stays aware of emerging technologies – The information security officer is responsible for maintaining knowledge of new technologies as they emerge onto the market, as well as the analysis of these new technologies and their use in the company's systems.

## Reporting Models

It is imperative that the information security organization report as high in the company as possible in order to keep the proper amount of visibility on information security topics and to limit the amount of distortion which can happen to information which is translated through layers of bureaucracy. The following are some of the different reporting structures which exist:

- Reporting directly to the CEO – This reporting model is often preferred by information security professionals as it dramatically increases the visibility of information security issues and reflects a serious interest in information security on the part of the CEO of the company.
- Reporting to the Information Technology (IT) department – In this reporting mode the information security officer reports directly to the head of IT. While this has the advantage of being useful for many of the technical security functions, it can be a problem if the head of IT has alternative priorities which counter information security requirements.
- Reporting to corporate security – This has the advantage of putting the information security officer under a security branch of the company which can be a disadvantage because many corporate security departments are focused on physical and not information security.
- Reporting to the administrative services department – This reporting structure has its advantages because the department has access not only to the technological information security resources, but also the other forms of information including paper. The disadvantage is the head of this department may not have the technical skills which are required to inform the CEO of specific information security issues.
- Reporting to the insurance and risk management department – While this type of reporting model may have its advantages in certain industries (banking), it has the same downside with other reporting structures with management not having sufficient technical skill to convey technological information security issues.
- Reporting to the internal audit department – This reporting model causes a conflict of interest as it is the job of the internal audit department to evaluate the effectiveness of the organization's control structure including information security.
- Reporting to the legal department – While this reporting model may be useful in highly regulated industries, it is not the best fit as this department's focus in information security is mainly compliance.

## Personnel Security

One of the main things which can affect the security of a company is their personnel. It is important that the personnel of the company are trustworthy and competent. In order to maintain a high level of security it is imperative to implement thorough personnel security controls. The following hiring practices are recommended prior to an individual beginning employment:

- Advertise a well-written, thorough job description.
- Obtain signed employee agreement(s) which include non-disclosure agreements and intellectual property agreements.
- Perform a number of reference checks.
- Perform background checks on applicants, including criminal checks.
- Perform credit checks on applicants (typically done in financial industries).
- Perform driving checks on applicants using company equipment.
- Perform drug or substance abuse tests.
- Perform education, licensing and certification verifications.
- Perform social security number verification tests.
- Perform terrorist watchlist checks

## Security Awareness Training

All organizations should provide some level of information security training to all employees. The type, depth, and scope of the training should vary based on the needs of the organization and the individual responsibilities of the trainee with respect to information security.

Elements of a security awareness training program usually include:

- Initial training for new employees upon hire or orientation
- Recurring training for existing employees
- Retraining for employees who gain new responsibilities
- Remedial training for employees responsible for security incidents
- Security reminders for all employees
    - Posters
    - E-mail messages
    - Newsletters

There are several levels of security awareness that should be addressed:

- Security awareness focuses on raising the overall awareness of individuals to their security responsibilities.
- Security training provides specific job-related knowledge for employees depending on the level of their information security responsibilities.
- Security education provides more general security background knowledge to information security professionals. Not all components of education are job-related. For example, a security professional might be trained in all ten CISSP CBK domains but practice only one or two of them on a day-to-day basis.
- Security certification, through programs such as the CISSP, provides external assurances that an individual has met certain standardized requirements for the profession.

## Risk Management

The prime objective of security controls is to reduce the effects of threats and vulnerabilities to a level that is tolerable (i.e., mitigate risk). It is important to remember that the entire risk management process should be based upon prior determination of the value of particular data elements. It would be nonsensical to spend more on protecting a data element than that data element is worth in the first place.

### Risk Analysis (RA)

A risk is a potential harm or loss to a system; the probability that a threat will materialize.

- Identifying risks:
  - Actual threat
  - Possible consequences if threat is realized
  - Probable frequency of occurrence of threat
  - Confidence threat will happen

**Key Terms**

- Asset – A resource, process, product, system, etc. The value is composed of cost of creation, development, license, support, replacement, public credibility, considered costs, lost intellectual property if disclosed, and ownership values.
- Threat – Any event that causes an undesirable impact on an organization. Data classification, information warfare, personnel, criminal, application, operational.
- Vulnerability – Absence of a safeguard.
- RM triple – Asset, threat, and vulnerability.
- Exploit – A technical means to exploit a vulnerability.
- Exposure Factor (EF) – Percentage loss a realized threat would have on an asset. A hardware failure on a critical system may result in 100% loss.
- Single Loss Expectancy (SLE) – Loss from a single threat. SLE = Asset Value($) x EF.

- Annualized Rate of Occurrence (ARO) – Estimated frequency in which a threat is expected to occur. The ARO range is from 0 (never) to a large number (e.g., minor threats, such as misspellings).
- Annualized Loss Expectancy (ALE) – The total of the SLE multiplied by the ARO. ALE = SLE x ARO
- Safeguard – Control or countermeasure to reduce risk associated with a threat.
  - The absence of a safeguard creates a vulnerability.
  - Look at the cost/benefit analysis of deploying a safeguard. Include the impact on the organization of implementing the safeguard.
  - The safeguard must be auditable.
  - Value to organization of safeguard = ALE (before implementation) – ALE (after implementation) – annualized safeguard cost.

### Elements of Risk Analysis

- Quantitative RA – Assigns objective dollar costs to assets
- Qualitative RA – Intangible values of data loss and other issues that are not pure hard costs (i.e. high, medium, and low risk categories)

### Risk Analysis Steps

1. Identify asset. Estimate potential losses to assets by determining their values.
2. Identify threats. Analyze potential threats to assets.
3. Determine risk. Qualitatively and/or quantitatively evaluate the degree of risk.

## Risk Management Techniques

Once you have identified risks, you may choose one or more of the following four risk management techniques for each identified risk:

- Mitigate the risk – Put controls in place that reduce the risk to the organization (e.g., install a lock on a door to reduce the risk of unauthorized entry).
- Avoid the risk – Change the organization's activities to completely avoid the risk (e.g., move from Florida to Indiana to avoid hurricanes).
- Accept the risk – Acknowledge the risk and take no action whatsoever (e.g., realize that there's a slight chance that a volcano might erupt in southern California but accept that risk without doing anything about it).
- Transfer the risk – Place the burden of the risk on someone else (i.e., buy insurance to protect against fire).

# Access Control

## Key Concepts

There are four main concepts which are used to enable security management:

- Specification of users who can access the system – During this step the individuals who can access the given system or information are determined.
- Specification of what resources these users can access – During this step the specific resources which will be accessible to both individuals and to the community will be determined.
- Specification of what operations the users can perform – During this step the specific levels of permission are determined both for each user and for each resource.
- The ability to provide individual accountability – This step makes sure that it is possible for the company to administer individual accounting for the specific actions that are taken.

## Information Classification

ISC$^2$ defines information classification as "The practice of evaluating the risk level of the organization's information to ensure that the information receives the appropriate level of protection." It is important that the information within a company be classified, as this enables the control of which information is able to be accessed by specific individuals and groups, as well as several other advantages.

In order to provide a good system of classification, it is important that a data classification program be established. The following are the recommended steps to follow in establishing a data classification program:

1. Determine data classification project objectives – Involves the documentation of specific project objectives that contain the scope of the effort and determine when the early deliverables are completed.
2. Establish organizational support – Involves the essential continued operational support of senior management within the company.
3. Develop data classification policy – Involves the development of a policy which communicates the requirements to classify the information assets to the company.
4. Develop data classification standard – Involves the development of a standard which communicates how to determine the classification of a specific information item and how each item should be handled.
5. Develop data classification process flow and procedure – Involves the development of a process and procedure which communicate the individual roles and requirements which are required for all involved parties.
6. Develop tools to support process – Involves the development of a process which dictates how the various tools used by the company can be used to effectively help the data classification process.
7. Indentify application owners – Involves the identification of all specific business owners of each application. These individuals are typically the ones most aware of how the applications and the data from them are used.

8. Identify data owners and data owner delegates – Involves the identification of all specific data owners. These individuals are typically the ones most aware of the specific data and how it is used.
9. Distribute standard templates – Involves the distribution of a template which is developed from the earlier steps and can be used by all parties to classify their data.
10. Classify information and applications – Involves the actual classification of all data by their specific owners using the template distributed. There are typically three to four main levels of classification which are used in most companies:
    - Public – Able to be disclosed to the general public.
    - Internal Use Only – Able to be disclosed to individuals within the company.
    - Confidential – Able to be disclosed to only specific individuals within a company as the information could cause serious harm to the company if it was released publically. This includes information like trade secrets, intellectual property, and research designs, among others.
    - Another higher level of security – Some companies need an additional level of security above these pre-defined levels; these companies create their own, internal labels.
11. Develop auditing procedures – Involves the process of reviewing specific classifications to ensure the accuracy of the information.
12. Load information into central repository – Involves the development of a central repository tool which is used to provide the ability to examine the classification information from multiple perspectives.
13. Train users – Involves the training of users on the use of the specific data classifications and how to use them and handle them correctly.
14. Periodically review and update data classifications – Involves the review of the data classification policy and standards as well as a review of the specific classifications being used.

## Control Categories

There are many different types of control categories:

- *Preventative controls* – Designed to prevent unwanted activity from occurring.
- *Detective controls* – Provide a means of discovering unwanted activities that have occurred.
- *Corrective controls* – Provide mechanisms for bringing a system back to its original state prior to the unwanted activity.
- *Deterrent controls* – Used to discourage individuals from attempting to perform undesired activities.
- *Compensatory controls* – Implemented to make up for deficiencies in other controls.
- *Recovery* – Involves the recovery of conditions back to normal.

## Types of Controls

- Administrative controls – Consist of policies and procedures, disaster recovery plans, awareness training, security reviews and audits, background checks, review of vacation history, separation of duties, and job rotation.
- Physical controls – Protect access to the physical facilities housing information systems and include guards and building security, biometric access restrictions, protection of cables, file backups.
- Logical/Technical controls – Restrict access to systems and the protection of information. Encryption, smart cards, anti-virus software, audit trails, log files, ACLs, biometrics, and transmission protocols (e.g., Kerberos and Internet Protocol Security [IPSec]).

## Access Control Threats

Access controls are vulnerable to a number of threat types. These include:

- Denial of service (DoS) – It is not necessary to break into a system to successfully attack it. Attackers can confuse the system into an inoperable state or flood it with so much traffic that it can't provide service to legitimate users. DoS can be just as effective as a successful penetration.
- Buffer overflows – Sometimes it is possible for an attacker to use poorly coded memory management and control to gain control of the system's memory buffer (or one of them). It is possible for an attacker to use this vulnerability for a number of different attacks including DoS and malicious code injection.
- Mobile Code – This type of threat involves code which is downloaded from a remote location and run on the local device. This can include a number of different technologies including Java, ActiveX, and other scripting languages.
- Malicious Software – This threat involves a number of different methods of attack including infected software, applications, applets, and scripts, among others. Inside these categories are a number of different sub-types of threat which are commonly known:
  - Viruses
  - Worms
  - Trojan Horses
  - Spyware
  - Malware
- Password Crackers – This type of threat involves many different types of techniques which are used to obtain a secret password or passphrase. There are several different techniques, including:
  - Brute force – In this type of attack, the attacker simply guesses passwords over and over again until eventually succeeding. Brute force attacks are especially effective against short passwords or cryptographic keys.
  - Dictionary – In this type of attack, the attacker uses the password encryption algorithm to encrypt a dictionary of common words, and then compares the encrypted words to the password file. When a match is found, the attacker has discovered a password. This type of attack makes it important to ensure that users do not have real-word passwords.

- Spoofing – These attacks occur when an individual or system poses as a third party. Spoofing attacks are especially effective against standard e-mail, which performs no sender authentication.
- Sniffers, Eavesdropping, and Tapping – Communication at some point needs to be passed from one location to another through networks. It is possible to use one of these methods to "listen" to the information being passed between parties. There are a number of different techniques for performing this, including:
    - Man-in-the-middle – A malicious individual might be able to convince two communicating parties that they are communicating with each other when they are both actually communicating with the intruder. The intruder passes all traffic through to the other end but may eavesdrop on the conversation or even alter the content of the communication.
    - Sniffer – An individual who has access to a network may be able to install and run software like tcpdump or Ethereal that allow a user to "sniff" (or monitor) all traffic occurring on the same network segment.
- Emanations – These attacks use the proliferation of a signal to obtain information which can be used to either perform another attack or to obtain the data itself. This is most obvious with wireless networks which have ranges outside the intended company premises. This can also be an issue with electrical communications lines as they can be listened to by using the electromagnetic loops created by the communications equipment on either side of the cable.
- Shoulder Surfing – This is a social style of attack as it requires that the attacker be close to the intended victim and use direct observation of the target.
- Data Reminisce – This involves the removal of information which was not completely removed from recycled equipment. Many different companies recycle their equipment which includes the original hard drive equipment, which can be used by attackers if the data was not properly removed and overwritten on the drive.
- Unauthorized Targeted Data Mining – This involves the collection of a large amount of data to be used to perform predictions. If enough information is obtained it may be possible for an attacker to predict the various operations, practices, technical architecture, and business cycles of a business.
- Dumpster Diving – Sometimes it is best for an attack to use a simple style of attack to obtain very useful information. This is done through the simple removal of potentially useful data from a company's trash.
- Backdoor/Trapdoors – These are access points which are created by an application or hardware developer to obtain high-level access easily without using the front-door of the system. If these become known to an attacker then a line of protection is instantly removed.
- Theft – Theft can be done by a number of different means outside the traditional unauthorized physical removal of an item. This can include anything from theft of network and phone services to unauthorized power use.
- Social Engineering – This is one of the oldest styles of attack as it requires no amount of technical know-how but simply an ability to remove useful information from unsuspecting individuals inside a company.

## System Access

Access control systems are designed to enforce the requirement that resources be available only to authorized individuals. The process of ensuring accountability for access to system resources includes four phases:

- *Identification phase* – The user makes a claim as to his or her identity. This is usually as simple as entering a user name. At this point the system makes no judgment about the validity of this claim.
- *Authentication phase* – The user proves his or her identity using one or more authentication mechanisms. When the system verifies these mechanisms, the user is authenticated and the system believes the identity claim made in the previous phase.
- *Authorization phase* – The system makes decisions about what resources the user is allowed to access and the manner in which they may be manipulated.
- Accounting phase – The system keeps an accurate audit trail of the user's activity.

## Authentication Types

There are three different types of authentication including:

- Authentication by knowledge – What a person knows
- Authentication by ownership – What a person has
- Authentication by characteristic – What a person is or does

### Authentication by knowledge

The typical representation of authentication by knowledge is that of a password. A password is used by an individual to obtain access to specific resources inside or outside a company. Passwords are the most commonly implemented authentication technique. There are a number of principles you should keep in mind when using password authentication:

- Passwords should only be known to a single individual and should never be shared unless absolutely necessary.
- Strong passwords should not contain dictionary words.
- Strong passwords should not be a variant of the username.
- Strong passwords should contain at least eight characters.
- Strong passwords should contain a combination of uppercase letters, lowercase letters, numbers, and punctuation.

Another form of authentication by knowledge is that of a passphrase. Passphrases are typically longer then passwords and are harder to attack.

## Authentication by ownership

Typically a user utilizing authentication by ownership is provided a token or smart device. This token or device is either used in place of or in addition to a password or passphrase. When used in addition to a password or passphrase it is considered a two-factor method. There are two types of two-factor security methods:

- Asynchronous
    - Challenge Response Technology
    - Dialog is required between the device and a authentication service
- Synchronous
    - Authorization is based on event-based, location-based, or time-based synchronization.

There are also two main authentication devices which are used to authenticate users: a memory card or a smart card. The main difference between the two is the ability of a smart card to process information while the memory card requires a separate device to process the data. Another problem exists with memory cards: the data on the device is not encrypted and, thus, not protected. The smart cards have the ability to protect the data through security control built into the integrated circuit.

There are two basic types of smart cards, and they differ in the way that they interact with other systems. One communicates with other systems through physical contact, and the other uses proximity technology. Cards using physical connections use a contact systems based on ISO 7816-2 and provide 8 total electrical contacts, 6 of which are currently used. Proximity technology-based smart cards are gaining popularity because of their durability. These proximity technologies work by utilizing an inductive loop using low-frequency electronic magnetic radiation. A Proximity Coupling Device (PCD) provides all power and signaling control with the card.

## Authentication by characteristic

There are a number of different characteristics which can be measured in order to authenticate a specific user. Biometrics is used to determine specific biological indicators of the human body or behavioral characteristics that can be used to calculate uniqueness. There are two different types of biometrics:

- Physiological
- Behavioral

### Physiological Biometrics

Physiological biometrics uses unique physical characteristics to obtain the identity of a person. There are number of different characteristics used to identify people, including:

- Fingerprints – one of the oldest used biometrics, unique for each individual.
- Hand geometry – discerns several attributes from each individual's hand to determine identity.
- Palm and hand scans – combines capabilities of fingerprints and hand geometry.
- Retina scanning – scans the blood vessels at the back of the eye to identify distinctive patterns.
- Iris scanning – scans the color material surrounding the pupil to determine granular characteristics in order to identify an individual.
- Voice pattern recognition – matches prerecorded voice patterns against a currently drawn sample.
- Facial recognition – compares preexisting facial scans to a current scan or video sample. Uses both facial geometry and heat signature in order to determine a match.

### Behavioral Biometrics

Behavioral biometrics works by determining unique characteristics about a person from different patterns in their actions. The most common of these in use is key stroke dynamics which not only matches against a preexisting password or passphrase but also compares how an individual types these in.

### Biometric Elements

- The **False Rejection Rate (FRR)** consists of the percentage of cases in which a valid user is incorrectly rejected by the system. This type of mistake is known as a Type I error. A high FRR may frustrate system users. The FRR may be decreased by lowering the sensitivity of the system.
- The **False Acceptance Rate (FAR)** consists of the percentage of cases in which an invalid user is incorrectly accepted by the system. This type of mistake is known as a Type II error. A high FAR jeopardizes system security. The FAR may be decreased by increasing the sensitivity of the system.
- The **Crossover Error Rate (CER)** is the rate at which FRR=FAR for any given system. The CER is commonly used to compare the accuracy of disparate systems. The lower the CER, the more accurate the system.

## Control System Architecture

- Host – a system user application or services providing an identification and authentication interface.
- Requester – a system providing a challenge to the host also commonly referred to as a network access server or NAS.
- Authenticator – a system that performs validation of an individual's credentials.

## Identity Management

ISC$^2$ defines identity management with the intention to solve difficulties in managing the identity of employees, contractors, customers, partners, and vendors in a highly complex organization. These different technologies attempt to simplify the administration of several distributed overlapping organizational technology systems.

### Identity Management Challenges

There are many different challenges that come with the management of identities in a corporate environment, including: the provisioning of user processes, oversight, and management. There are several problems that arise using the standard identity methods including:

- Backlog of access right requests
- Delayed requests
- Complex policies and procedures cause errors
- Identity management forms are not fully completed
- Precise auditing reports are rarely maintained
- Departed or terminated employee user profiles are not deleted in a timely manner

### Identity Management Solutions

There are a number of recommended guidelines that can be followed to reduce identity management problems:

- Consistency – User profile data should be consistent across various systems.
- Efficiency – Reduce the amount of user setup by using various tools available that eliminate repetitive user profile data entry.
- Usability – A reduction of multiple system login prompts.
- Reliability – User profile data should be reliable across all systems.
- Scalability – The identity management solution should provide a high amount of scalability across the entire organization.

### Identity Management Technologies

A comprehensive identity management solution needs to allow the streamlining of the management process, including the management of data consistency across multiple systems. The various technologies that provide this include:

- Directories – A comprehensive system designed to centralize the management of data.
- Web access management – This solution provides a single sign-on process for various web based applications. Typically implemented using a plug-in on a front end web server.
- Password management – Involves the creation of a password policy which ensures both password freshness and password complexity. These systems can also be used to provide a single repository of various system passwords that allow a single password to be entered to log into multiple systems.
- Legacy single sign-on – These types of systems offer a single master system which manages the repeated prompting of sign-on of multiple systems.
- Account management – These systems will include the creation modification and decommission of users within a company.
- Profile update – The maintenance of user profiles that include personal information as well as related privileges.

## Access Control Technologies

There are four different access control technologies:

- Single sign-on (SSO)
- Kerberos
- Secure European System for Applications in a Multi-Vendor Environment (SESAME)
- Security Domains

### Single sign-on

A single sign-on technology is simply a system which allows a single login session which then enables a user to access multiple systems. There are a number of advantages to this type of system, including an efficient login process, and the potential for stronger passwords. There are, however, disadvantages to using this type of system, such as the risk of a single compromised password providing system-wide access. It may also be very complex to interconnect multiple types of systems using this system.

## Kerberos

Kerberos is software used on a network to establish a user's identity. Kerberos uses symmetric key encryption. Users/systems are given tickets that can be used to identify themselves to other systems and secret crypto keys are provisioned for secure communications.

Kerberos consists of three components:

- Key Distribution Center (KDC)
- Authentication Service (AS)
- Ticket Granting Service (TGS)

Kerberos authentication takes place following this six-step process:

1. The client contacts the AS on the KDC and requests a Ticket Granting Ticket (TGT).
2. The AS sends the client a TGT encrypted with the TGS key and a session key used to communicate with the TGS encrypted with the user's key.
3. The client sends a message to the TGS containing a request for authentication to a particular service, the TGT obtained from the AS and an authenticator encrypted with the session key obtained in Step 2.
4. The TGT sends the client a session ticket encrypted with the application server's key and a session key to be used for communication with the application server encrypted with the TGS session key.
5. The client sends the session ticket to the application server along with an authenticator encrypted with the application server session key.
6. The application server verifies the session ticket and grants appropriate access.

## SESAME

Kerberos' greatest weakness is its use of symmetric key cryptography. A public-key based alternative, SESAME, was developed to address some of the weaknesses in Kerberos.

There are many different types of authentication techniques, but they may all be divided into three broad factors:

- Some techniques make use of something you know. The most common technique in this category is the use of a password or passphrase for authentication.
- Other techniques make use of something you have, such as an access token, a physical key, or an identification card.
- The third category of authentication techniques measures something you are. These techniques, known as biometric authentication techniques, include fingerprint scans, retinal scans, voiceprint identification, behavior patterns, and similar measures.

### Security Domains

A security domain is based on a trust between resources or services that share a single security policy and single management. Security domains allow easy support for hierarchical relationships.

## Access Control Systems

There are four types of access control systems:

- Mandatory access control (MAC) – Authorization of subject's access to an object depends on labels (sensitivity levels), which indicate a subject's clearance, and the classification or sensitivity of the relevant object. Every object is assigned a sensitivity level or label and only users authorized up to that particular level can access the object. Access depends on rules and not by the identity of the subjects or objects alone. Only an administrator (not an owner) may change the category of a resource. This is a rule-based AC.
- Discretionary access control (DAC) – Subject has authority, within certain limits, to specify what objects can be accessible (e.g., use of ACL). User-directed means a user has discretion. Identity-based means discretionary access control is based on the subject's identity. This type of control is very common in commercial contexts because of flexibility. Orange Book C level. Relies on object owner to control access. This is an identity-based AC.
- Non-discretionary access control (NDAC) – Administrator determines which subjects can have access to certain objects based on organization's security policy. Access may be based on the individual's role in the organization (role-based) or the subject's responsibilities or duties (task-based).
- Lattice-based access control (LBAC) – Administrator specifies upper and lower bounds of the authority for each subject and uses those boundaries to determine access permissions. LBAC systems are a variant of non-discretionary access controls.

Access control systems may also be classified by their location:

- Centralized access control systems – Serve as a central authentication and/or authorization point for an enterprise. Three common types of centralized ACSs include Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access System (TACAS), and Active Directory. These systems require dedicated hardware and software but offer ease of administration by allowing a single administrator or team of administrators to manage access control from a single point.
- Decentralized access control systems – Consist of a series of diverse access control systems at different points throughout the enterprise. These are normally built into other systems. They normally do not require dedicated hardware or software; however, they are difficult to manage and maintain in a synchronized state.

## Intrusion Detection and Protection Systems

Intrusion detection systems (IDSs) are commonly used to detect malicious activity on a host or network. IDSs are divided based upon the *monitored environment* and the *detection methodology* that they implement.

The types of intrusion detection systems when classified by *monitored environment* include:

- Host-based IDSs reside on a single system and monitor that system's event log and audit trail for signs of unusual activity. They do not monitor network activity "on the wire" but are useful for detecting attacks that might impact only a single host without generating network traffic.
- Network-based IDSs typically perform real-time monitoring in a passive manner by monitoring all of the traffic on a specific network segment.

Intrusion prevention systems (IPSs) are a subset of IDSs that actually intervene when they detect an attack.

The types of intrusion detection systems when classified by *detection methodology* include:

- Signature-based IDSs store characteristics of known attacks (known as "signatures") and then compare activity in the monitored environment to those signatures. When a match is detected, the IDS generates an alert. Signature-based IDSs are highly accurate when attempting to detect known attacks but are ineffective against new attack variants for which there are no previous signatures.
- Anomaly-based IDSs measure user, system, and/or network behavior over an extended period of time to develop baselines. They then measure future activity against those baselines and generate an alert when activity seems anomalous. Anomaly-based IDSs tend to have higher false positive rates than signature-based IDSs, especially when legitimate user behavior is erratic.
- However, they are equally effective against known and novel attack types.

It is important to note several things about intrusion detection systems:

- To be effective, the system must be able to operate at the speed of the monitored environment.
- IDSs cannot "see" inside of encrypted traffic unless privy to the encryption keys.
- On a switched network, IDSs must be connected to a SPAN port in order to see traffic directed to all hosts on a switch.
- IDSs require frequent tuning and maintenance to remain effective against attacks.

# Penetration Testing

## Penetration Testing Types

ISC$^2$ defines penetration testing as the employment of exploitive techniques to determine the level of risk associated with a vulnerability or collection of vulnerabilities. It is important for companies to utilize occasional testing of their systems in order to make sure that their systems continue to meet security requirements. There are a couple of main types of penetration testing:

- Zero Knowledge – The tester is not given any of the information about the target network other then the ability to discover it.
- Partial Knowledge – The tester is given only the information that allows them to get started with the testing.
- Full Knowledge – The tester is given all known information about the tested network.

## Penetration Testing Methodologies

- Reconnaissance/Discovery – This methodology identifies and documents specific information about the target.
- Enumeration – This methodology obtains additional information through more intrusive methods.
- Vulnerability Analysis – This methodology maps out the known vulnerabilities of a company's environment.
- Exploitation – This methodology involves active attempts to gain user and privileged access to the company's network.

# Additional Testing Types

Along with penetration testing there are a number of testing types which can be used by a company to ensure security. These additional testing types include:

- Application Testing – Works by evaluating the applications in use and ensures control.
- Denial-of-Service (DoS) Testing – Works by evaluating the risk of the company network to DoS attacks.
- War Dialing Testing – Works by evaluating the risk of the company's modem, remote-access and maintenance connections.
- Wireless Network Testing – Works by evaluating any potential security gaps or flaws in the wireless network and design.
- Social Engineering Testing – Works by reviewing the susceptibility of a company to social engineering attacks.
- Private Branch Exchange (PBX) and IP Telephony Testing – Works by evaluating the controls included with both company PBX and IP telephony networks.

# Cryptography

## Key Definitions

- Cryptology – The science that involves the use of codes and ciphers to obscure the meaning of a message. It consists of two subdisciplines: cryptography and cryptanalysis.
- Cryptography – The science of protecting data so that it may be stored and transmitted between parties while preserving confidentiality and integrity.
- Cryptanalysis – The science of breaking cryptographic algorithms to obtain the secret message without authorization.
- Cryptosystems – Sets of techniques that implement cryptography.
- Collision – This occurs when a hash function generates the same output for different inputs.
- Algorithm – The mathematical function used to encrypt and decrypt messages. Kirchoff's law specifies that cryptographic algorithms should be open to public scrutiny without fear of compromising the cryptosystem. This law is often expressed as "the secrecy should be in the key" or "avoid security through obscurity."
- Key – The binary sequence used to provide secrecy to the algorithm. Different algorithms use public/private keypairs or secret keys.
- Key Space – Total number of possible values of keys in a cryptographic algorithm.
- Plaintext – The original message in an unencrypted, readable form.
- Ciphertext – The encrypted version of the message, unreadable without use of the correct algorithm and key.
- Encryption – The practice of transforming plaintext into ciphertext with an algorithm and key.
- Decryption – The practice of transforming ciphertext into plaintext with an algorithm and key
- Codes – Symbols or words to represent other words or phrases. For example, "Mayday" is code for "I need help" whereas a red cross is a symbol for medical assistance. Codes are not necessarily secret and are often used for international recognition or brevity.
- Ciphers – Mathematical functions to transform bits or characters into other bits or characters. Ciphers are used to ensure confidentiality and/or integrity between trusted parties.
    - Block ciphers – Work on plaintext and ciphertext in chunks of a discrete size.
    - Stream ciphers – Work on plaintext and ciphertext in a bitwise or characterwise fashion.
- Transposition or Permutation – The process of reordering the plaintext to hide a message.
- Substitution – The process of exchanging one letter or byte for another to hide a message.
- Confusion – Is provided bymixing key values used during rounds of encryption.
- Diffusion – Is provided by missing up the location of the plaintext throughout the ciphertext.
- Nonces – Random numbers used to introduce unpredictability into a cryptosystem.
- Work Factor – The time and effort required to break a protective measure.

# Protecting Information

## Data Storage

It is important for data to be secured in its stored state. This includes a number of different technologies which must have their security managed. These technologies include hard drives, backup tapes, external drives, and off-site storage among others. This security is typically achieved through the use of high-strength encryption mechanisms. Some modern mechanisms include both encryption and compression in the same process.

## Data Transmission

Data must also be secured in its transmission state. This is accomplished through a number of different mechanisms including:

- Link encryption – When using link encryption the data is encrypted only across specific network links. This mechanism is typically deployed by various circuit vendors.
- End-to-End encryption – When using End-to-End encryption the data is encrypted from one end of a connection to the other. This mechanism is typically deployed by the customer.

# Cryptography Uses

- Availability – Cryptography can provide limited access to systems through the use of passwords or passphrases.
- Confidentiality – Cryptography can provide confidentiality through the altering or hiding of a message.
- Integrity – Cryptography can provide integrity checks that allow the ability to ensure the message being sent was not altered.

# Cryptography Methods

There are two main methods of encrypting data including:

- Stream-based ciphers
  - Bit-by-bit encryption
  - Faster
  - Typically mixes plaintext with a keystream that is generated by the cryptosystem usually using an exclusive-or (XOR) operation.
  - Typically uses substitution
- Block-based ciphers
  - Block-by-block encryption
  - Block size is typically a multiple of ASCII character size (i.e. 64, 128, 192, et cetera)
  - Slower
  - Typically considered stronger than stream-based cipher
  - Typically uses a mixture of substitution and transposition

# Encryption Systems

## Substitution Ciphers

Substitution ciphers simply replace one character with another. The simplest form of substitution cipher is the “Captain Crunch decoder ring,” on which each letter of the alphabet simply maps to another letter.

The **Caesar cipher** is a historical substitution cipher that is generated by shifting each character three places to the right. (“A” becomes “D,”“B” becomes “E,” et cetera.) The full Caesar cipher is shown as follows:

Plaintext
**ABCDEFGHIJKLMNOPQRSTUVWXYZ**

Ciphertext
**DEFGHIJKLMNOPQRSTUVWXYZABC**

Basic substitution ciphers provide practically no confidentiality as they are simple to defeat using **frequency analysis**. For example, the most commonly used letters in the English language are E, T, A, O and N. Therefore, if you look at the ciphertext and determine the five most commonly used letters, they most probably map to E, T, A, O and N. The rest of the cryptosystem may be deduced in a similar fashion.

**Polyalphabetic substitution ciphers** overcome this limitation by using multiple alphabets on a rotating basis but they are subject to more advanced cryptanalytic techniques.

## Transposition Ciphers

Transposition ciphers move the letters of a message around in a manner that obscures their meaning. For example, you could perform a **columnar transposition** by taking the message “I wish to ensure the confidentiality and integrity of this message” and writing it in six columns as follows:

| | | | | | |
|---|---|---|---|---|---|
| I | W | I | S | H | T |
| O | E | N | S | U | R |
| E | T | H | E | C | O |
| N | F | I | D | E | N |
| T | I | A | L | I | T |
| Y | A | N | D | I | N |
| T | E | G | R | I | T |
| Y | O | F | T | H | I |
| S | M | E | S | S | A |
| G | E | | | | |

To create the ciphertext, you simply read down the columns instead of across the rows to get:

**OENTYTYSGWETFIAEOMEINHIANGFESSEDLDRTSHUCEIIIHSTRONTNTIA**

Numerous variations exist that use different numbers of columns and different transformation techniques.

### Vernam Ciphers

Vernam ciphers are the only truly unbreakable ciphers. They make use of a "one-time pad" that uses a new key for each message, preventing most cryptanalytic techniques. The length of the key is equal to the length of the message.

The problem with Vernam ciphers is key distribution. You must be able to secretly exchange keys that are just as long as the message. Presumably, if you have the ability to secretly exchange the keys, you could simply use that same capability to exchange the secret message instead.

However, Vernam ciphers are useful when you have the ability to exchange the keys securely now but may not have that capability in the future. For example, a spy could physically obtain the one-time pads in bulk while at headquarters and then use them to exchange messages in the field.

### Running Key Ciphers

Running key ciphers use an extremely long key, usually drawn from a source such as a book. (They are also known as "book ciphers.") The two parties use the same key source and perform modular arithmetic on the message with the key to perform encryption and decryption.

### Steganography

Steganography is the use of image manipulation techniques to hide information in images. Steganography has gotten a bad name due to its prolific use among purveyors of child pornography.

### Watermarking

Watermarking is the process of adding identifiable information into a file or document. The watermark may or may not be visible when normally used.

## Secret Key Cryptography

In a secret key cryptosystem, the two parties communicate with each other using the same secret key to encrypt and decrypt messages.

- Secret key cryptosystems are extremely fast and are suitable for implementation in hardware.
- The major problem with secret key cryptography is the secure exchange of the secret key.

### Data Encryption Standard (DES)

DES was once the federal government's only approved symmetric cryptosystem for the exchange of classified information among government entities.

- DES was created in 1972 and uses a 56-bit key, which was considered extremely secure at the time.
- DES operates on 64-bit blocks of data.
- Four modes of encryption are available:
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
- CBC and CFB modes have the inherent problem that errors propagate. An error in the transmission of one block affects the ability to decrypt subsequent blocks.

DES is now considered too weak to provide confidentiality, because it is possible to perform a brute-force attack against its relatively short key.

An alternative to DES is Triple DES (3DES), which encrypts the same message three times using two or three different keys. This increases the effective length of the key to 168 bits. There are four 3DES modes:

- DES-EEE3 uses three different keys in encrypt mode.
- DES-EDE3 uses three different keys: two in encrypt mode and one in decrypt mode.
- DES-EEE2 uses two different keys to perform three encryption operations.
- DES-EDE2 uses two different keys to perform two encryption operations and one decryption operation.

The use of two different keys (EEE2 or EDE2) yields an effective key length of 112 bits while the use of three keys (EEE3 or EDE3) yields an effective key length of 168 bits.

### Advanced Encryption Standard

The **Rijndael block cipher** was selected in a competition to succeed DES as the Advanced Encryption Standard (AES). Its use is mandated by a Federal Information Processing Standard (FIPS-197).

- AES uses a variable length key of 128, 192, or 256 bits.
- Operates on 128-bit blocks of data.

### Other Symmetric Algorithms

Other commonly found symmetric encryption algorithms include:

- Blowfish (an AES finalist) allows the use of a variable length key, ranging from 32 to 448 bits.
- Twofish (another AES finalist) uses 256-bit keys to operate on 128-bit blocks.
- RC5 uses keys up to 2,048 bits in length to operate on 32-bit, 64-bit, or 128-bit blocks of data.
- International Data Encryption Algorithm (IDEA) uses a 128-bit key to operate on 64-bit blocks.

## Public Key Cryptography

In a public key (asymmetric) cryptosystem, each user has a pair of keys: one public and one private.

- The public key is freely shared with all users of the cryptosystem whereas the private key is maintained as a personal secret.
- A message encrypted with one key in the pair may only be decrypted with the other key from the same pair.
- When user X wants to send an encrypted message to user Y, he encrypts it with user Y's public key. It may then only be decrypted by user Y's private key. Therefore, user Y (the only one with knowledge of Y's private key) is the only user that can decrypt the message. User X cannot decrypt the message that he himself encrypted.

- Key exchange is not an issue in public key cryptography. The only thing a user needs to communicate with another user is knowledge of the other user's public key, something which may be freely exchanged.
- Public key cryptography is much slower than private key cryptography. Therefore, public key cryptosystems are commonly used to create an initial session between to users, who then exchange a symmetric session key that they use for the remainder of the session.
- Keys used in public key cryptography must be longer than keys used for private key cryptography to achieve the same level of security.

## RSA Algorithm

The RSA algorithm (developed by Rivest, Shamir, and Adelman) is one of the most common public key cryptosystems.

- It is based on the difficulty of factoring a number that is the product of two very large prime numbers.
- It provides confidentiality, integrity, and non-repudiation.

## Diffie-Hellman Key Exchange

Diffie-Hellman key exchange is based on the algorithm developed by Whitfield Diffie and Martin Hellman. It allows two users who do not know each other to securely exchange a secret key for symmetric communication.

The steps in a Diffie-Hellman exchange are:

1. User1 and User2 agree on two large positive integers, n and g, which meet a number of criteria.
2. User1 chooses another large positive integer, X1, which is smaller than n.
3. User2 chooses another large positive integer, X2, which is smaller than n.
4. User1 computes a public key: Y1 = gX1 mod n.
5. User2 computes a public key: Y2 = gX2 mod n.
6. User1 sends Y1 to User2.
7. User2 sends Y2 to User1.
8. User1 computes the secret key: k = Y2X1 mod n.
9. User2 computes the same secret key: k = Y1X2 mod n.
10. They communicate using the shared secret key k.

### Other Asymmetric Algorithms

- El Gamal – An extension of the Diffie-Hellman key exchange algorithm, which includes encryption and signature capability.
- Merkle-Hellman Knapsack – An older algorithm based upon the difficulty of solving the knapsack problem and is no longer considered secure.
- Elliptic Curve Cryptography (ECC) – Based on the geometric properties of an elliptic curve. It allows the use of much shorter keys to achieve strong security and is commonly used in wireless devices.

## Hashing

A hash is calculated using a number of different algorithms to ensure that a specific message has not been changed without detection. ISC$^2$ defines a hash function as accepting an input message of any length and generates a one-way fixed length output. The assurance required is done through comparing differing hash algorithm outputs. If a hash algorithm was run on a specific message before it was sent and then after it was sent and the hash changes, then the message has been changed in transit. A hash does not use a secret key.

### Hashing Algorithms

- Message Digest 5 (MD5) hashes a message of arbitrary length to a 128-bit digest.
    - MD2 and MD4, older variants of MD5, are no longer considered secure and should not be used.
- Secure Hash Algorithm (SHA) is an implementation of the Secure Hash Standard (SHS).
    - SHA-1 produces a 160-bit digest.
    - SHA-256 uses the same algorithm to produce a 256-bit digest.
    - SHA-512 uses the same algorithm to produce a 512-bit digest.

### Message Authentication Code (MAC)

A MAC is a small block of data that is generated using a secret key and then appended to a message. This differs from a hash because a secret key is used and is required for verification from both the sender and the receiver of the message. Like a hash the MAC is very small and is also almost impossible to reverse without the private key.

## Digital Signatures

Digital signatures use asymmetric algorithms to certify the integrity of a message while in transit and ensure non-repudiation.

The digital signature process is as follows (assume user1 wants to sign a message to user2):

- User1 uses a hash function to create a message digest.
- User1 encrypts the message digest with his private key. This encrypted digest is the digital signature.
- User1 sends the message and the digital signature to user2.
- User2 decrypts the digital signature using user1's public key.
- User2 computes the message digest by using the same hash function that user1 used on the message.
- User2 compares the message digest generated with the hash function to the message digest generated by decrypting the digital signature. If they match, the message is authentic. If they do not match, the message was either altered in transit or was not created by user1.

## Encryption Management

### Key Management

Key management is defined as the control over the issuance, revocation, recovery, distribution, and history of cryptographic keys. Secure key management is one of the most important things that a company can do in order to make sure their communications stay secure. If an encryption method is used but the key management is non-existent then the potential for key vulnerability is very high.

### Key Recovery

It is also important when implementing an encryption management system that a method of key recovery is also employed. Without a method of message retrieval the simple loss of a key could make important data become useless.

## Public Key Infrastucture

The Public Key Infrastructure (PKI) solves the problem of distributing authenticated public keys among users of an asymmetric cryptosystem. PKI is based on the use of **X.509v3 certificates**, and works as follows:

1. A user submits his public key to a certification authority (CA) along with proof of identity.
2. The CA issues an X.509 certificate that contains:
    - Serial number
    - Version number
    - Cryptosystem information
    - User's identity
    - Validity dates (starting and ending)
    - Signature of the certificate authority
3. The CA sends the certificate to the user who may then distribute it to anyone needing the user's public key.
4. Recipients of the certificate may verify it by confirming the digital signature contained within the certificate using the CA's public key.

As the CA is the one actually signing the user's key, the PKI model works only if all users of the system trust the CA's determination of a user's identity.

## Cryptographic Attacks

There are a number of attacks possible against cryptographic systems:

- Brute-force – Guess the key by exhaustively checking all possibilities. Brute-force attacks are more effective against shorter-length keys, because there are fewer possibilities.
- Vulnerability exploits – Look for weaknesses in the cryptographic algorithm itself or a particular software or hardware implementation of a cryptographic algorithm.
- Statistical – Use mathematical analysis of a message to break the cryptosystem. One example is the frequency analysis discussed as an attack against substitution ciphers.
- Known plaintext – Begin with the attacker having knowledge of a plaintext message and the corresponding ciphertext.
- Chosen plaintext – Occurs when the attacker is able to determine the ciphertext that corresponds to a plaintext message of his or her choosing.
- Chosen ciphertext – Occurs when the attacker is able to determine the plaintext message that corresponds to a ciphertext of his or her choosing.
- Birthday – Occurs when the attacker is able to find two plaintext messages that generate the same ciphertext.
- Meet-in-the-middle – Occurs when an attacker has the plaintext and ciphertext and is able to use both simultaneously to determine the secret key.
- Man-in-the-middle – Occurs when the attacker is able to trick both communicating parties into thinking they are communicating with each other when they are both really communicating with the attacker who relays messages between the two.
- Replay – Occurs when an attacker is able to obtain the ciphertext and later use it to impersonate the transmitter by simply using the same ciphertext, even though she may not even know the corresponding plaintext.

## E-mail Encryption

E-mail encryption is commonly used to provide confidentiality, integrity, and non-repudiation for messages. Encryption functionality is now built into most commercial e-mail software.

E-mail encryption standards include:

- Secure Multipurpose Internet Mail Extensions (S/MIME) uses X.509 certificates. It is the most common form of encrypted electronic mail.
- MIME Object Security Standard (MOSS) is a competitor to S/MIME that is not as commonly used.
- Privacy Enhanced Mail (PEM) uses 3DES, RSA, MD5, and X.509.
- Pretty Good Privacy (PGP) uses a web of trust to allow users to vouch for each other's keys.

## Transaction Security

A number of standards have been proposed for secure financial transactions over the Internet:

- Secure Sockets Layer (SSL) – A standard proposed by Netscape and commonly used today to secure communications over the Web and other Internet protocols. It supports RSA, IDEA, DES, 3DES, and MD5.
- Secure Electronic Transactions (SET) – A standard proposed by credit card issuers in 1997 but never became widely adopted. It used DES and RSA algorithms.
- Transport Layer Security (TLS) – A follow-on protocol to SSL used to secure application layer protocols including SMTP, IMAP, POP3, and HTTP. It uses public key cryptography to initiate a session and then exchange a symmetric key.

# Physical (Environmental) Security

## Threats

There are three main physical threat types:

- Natural and environmental threats
- Threats from utility systems
- Man-made and political threats

### Natural and Environmental

There are a number of different threats which come from the physical environment. All of these are just as harmful as any other threat. The following are some of the main threats to account for:

- Water and humidity
- Dust and material contamination
- Excessive temperature variations

### Threats from Utility Systems

The threats from utility systems must also be considered as they are relied on for many different functions. The following are some of the main threats:

- Power fluctuations
- Temperature variations

### Man-made and Political Threats

There are a number of different threats which can come from man-made and political sources. These types of threats can be generally spread into two main categories: malicious threats, and accidental threats.

**Malicious threats**
Malicious threats are those which are perpetrated in a way that is intended to inflict harm on either an individual or the company. It is important to consider that damage to the physical structure must be fixed before any internal systems can be fixed. This should always be kept in mind when planning for these types of threats. The following are some of the main malicious threats:

- Physical attack
- Sabotage
- Vandalism
- Arson
- Theft

**Accidental threats**
Accidental threats are those which happen without the intention of being malicious. These include the largest number of internal attacks. The following are some of the potential accidental threats:

- Food contamination
- Relaxed security policy enforcement
- Cut cables (power or data)

## Site Location

There are a number of different considerations which must go into choosing a secure site location. In-town locations can provide convenience but will typically be in a location with less physical control. These in-town locations are typically shared with other companies and thus raise different security questions. Physical security may not be in the control of the company and may need to be trusted to a third party. Out-of-town locations allow the company to build to a particular specification but have the potential to be less convenient.

Another thing that comes up with location selection is where it is physically located in relation to water sources (oceans, lakes, and rivers) which may raise the potential for flood risks. The crime rate of a location is also a consideration, as it directly affects how much security the location requires.

## Site Infrastructure

The layout of a site is very important to the security planning. Obviously, the routing of water, power, and data lines is very important. Other systems to keep track of include HVAC and ventilation which are both very important to both the individuals working and the physical equipment.

## Layered Defense Model

The best type of design defense is one that has several layers of security which allow the parts of the system that require the highest amount of security to be protected by the highest number of layers. This is also referred to as Defense-in-Depth and is defined as "a layered combination of complementary countermeasures." Typically, there will be an outermost perimeter which is usually physical, an inner perimeter, and specific internal security zones. The outermost perimeter can comprise a number of different materials including fencing and landscaping in rural locations and building or floor security in urban locations.

## Physical Procedural Control

It is important that a clear procedure exists for the various entry points into the site location. It is also important that control exists over individuals and items going in and out of a site. The following are areas and things which must be closely controlled:

- Guard Posts – These points are not only typically located at entry points but also potentially control the gate for traffic and individuals, parameter patrols, and vehicle inspections, among other duties.
- Visitors – It is important that the visitors that go in and out of a site be managed closely as they can be a large security risk. These visitors can also be a health risk as they have the ability to bring something harmful into the site.
- Deliveries – the delivery of items into a site must be clearly monitored as these can also be potential security risks. As deliveries can come in through various points at a site they must be monitored at multiple points.

## Fire Prevention, Detection and Suppression

One of the primary items that need to be addressed with infrastructure is fire. It is a risk not only to the individuals inside the building but also to the equipment in the building. There are also different requirements to putting out a fire for only individuals and putting out a fire for sensitive equipment. Many of the environments which house these types of equipment also contain false floors or ceilings and inside these areas are a number of different cables. It is important that these cables are rated to be safe for these areas. Many different types of cables produce poisonous gases when burned which are harmful to individuals.

### Fire and Smoke Detection

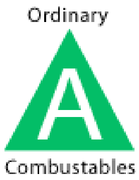
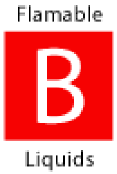
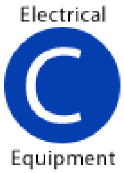
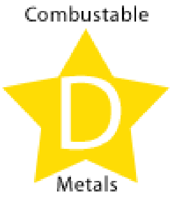
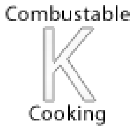
There are a number of different fire and smoke detection systems which are available. The following are the most commonly used:

- Ionization – Reacts to charged particles in the smoke.
- Photoelectric – Reacts to changes in or blockage of light caused by smoke.
- Heat – Reacts to significant changes in temperature.

## Fire Suppression

Along with fire detection mechanisms there must be fire suppression systems. These systems are created to put out specific types of fires. There are five classes of fire extinguishers, each of which is suitable for a different type of fire, as described in the following table:

### Fire Extinguisher Classes:

| Class | Description | Suppression Medium | Symbol |
|---|---|---|---|
| A | Ordinary combustibles | Water or soda acid |  |
| B | Flammable liquids | CO2, soda acid, Halon |  |
| C | Electrical | CO2 or Halon |  |
| D | Combustible metals | Copper, sodium chloride |  |
| K | Combustible cooking | Commercial kitchen extinguishers |  |

Fire extinguishers work well for small fires, but when you are trying to put out a large-scale fire then other larger systems are needed. Usually these systems use water to extinguish the fire which works well for saving individuals but wreaks havoc on electronic equipment. For these situations another solution is needed.

Water-based fire extinguishing systems come in four forms:

- Wet pipe systems are always full of water and discharge water immediately upon trigger.
- Dry pipe systems do not contain water and are useful in areas where bursting pipes are a risk. When the trigger occurs, they fill with water.
- Deluge systems literally soak an entire area when one of the sensors is triggered.
- Preaction systems are a combination of wet pipe and dry pipe systems.

Gas-based fire extinguishing systems:

- The most common gas-based extinguishers use carbon dioxide to remove oxygen from a fire.
- Data centers commonly used Halon systems in the past to prevent damage to sensitive electronic equipment. However, Halon systems are shown to damage the environment and jeopardize human life.
- The current "gas of choice" for fire suppression systems is FM-200.

## Key and Locking Systems

### Key and Deadbolt Locks

Key locks require a physical key which is used to open the lock. A deadbolt lock uses an additional bolt or bolts which can be inserted from the door into the door frame to provide added security.

Typically most locks are keyed in such a way that each door has an individual key which is the only one which unlocks the door. However, in a business environment this type of lock can be a problem as the number of keys to access every door would be cumbersome. In these situations a master key system is used, where both a master key and an individual key unlock the door.

### Combination Locks

Combination locks use a numbered tumbler mechanism which unlocks when a specific combination is entered.

### Key pad or Pushbutton Locks

These types of locks are simple and require a specific combination be entered on the key pad before unlocking.

### Smart Locks

Smart locks use a smart card mechanism to validate the credentials of the party trying to unlock the door. These types of locks can also be combined with a key pad lock to achieve better security.

## Closed Circuit Television (CCTV)

Closed circuit television (CCTV) is used to monitor a number of different cameras inside the control of the security staff. It has the ability of giving security officers a way to monitor many parts of a physical location without actually have to go to each individual location. CCTV does however require human intervention when attempting to capture images which are refined and specific to a potential threat. Without this the system will typically only capture a wide angle of a specific location. In order to design an effective CCTV system there are a couple of points to follow:

- Position cameras in a location which is hard to physically attack
- Distribute enough cameras to limit the number of blind camera angles
- Provide adequate lighting in all locations, for security and for good pictures
- Use appropriate lenses for the camera application
- Have the ability to pan, tilt, and zoom cameras
- Have the ability to record the camera feeds for as long as storage allows.
- Ensure regular servicing of all cameras.

## Intrusion Detection Systems

Intrusion protection systems provide the ability to protect specific areas inside the site. There are several different technologies which are used to provide this. The following is a list of the main technologies used:

- Electrical Circuit – This technology uses foil or wire contacts to carry a low level electrical current. When the current is interrupted then an alarm is triggered. This type of technology is typically deployed on windows and doors.
- Light Beams – This technology uses a photoelectric cell which receives a small light source across a boundary. If the path of the light is interrupted then an alarm is triggered. The problem with this technology is that dust or other small materials may be able to interrupt the light enough to trigger a false alarm.
- Passive Infrared Detector (PIR) – PIRs detect and measure light energy with a specific physical range; when the energy level of the light changes, then an alarm is triggered. This type of technology works well in detecting heat and movement but must be carefully calibrated to work correctly.
- Microwave and Ultrasonic Systems – These technologies measure either distance (microwave) or acoustic energy (ultrasound); when there is a change in these signals an alarm is triggered.

# Security Architecture and Design

## Systems Architecture

Systems architecture is basically defined into three main components:

- Central Processing Unit (CPU) – The brains of the system and performs the operations of all devices in the system
- Storage Devices – Provides both long and short storage of data
- Peripherals – Devices which provide both data input and output into the CPU.

### Storage Types

There are a couple of types of storage which are used on a system. These include:

- Primary Storage – Implemented as memory, cache or registers and stores data that has a high probability of being requested by the CPU.
- Secondary Storage – Typically implemented as a hard drive on most systems and stores data in a nonvolatile way. Secondary storage is also higher in capacity then primary storage.
- Virtual Memory – Uses secondary storage as a way of simulating primary storage on systems without sufficient primary storage.

## Diskless Workstations/Thin Clients/Thin Processing

There are a number of different systems which work by not having much or any storage capacity. These are split into a number of different types including diskless workstations and thin clients. When using a diskless workstation or thin client the computer relies on a central server which is used to perform booting and most processing duties. The local computer is limited to being a terminal when storage and applications are put off onto a central server.

## ISO/IEC 27002:2005

ISO/IEC 27002:2005 is a "code of practice for information security management" and defines the best practices to be followed in information security. It lays this out with 11 main sections including:

- security policy
- organization of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development, and maintenance
- information security incident management
- business continuity management
- compliance

## Operating Systems

Operating systems maintain stability by separating out the access of certain lower level and higher level software. These are referred to as levels or rings of privilege. Typically the operating system itself and its various hardware interfacing software are given the highest level of 0 and normal user applications are given the lowest level of 3. This type of system is used in order to maintain the integrity of the system itself from malicious software. The system kernel of an operating system is used mainly to control access to system resources and is considered the heart of all operating systems.

## Application Programs

Applications are programs which are used for a variety of purposes by individuals. These include everything from a common word processing program to high-level math and graphics programs.

## Trusted Computing Base (TCB)

The Trusted Computing Base is the combination of protection mechanisms within a system.

- The security perimeter is a boundary separating the TCB from the remainder of the system. The TCB must be tamperproof and unable to be compromised.
- Security Kernel consists of hardware, software, and firmware elements of the TCB that implement the reference monitor concept.
- The reference monitor is a system component that enforces access controls on an object. The reference monitor concept is an abstract machine that mediates all access of subject to objects.

## Security Models and Architecture

- In the **Lattice model** every resource and user is associated with one of an ordered set of classes. Resources of a particular class may only be accessed by those whose associated class is as high or higher than that of the resource.
- The **state machine model** allows the operating system to transition only between a series of well-defined states.
- **Research models** include the noninterference model and the information flow model.
- The **access matrix model** uses a combination of Read, Write, and Execute permissions assigned to various users. Each row in the matrix represents a user and each column represents a resource. The columns are also called access control lists (ACLs) and the rows are called access control entries (ACEs).
- The **take-grant** model uses directed graphs to illustrate the security permissions that one object can take from another object and those that an object can grant to another object.
- The **Bell-LaPadula model** (Orange Book) defines relationships between objects and subjects. Relationships are described in terms of a subject's assigned level of access or privilege (security clearance) and the object's level of sensitivity (security classification). This model enforces the lattice principle, which specifies that subjects are allowed write access to objects at the same or higher level as the subject, read access to objects at the same or lower level, and read/write access to only those objects at the same level as the subject.

- The Biba model is a lattice-based model that is similar to the Bell-LaPadua model. It has two rules:
    - Users can never write information to a higher security level (that is, a user with Secret access permissions can never write to a Top Secret file). This is the "no write up" rule or "Simple Integrity Axiom."
    - Information can never flow from a low level to a higher level (that is, a user with Top Secret access permissions cannot read information at a Secret level). This is the "no read down" rule or "Integrity Axiom."
- The **Clark-Wilson model** enforces separation of duties to maintain data integrity.
- The **Graham-Denning model** had three parts: a set of objects, a set of subjects, and a set of rights. The subjects are separated into a process and a domain. The domain controls the constraints on how subjects may access objects.

## Rainbow Series

In 1985, the National Computer Security Center published a series of books identified by the color of their covers. Major works in this series include:

- The Orange Book includes the DoD Trusted Computer System Evaluation Criteria (TCSEC).
- The Red Book is the Trusted Network Interpretation of the TCSEC.
- The Purple Book is the DoD Trusted Database Management System.
- The Green Book is the DoD Password Management Guideline.
- The Amber Book is the Guide to Understanding Configuration Management in Trusted Systems.

### Trusted Computer System Evaluation Criteria

The TCSEC has three purposes:

- Provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information.
- Provide guidance to manufacturers as to what to build into their new, widely available trusted commercial products to satisfy trust requirements for sensitive applications.
- Provide a basis for specifying security requirements in acquisition specifications.

The criteria for evaluating systems as specified in the TCSEC are:

- Security policy – The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
- Identification – The ability to uniquely identify each user of a trusted system.
- Labels – Elements assigned to each security object describing the sensitivity of that object.
- Documentation – Written evidence of a trusted system's compliance with TCSEC criteria.
- Accountability – The ability to audit user actions at an individually identifiable level.
- Lifecycle Assurance – The use of formal methods to validate the system design and implementation process.
- Continuous Protection – Elements of the trusted computing system must be continuously protected against tampering and/or unauthorized changes

The designations that may be awarded under TCSEC are defined in the Orange Book as:

- Minimal Protection (D) includes those systems that have been evaluated but fail to meet the requirements for a higher evaluation class.
- Discretionary Protection (C1) includes systems that nominally satisfy the criteria for discretionary access controls. Specific requirements for C1 certification include:
    - Discretionary Access Control Security Policy
    - Identification and Authentication
    - Operational Assurance of System Architecture and System Integrity
    - Lifecycle Assurance of Security Testing
    - Documentation including a Security Features Users' Guide, Trusted Facility Manual, Test Documentation, and Design Documentation
- Controlled Access Protection (C2) includes systems that have more finely grained discretionary access controls. C2 systems must meet all of the criteria for C1 systems and the following additional requirements:
    - Object Reuse Security Policy
    - Audit
- Labeled Security Protection (B1) systems introduce labeling requirements. B1 systems must meet all of the criteria for C2 systems and the following additional requirements:
    - Label Integrity Policy
    - Policy on Exportation of Labeled Information to Single-Level Devices, Multilevel Devices, and Human-Readable Output
    - Mandatory Access Control Policy
    - Lifecycle Assurance of Design Specification and Verification

- Structured Protection (B2) systems are cited in the Orange Book as relatively resistant to penetration. B2 systems must meet all of the requirements for B1 systems with the following additions:
  - Additions to Labeling Policy that Address Subject Sensitivity Labels and Device Labels
  - Trusted Path for Identification and Authentication
  - Additions to Operational Assurance of Covert Channel Analysis and Trusted Facility Management
  - Addition of Configuration Management to Lifecycle Assurance
- Security Domains (B3) systems are cited in the Orange Book as highly resistant to penetration. B3 systems must meet all of the requirements for B2 systems and must also implement:
  - Trusted Recovery Operational Assurance
  - Use of a Trusted Computing Base (TCB) small enough that it can be subjected to rigorous testing
- Verified Design (A1) systems do not add any additional architectural features or policy requirements. Rather, they must be developed using formal design specification and verification techniques that follow a five-step model:
  1. Develop a formal model of the security policy including a mathematical proof.
  2. Develop a formal top-level specification (FTLS) of the design including abstract definitions of TCB functions.
  3. Use a combination of formal and informal techniques to verify that the FTLS of the TCB is consistent with the model.
  4. Show that the implementation of the TCB is consistent with the FTLS through informal techniques.
  5. Perform a formal analysis designed to identify any covert channels in the system.

## Common Criteria

In the late twentieth century, several governments banded together to revise their information security models and develop the Common Criteria for Information Technology Security Evaluation (CC). They are described by ISO/IEC 15408. The Common Criteria model was designed to replace the following models:

- The U.S. Trusted Computer System Evaluation Criteria (TCSEC)
- The European Information Technology Security Evaluation Criteria (ITSEC)
- The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

The Common Criteria use a combination of **protection profiles** which specify security requirements for a product and **security targets**, which are the design claims made by vendors to provide a structured system for the evaluation of information technology products.

The security concepts defined by the Common Criteria are illustrated in Figure 1.

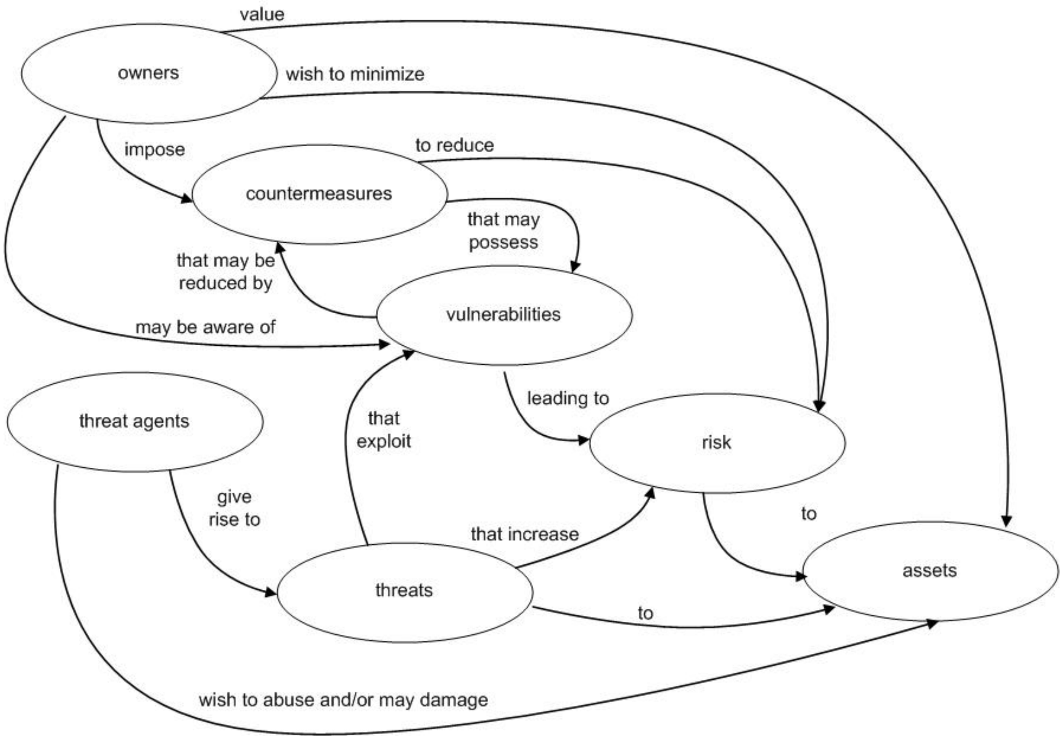


**Figure 1 -** Common Criteria Security Concepts

Products evaluated under the Common Criteria are assigned an Evaluation Assurance Level (EAL) from the following hierarchy:

- EAL1: Functionally Tested
- EAL2: Structurally Tested
- EAL3: Methodically Tested and Checked
- EAL4: Methodically Designed, Tested and Reviewed
- EAL5: Semiformally Designed and Tested
- EAL6: Semiformally Verified Design and Tested
- EAL7: Formally Verified Design and Tested

### Certification versus Accreditation

Certification and accreditation are distinct processes defined by security professionals.
The U.S. Department of Defense offers the following definitions to guide the process:

- Certification is a comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.
- Accreditation is a formal declaration by the Designated Accrediting Authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

## Business Continuity and Disaster Recovery Planning

The focus of Business Continuity Planning (BCP) is maintaining business function in the wake of a disaster. It is designed to help businesses "weather the storm" without disruption.

The focus of Disaster Recovery Planning (DRP) is restoring business function as quickly as possible when the business is disrupted.

As with other policies, BCP and DRP are only successful if they have the full support of senior management. Senior managers should be interested in these components of the business as they fall within the due care and due diligence requirements that managers have to business owners and shareholders. The Foreign Corrupt Practices Act of 1977 imposes civil and criminal penalties if publicly held companies fail to maintain adequate controls over their information systems.

Both the BCP and DRP should include all of the technical and nontechnical elements necessary to restore business functions. Some elements of these plans may include (but are not limited to):

- Networking
- Workstations
- Servers
- Data recovery
- Applications
- Facilities for computing infrastructure
- Facilities for workers
- Food and housing for workers

## Standards

- National Fire Protection Association (NFPA) 1600 – The benchmark that allows continuity planners a source of guidance in methodological development, risk identification, or planning guidelines.
- ISO 27002 – Is defined as "a comprehensive set of controls comprising best practices in information security."
- Defense Security Service (DSS) – Conducts personnel security investigations as well as offers security education and training to Department of Defense (DoD) other government entities.
- National Institute of Standards and Technology (NIST) – Provides requirements for federal contingency planning.

## Potential Loss Categories

- Revenue Loss – The permanent or temporary interruption of cash flow is a significant factor to be mitigated in a continuity planning program.
- Extra Expense – The extra expenses that are needed to deal with a disaster situation.
- Compromised Customer Service – Interruptions in either internal or external customer service drives short term recovery windows.
- Loss of Confidence – The financial impact that the loss of confidence in a company can have in disaster situations is hard to measure.

## BCP/DRP Project Management

### Project Initiation Phase

In this phase all of the project preplanning is completed which includes:

- Establishing the organization's continuity planning scope and objectives
- Displaying of support by management
- Forming the Continuity Planning Project Team (CPPT) and define roles
- Defining and obtaining continuity project resource requirements
- Understanding existing disaster avoidance preparations

**Disaster Recovery Plan (DRP)**
A traditional DRP addresses centralized and decentralized IT capabilities and voice and data communications network support.

**Business Continuity Plan (BCP)**
A traditional BCP addresses business issues involved with the loss of supporting technical resources.

**Crisis Management Plan (CMP)**
A CMP must provide the leadership which is required should an enterprise-wide disaster occur. This includes the formation of management teams which must train for these specific situations.

### Continuity Planning Project Team (CPPT)

The CPPT must be made up of a number of different individuals including both technical and business experts. These experts must have knowledge of the continuity plan process. Senior and knowledgeable staff will always be part of the team with other lower management involved to the point of training required.

## Current State Assessment Phase

- Understanding of enterprise strategies, goals and objectives
- Threat analysis completion
- Business Impact Assessment (BIA)
- Continuity Plan Process (CPP) assessment
- Benchmarking and peer review

### Threat Assessment

The objective of the threat assessment is to evaluate the existing organizational controls and procedures that may reduce the likelihood of potential interruption of services.

A general threat assessment includes three different types of assessment:

- Physical and personnel security – includes loss of key personnel, physical access weaknesses, supply chain failures, war or terrorism, and shortage of materials, among others.
- Environmental security – Fire detection and suppression, utility failure, gas leaks, HVAC controls, and telecommunications availability.
- Information security – Off-site data storage, logical access control weaknesses, continuity planning, change and problem management.

### Business Impact Assessment

A business impact assessments goal is to provide enterprise management a prioritized list of time-critical business processes and an estimate of time recovery objective for each.

## Design and Development Phase

- Develop suitable recovery strategies
- Develop continuity and crisis management plans
- Develop strategies for continuity and crisis management testing, maintenance and training
- Obtain recovery resources

### Work Plan Development

The work plan is a high-level project plan that will serve as an outline of implementation, testing, maintenance, and management steps.

**Recovery Strategies**

These can be development in a number of different ways including:

- IT and IT infrastructure strategy development
- Business processes strategy development
- Facilities strategy development

**Alternative recovery considerations**

- Hot sites are ready-to-run, dedicated sites that have equipment, software, and real-time data in place.
- Are the most expensive type of disaster recovery arrangement
- Generally used by organizations in extremely data-sensitive industries, such as financial services, public safety, and healthcare
- Warm sites provide all of the equipment and environmental controls necessary to restore operations but do not have applications installed or data restored.
    - Take longer to activate than hot sites but are typically much less expensive
    - May be shared by multiple organizations
  - Cold sites are buildings with proper infrastructure to support computing operations (i.e., power, environmental controls, etc.) but without any computer equipment, data, or software in place.
    - Are the cheapest alternative
    - Take a very long time to bring to an operational state
    - Useful only in those disasters that last for an extended period of time
  - Hot sites, warm sites, and cold sites may be either owned and operated by the organization that they serve, or by a subscription service that keeps the facilities available for its clients.
  - If operating in a shared subscription environment, you must make the distinction between services that maintain a facility dedicated to your organization and those that operate a pool of shared facilities that any organization in a disaster state may draw upon.
  - In a pooled environment, recognize that the facility may be quickly overrun in the event of a major disaster. For example, if you have a fire in your office building, the data center will probably be available. On the other hand, if an earthquake or hurricane destroys a major portion of your city, the data center may have more customers declare emergencies than it is capable of supporting simultaneously.
  - Many large organizations arrange for data centers in remote cities to avoid this concern.
  - Other alternatives include mobile data recovery sites and prefabricated relocatable buildings.

### Transaction Redundancy Implementation

A number of online solutions may be used to ensure the integrity of database transactions:

- Electronic vaulting – Transfer of backup data to an offsite location. Done by batch over telecom lines to alternate location.
- Remote journaling – Parallel processing of transactions to an alternate site. Telecom line transmits live data as it occurs.
- Database shadowing – Uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers.

## Implementation Phase

- Analyze and validate CPPT implementation plans
- Work with the specific organizational departments that will be impacted by implementation
- Monitor recovery resource acquisition
- Long-term and short-term testing of strategy

### Testing types

- Checklist – involves the continuity planners and recovery team members validating the plan checklists by physically walking though the checklists and verifying each of the items.
- Tabletop-Walk-Through – involves the continuity planners and members achieving two main objectives:
    - The through study of the plans by challenging every assertion, assumption, activity, task and action in the plan.
    - A walk-through of the plan for training and awareness purposes.
- Simulation – The organization simulates some level of disaster event.
- Parallel – The organization decides to retrieve yesterday's backup data and apply today's transactions against the data in a parallel way to compare results.
- Full Interruption – The organization decides to perform a full interruption test of all systems to tests the plan's effectiveness in an all-encompassing situation.

## Management Phase

- Focuses on day-to-day activities of CPPT members
- CPPT members continue ongoing work with business process owners

# Telecommunications and Network Security

## Network Models

### OSI Reference Model

| Layer Number | Layer Name | Description |
|---|---|---|
| 7 | Application | Security: Confidentiality, authentication, data integrity, non-repudiation<br>Technology: Gateways<br>Protocols: FTP, SNMP, SMTP, DNS, TFTP, NFS, S-HTTP |
| 6 | Presentation | Security: Confidentiality, authentication, encryption<br>Technology: Gateways |
| 5 | Session | Security: None<br>Technology: Gateways<br>Protocols: RPC, SQL |
| 4 | Transport | Security: Confidentiality, authentication, integrity<br>Technology: Gateways<br>Protocols: TCP, UDP, SSL, SSH-2 |
| 3 | Network | Security: Confidentiality, authentication, data integrity<br>Technology: Virtual circuits, routers<br>Protocols: IP, IPSec, ARP, RARP, ICMP |
| 2 | Data Link | Security: Confidentiality<br>Technology: Bridges, switches<br>Protocols: HDLC, PPTP, L2F, L2TP, Token Ring, Ethernet, PPP, and SLIP |
| 1 | Physical | Security: Confidentiality<br>Technology: ISDN, repeaters, hubs<br>Protocols: IEEE 802, IEEE 802.2, X.21, HSSI |

It is important to learn the types of security, technology and protocols that reside at each layer within the OSI model. A popular mnemonic for remembering the seven layers of this model is "**A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing."

## TCP/IP Model

Another common network model is the Department of Defense TCP/IP model, which has only four layers.

| Layer Number | Layer Name | Protocols |
|---|---|---|
| 4 | Application | -- |
| 3 | Host-to-Host | TCP and UDP |
| 2 | Internet | IP, ARP, RARP, and ICMP |
| 1 | Network Access (Link) | -- |

Data encapsulation is process in which information from one packet is wrapped around or attached to the data of another packet. Each layer encapsulates the layer immediately above it.

The two common transport protocols are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

| TCP | UDP |
|---|---|
| Acknowledged | Unacknowledged |
| Sequenced | Subsequence |
| Connection-oriented | Connectionless |
| Reliable | Unreliable |
| High overhead | Low overhead (faster) |

TCP uses a three-way handshake to establish communications between two hosts. The steps of this process are:

- Initiating host sends a packet with the SYN flag set
- Responding host sends a packet with the SYN and ACK flags set
- Initiating host sends a packet with the ACK flag set

TCP, UDP, and other Transport layer protocols rely upon the network protocol to provide data routing. The most common routing protocol, the Internet Protocol (IP) uses a hierarchical series of IP addresses to route traffic.

There are several important facts you should know about IP:

- IP does not guarantee receipt. It relies upon the transport protocol to provide this guarantee, if necessary.
- IP addresses uniquely identify a network destination.
- Ports uniquely identify a service on a destination system for a given protocol (e.g., TCP/UDP).
- An IP address combined with a port uniquely identifies one side of a network connection. This is known as a socket.
- A network connection may be uniquely identified by two sockets.

There are three methods of network communications in IPv4:

- Broadcast - Communications are from a single host directed to all hosts.
- Unicast - Communications are between two individual hosts.
- Multicast - Communications are from a single host to many separate hosts.

**TCP/UDP Port Numbers**
Servers use well-known ports (in the range of 0 to 1023) to offer services to Internet hosts. Clients use high-numbered ports (in the range of 1024 to 65536) to initiate connections.

Common protocols and their associated well-known ports include:

- File Transfer Protocol (FTP) (ports 20 and 21)
- Secure Shell (SSH) (port 22)
- Telnet (port 23)
- Simple Mail Transfer Protocol (SMTP) (port 25)
- Domain Name Service (DNS) (port 53)
- Trivial File Transfer Protocol (TFTP) (port 69)
- Hypertext Transfer Protocol (HTTP) (port 80)
- Post Office Protocol v3 (POP3) (port 110)
- Simple Network Management Protocol (SNMP) (ports 161 and 162)
- Secure Hypertext Transfer Protocol (HTTPS) (port 443)

## Network Security Role

### Network as a target

Many attacks are targeted directly at the network in order to affect the availability of the network. If the network is affected so are all of the services used by the network.

### Network as an attack enabler

There are two main ways a network can be used as an attack enabler:

- Network used as a channel of attack (i.e. the Internet)
- Compromised network used as source of attack

### Network as a bastion of defense

The network can be considered the most valuable of strategic resources for a company. Because of this it can also be used as a means of defense to internal systems by building the network as a fortification.

## Network Security Objectives

### Access Control

The control of who can access the resources of a network is one of the highest objectives when dealing with network security. This includes efforts both internal to the company and external to the company.

### Availability

In most company environments the network is the central resource which is used for most services. If the network goes down for whatever reason this not only affects the network but all these services that rely on it.

### Denial of Service (DoS) Mitigation

One of the easiest ways to affect the availability of a network is to perform a DoS attack; this is because it takes very little knowledge to perform. There are a number of different ways in order to mitigate a DoS attack of a network including having a redundant network or network path, load balancing, Quality of Service configuration, and simple IP/DNS configuration changes during the attack.

### Confidentiality

The network can also be tasked with the role of protecting data as it is transmitted between systems. Much of the data that crosses the network in a corporate environment needs to stay confidential. Different technologies exist which can be used to provide this ability on the network devices before data is transmitted.

## Network Topology

LANs may be laid out using one of several topologies. The physical topology may differ from the logical topology. Common topologies include:

- In a bus topology, all hosts are connected to a single conductor. That conductor is a SPOF. Ethernet uses a logical bus topology.
- In a ring topology, each host is connected to two adjacent hosts, forming a ring. In this topology, any single host is a SPOF. Token Ring uses a logical ring topology.
- In a star topology, all hosts are connected to a central hub (or other networking device). The networking device is a SPOF. Ethernet and Token Ring can both use a physical star topology.
- In a tree topology, several busses or stars are connected together retaining the SPOFs of those methodologies. Ethernet can use a physical tree topology.
- In a mesh topology, there are several links between hosts. No host serves as a SPOF.

## Network Cabling

Network cabling comes in a variety of mediums:

**Coaxial** cable uses an insulated copper conductor.

- It is available in 50-ohm and 75-ohm resistances.
- It is resistant to eavesdropping and electromagnetic interference.
- It normally uses BNC connectors.
- 10Base2 (Thinnet) coax can carry 10 Mbps up to 185 meters per network segment.
- 10Base5 (Thicknet) coax can carry 10 Mbps up to 500 meters per network segment.

**Twisted-pair** cabling uses pairs of conductors that are twisted around each other.

- Unshielded twisted-pair (UTP) cable is inexpensive but susceptible to electromagnetic interference (EMI).
- Shielded twisted-pair (STP) cable is less susceptible to EMI but more expensive.

There are seven categories of twisted pair cable:

- Cat 1 is not suitable for data communications.
- Cat 2 is not suitable for networks but may be used to connect terminals to mainframes.
- Cat 3 can carry 10 Mbps and is commonly used in 10BaseT Ethernets.
- Cat 4 can carry 16 Mbps and is commonly used in Token Ring networks.
- Cat 5 can carry 100 Mbps and is commonly used in 100BaseTX networks.
- Cat 6 can carry 155 Mbps.
- Cat 7 can carry 1 Gbps.

**Fiber-optic** cabling is the most expensive type of conductor.

- It uses light instead of electromagnetism so it is completely resistant to EMI.
- It may be used for distances up to 2km.
- It is difficult to install and manipulate.
- It is the most resistant to eavesdropping.

**Wireless networks** are becoming increasingly pervasive. They use radio frequencies to eliminate the need for conductors.

Issues with network cable include:

- Crosstalk occurs when conductors in close physical proximity interfere with each other.
- Attenuation occurs when a signal weakens when traveling across a long network segment.
- EMI occurs when external sources of electromagnetic energy interfere with communication.

Networks use a variety of access control techniques to determine who may "speak" on a network at any given time. Common techniques include:

- Circuit-Switched – Establish a dedicated connection between endpoints. Transmission is not initiated until the circuit is established.
- Packet-Switched – Data is divided into packets and is transmitted on a shared network.
- Carrier Sense Multiple Access (CSMA) – Is basically a free-for-all where systems check to see if a network is in use. If it's not, they simply start transmitting.
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) – Networks require each host to ask for permission before transmitting. AppleTalk networks use CSMA/CA.

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) – Networks use a variant on CSMA where hosts transmit when they believe the network is clear but continue monitoring for other hosts. If they detect another host transmitting at the same time (a "collision") they stop transmitting and wait a random period of time to begin again. Ethernet uses CSMA/CD.
- Ethernet – Utilizes CSMA/CD to process frames which are transmitted onto the network.
- Token Ring – Networks pass a logical token from host to host. A host may transmit only when it possesses the token.
- Polling – Networks use a master/slave hierarchy. The master system asks ("polls") each system on the network to see if it has traffic. When a system is polled, it may transmit any data in the queue.

## Network Devices

There are a number of common network devices found on LANs and WANs. These include:

- Repeaters amplify signals and operate at OSI Layer 1.
- Hubs are simply repeaters with multiple ports and operate at OSI Layer 1.
- Bridges connect similar networks and operate at OSI Layer 2.
- Switches block broadcasts and connect similar networks. They may be used to create virtual LANs (VLANs) to enhance security. Switches are also known as intelligent hubs. They operate at either OSI Layer 2 or OSI Layer 3.
- Routers also block broadcasts and connect similar networks. They operate at OSI Layer 3.
- Gateways connect dissimilar networks and operate at OSI Layer 7.

WANs may be implemented using a number of different technologies including:

- Dedicated lines include circuits such as T1, T3, E1, and E3 circuits, which are point-to-point links between networks.
- Nondedicated lines include DSL and ISDN circuits. They operate over the telephone network.
- X.25 networks use packet-switching with permanent virtual circuits (PVCs).
- Frame Relay networks also use PVCs but allow multiple PVCs on a single line.
- ATM networks use 53-byte cells and are able to allocate bandwidth on demand.

## Wireless Security Basics

There are a number of different security issues which come from the continued popularity of wireless technologies. There are two different types of authentication which are used by wireless networks. These include:

- Open System Authentication
- Shared-Key Authentication

### Service Set Identifier (SSID) Broadcasting

The SSID is the name of a specific wireless network and is one of the things used to connect to a wireless network. If the SSID is broadcast then everyone with a wireless receiver is able to view the available networks. One way of providing a little bit of extra security is to not broadcast the SSID; this makes it so it is not viewable. However, it is still possible to connect to a network without the SSID with supporting software.

### Wireless Standards

- IEEE 802.11a – Ratified in 1999, uses Orthogonal Frequency Division Multiplexing (OFDM) in the 5-Ghz band.
- IEEE 802.11b – Ratified in 1999, uses Direct Sequence Spread Spectrum (DSSS) in the 2.4-Ghz band.
- IEEE 802.11g – Ratified in 2003, uses Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM) in the 2.4-Ghz band.
- IEEE 802.11n – Ratified in 2009, uses Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM) in the 2.4-Ghz and 5-Ghz bands.

## Wireless Encryption

### Wireless Equivalent Privacy (WEP)

WEP uses a shared secret between the client and the access point. RC4 encryption is used to encrypt a packet with the shared secret and initialization vector. A CRC-32 checksum is used to increase packet integrity. Due to a flawed RC4 implementation and the reuse of the initialization vector, WEP is considered a weak encryption selection.

### WiFi Protected Access (WPA)

WPA uses shared secrets using the Temporal Key Integrity Protocol (TKIP) which changes the key for each packet. An improved implementation of RC4 is used for encryption and the initialization vector has been increased from 24 to 48 bits. The CRC-32 checksum was replaced by a message integrity check called Michael.

### WiFi Protected Access 2 (WPA2)

WPA2 works similarly to WPA but uses the Advanced Encryption Standard (AES) for encryption and TKIP and Michael were replaced by the Counter-Mode/CBC-Mac Protocol (CCMP) which deals with both the encryption keys and message integrity. WPA2 is an official encryption standard dubbed 802.11i. WPA2 also supports 802.1X authentication.

## WAN Technologies

- Public Switched Telephone Network (PSTN) – A circuit-switched public network which provides telephony connections, originally designed to provide analog voice connections.
- Integrated Services Digital Network (ISDN) – Provides a digital telephony connection, comes in two varieties: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI provides two 64-kbps digital voice or data channels and PRI provides 23 64-kbps digital voice or data channels.
- Point-to-Point Lines – Provides a point-to-point connection, connection type varies on the specific location and request.
- T1, T3, E1, and E3 – Provides a digital connection, can be configured for point-to-point, point-to-multipoint or multipoint-to-multipoint. T1 provides 24 64-kbps digital connections, T3 offers 28 T1 lines. E1 provides 32 64-kbps digital connections, E3 offers 16 E1 lines.
- Synchronous Optical Network (SONET) – Provides a variety of different high speed link options over an optical network. Lines include Optical Carrier 1 (51.84-Mbps) through OC-768 (39,813.12-Mbps) currently.

## Firewalls

Firewalls are network devices that sit between a protected network and an untrusted network and filter communications entering the protected network. There are four major types of firewalls:

- Packet filtering (screening router) – Examines source and destination address of IP packet. Can deny access to specific applications or services based on ACL. First generation firewall. Operates at network or transport layer
- Application-level firewall (proxy server, application-layer gateway) – Second generation. Reduces network performance. Circuit level firewall is a variation, creates virtual circuit between client and server
- Stateful inspection firewall – Third generation. Packets are captured by an inspection engine. Can be used to track connectionless protocols like UDP
- Dynamic packet filtering firewalls – Mostly used for UDP. Fourth generation
- Firewall architectures:
    - Packet-filtering routers – Use basic access control lists to determine what type of traffic is permitted onto the protected network. These systems work at the packet level only and do not maintain any session state intelligence.
    - Screened host systems – Use packet filtering router and a bastion host. Provide both Network layer packet filtering and Application layer proxy services.
    - Dual-homed host firewalls – Single computer with two NICs, one connected to trusted network and other connected to Internet (or untrusted network).
    - Screened subnet firewalls – Two packet-filtering routers and a bastion host. Provides demilitarized zone (DMZ).

## Virtual Private Networks (VPN)

Virtual private networks (VPNs) create secure communications links over inherently insecure networks, such as the Internet.

Common VPN protocols include:

- The Point-to-Point Tunneling Protocol (PPTP) is based upon the Point-to-Point Protocol (PPP) and allows the use of several authentication techniques, including:
    - Challenge Handshake Authentication Protocol (CHAP)
    - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
    - Password Authentication Protocol (PAP)
    - Extensible Authentication Protocol (EAP)
    - Shiva Password Authentication Protocol (SPAP)
    - Layer Two Forwarding (L2F) is a proprietary VPN protocol developed by Cisco that does not support encryption and is not commonly used.
    - Layer Two Tunneling Protocol (L2TP) combines elements of PPTP and L2F.
- It typically uses IPSec for security.
- IPSec is the most common VPN protocol in use today. It operates in two different modes:
    - In tunnel mode, the entire data packet is encrypted and encased in an IPSec packet.
    - In transport mode, only the datagram is encrypted, not the header.
- IPSec relies upon several underlying protocols:
    - The Internet Security Association and Key Management Protocol (ISAKMP) is used to negotiate and establish security associations (SAs) between hosts.
    - The Authentication Header (AH) protocol provides authentication and integrity assurances.
    - The Encapsulating Security Payload (ESP) protocol provides authentication, integrity, and confidentiality assurances.

## Common Attacks

Common attacks against networked communications include:

- Eavesdropping – Attacks occur when an intermediary is able to observe communications while in transit on a network.
- Masquerading – Attacks occur when one entity is able to successfully impersonate another entity.
- Replay – Attacks occur when one entity is able to eavesdrop on the authentication process used between two hosts and then reuse the captured packets to successfully authenticate with one of the hosts.
- Session hijacking – Attacks occur when one system is able to take over a connection being used by another system.
- Man-in-the-middle – Attacks occur when one host is able to successfully convince two other hosts that they are communicating with each other when, in reality, they are both really communicating with the attacker who is relaying the messages.

# Application Security

## Programming Languages

Programming languages are generally considered to belong to a specific generation of languages. The accepted generations are:

- First Generation Language (1GL) – Otherwise known as machine language, 1GLs use the native binary format recognized by the computer.
- Second Generation Language (2GL) – Otherwise known as assembly language, 2GLs consist of basic instructions that are specific to the hardware used but still may be interpreted by humans.
- Third Generation Language (3GL) – Otherwise known as high-level languages, 3GLs are compiled or interpreted from a human-friendly format to machine language. 3GLs include Java, C, Basic, FORTRAN and other common programming languages
- Fourth Generation Language (4GL) – 4GLs are designed to resemble natural language as much as possible. Structured Query Language (SQL) is a common example.
- Fifth Generation Language (5GL) – 5GLs use visual tools to create code in a 3GL or 4GL. Microsoft's Visual Studio is a good example.

Programs may be written in two types of high-level languages:

- Interpreted programs remain in the original programming language. The interpreter translates the program into machine language one line at a time when the program is executed. Interpreted programs are easy to modify and are more susceptible to malicious modification than compiled programs.
- Compiled programs - Are converted into machine language all at once by the programmer using a compiler. The machine language version is distributed to end users. Commercial software is generally compiled. Compiled software is harder to modify and, therefore, has a greater degree of security from malicious modification.

## Software Threats

### Buffer Overflow

A buffer overflow is one of the oldest software development threats. It happens when a program allows a memory buffer to be filled with more data than is expected. It is then possible to use this extra data in a way that can threaten the system.

### Citizen Programmers

A newer threat which exists is caused by the addition of scripting languages to many different operating systems and application packages. This allows a common uneducated user to potentially write an application or utility that can affect the security of a system.

### Malformed Input Attacks

It is possible that if the user inputs information into an application that is not expected, the application can then perform an action which is not expected. This type of action is most obvious with web and web browser attacks. Many sites take advantage of weaknesses in web browsers which can lead to gaining access to the user system.

### Memory Reuse

It is possible to take advantage of leftover data in memory from a previous application. It is recommended that the operating system zero out memory when it is released.

### Executable Mobile Code

Executable mobile code is software which is transmitted over a network from a remote source and executes on the local system.

### Trapdoor/Backdoor

A trapdoor or backdoor is a hidden method of accessing a system which bypasses the access control of a system.

## System Lifecycle

Phases of the system lifecycle include:

- Project initiation
- Functional design
- System design and specification
- Software development
- Installation
- Maintenance
- Revision

Common Software Development LifeCycle (SDLC) models include:

- Waterfall model allows for iteration back to the previous phase of development.
- Modified waterfall model incorporates verification and validation.
- Spiral model uses iterations of the entire process gradually refining the finished product.

All phases of the lifecycle should include testing for security vulnerabilities. Maintenance should take place in a controlled environment using a formal change control system. Configuration management should be used to ensure consistency in production environments.

The Software Engineering Institute's (SEI's) Capability Maturity Model (CMM) consists of five levels of ascending maturity:

- Level 1: Initiating
- Level 2: Repeatable
- Level 3: Defined
- Level 4: Managed
- Level 5: Optimized

The IDEAL model (based on CMM) also has five phases:

- Level 1: Initiating
- Level 2: Diagnosing
- Level 3: Establishing
- Level 4: Acting
- Level 5: Learning

## Object Oriented Programming

Object-oriented languages use individual objects that interact with each other to create programmed systems. Components of an object-oriented environment include:

- Attributes of objects are similar to variables. For example, a Person object might have the attributes Name, Eye Color, Hair Color, Height, and Weight.
- Methods are routines that manipulate objects. For example, a Person object might have the methods Eat, Move, and Sleep. Invoking the Eat method might modify the Person object's Weight attribute.
- A Class is a generalized description of a type of object. The Person class would follow our example. Objects can use class inheritance to make more specific cases out of the general case. For example, Man and Woman might be two classes that inherit from the Person class.
- An Instance is a particular instantiation of an object. For example, "George Washington" might be an instance of the Man class.

## Software Protection Mechanisms

### Security Kernels

The security kernel is responsible for enforcing the security policy of a system. This is implemented by the operating system and is fundamental to true system security.

### Processor Privilege States

Many processors are built with the capability to process different types of programs at different security or privilege levels. These protections can also be used to only allow each of these types of programs to access certain parts of memory depending on the privilege level.

### Security Controls for Buffer Overflows

The main protection which is used to prevent buffer overflows is parameter checking by the original programmer. This allows the overflows to never happen as only the expected amount of data is allowed. Hardware states can also prevent buffer overflows from happening if used.

### Memory Protection

Memory protection is used to prevent processes from interfering with the memory used by other processes.

### Password Protection Techniques

Many different operating systems and applications use passwords as a form of security. The specific rights are associated with each username and password which is entered.

## Malware Protection

There are a number of different attacks which can be considered malware and thus must be covered with some type of malware protection. There are a couple of different tools which can be used to both detect and mitigate the affects of malware on a system.

### Scanners

A scanner is rather simple in its implementation; it simply uses a database of signatures to compare against a given data stream, whether this be a file, a group of files, or a stream of currently running programs.

Another technology which is used by modern scanners is heuristic scanners. This type of scanner uses intelligent analysis to try to determine a program's intentions.

### Activity Monitors

Activity monitors work by looking for specific activities which are used by an infected virus. This can include calls to format a disk, write to or delete a file, or register something to the registry among other things. This type of tool is very user intensive at first as they ask lots of question to verify what programs are allowed to do what. They are also highly misused as users get irritated by the constant questions and just keep answering yes to the prompted questions.

### Change Detection

Change detection programs work by cataloging the system and program files on a computer and storing a checksum of the file which can be used to determine the change in a file. If a change does occur it is detected because the checksum of the changed file will not match that of the original.

### Anti-Malware Policies

Simple policies can also be used to deter the spread of malware. This includes a high amount of user education which will teach them what to do and not to do. There are a number of different policies which can be used, including avoiding the use of unauthorized software, not going to unauthorized sites, not bringing in outside data, and not connecting to unauthorized external devices, among others.

## Relational Database Management System (RDBMS)

Modern databases follow the relational database management system (RDBMS) model. This model is based on the concept of tables of data with rows representing individual records and columns representing attributes.

- Rows, records, and tables are synonymous in RDBMSs.
- A table's cardinality is equal to the number of rows in the table.
- Attributes and columns are synonymous in RDBMSs.
- A table's degree is equal to the number of columns in the table.
- Most relational databases use SQL for user interaction with the database and its data.

RDBMS systems rely upon keys to maintain record consistency.

- A candidate key is any combination of attributes that uniquely identifies the rows in a table. A given table may have many candidate keys.
- Each table has one primary key that is the candidate key selected by the database administrator to uniquely identify the rows of the table. The uniqueness of the primary key is enforced by the database system's management engine.
- Foreign keys are used to reference other tables in the same database.

# Operations Security

## Entities

### Operators

A system operator is a user who is typically located in a data center environment. These operators typically have elevated privileges but less than system administrators. These elevated privileges can be used to circumvent existing security policy.

### Ordinary Users

Ordinary users only have privilege enough to run the programs that they require. Typically, users operate on a least privileged model where permissions are strictly given on an as-needed basis.

### System Administrators

Administrators are given trusted permissions on a system for operations and maintenance tasks. It is the administrator’s responsibility to make sure the system is working as expected for the users and operators.

### Security Administrators

The security administrator is responsible for the oversight of system security. This includes account management, system security settings, file sensitivity labels, and the audit of system data.

### System Accounts

Many systems have a number of different accounts which are used to provide dedicated access for a variety of system services. These system accounts should only be given the minimum required access to operate on a system.

## Hardware

Like logical account management, physical security measures must also be provided on a least privileged basis. The following is a short list of hardware and the way they should be handled:

- Servers – Should be restricted to locations which are segregated, commonly a server room or data center.
- Operator Consoles or Workstations – Should be restricted as much as possible; user workstations which are used for sensitive functions should be located in a room which is limited physically to other users.
- Printing Devices – Users should be limited to printing on devices which are close in proximity to them. They should also be informed by policy to obtain printed materials as soon as they are printed in order to limit exposure to sensitive data.
- Firewalls – Firewalls act to prevent unauthorized traffic from entering areas of the network which are restricted.
- Virtual Private Network (VPN) Devices – These devices are used to encrypt and decrypt data which must traverse public networks. These devices protect the integrity and confidentiality of this traffic.
- Routers and Switches – These devices are used to transport data traffic between the various network devices.

## Operational Threats

- Disclosure – The threat of unauthorized information being released to outside parties.
- Destruction – The malicious unintentional and uncontrollable irreparable damage to the data and systems.
- Interruption – The failure of equipment and services can make a number of system components unavailable. Denial-of-Service attacks and malicious attacks (e.g. viruses) can also cause vital components to become unavailable.
- Corruption – The corruption of data can be due to a number of factors including environmental and service changes (i.e. temperature changes or electricity changes).
- Theft – The loss of data or equipment by insiders or burglary
- Espionage – The loss of control over data which is proprietary to a specific company can be a large threat.
- Hackers and Crackers – The threat of having a company's systems being penetrated for any reason can be a large threat.
- Malicious Code – This threat includes any type of code which has the potential to steal information from a system or to cause damage to that system.

## Control Categories

Controls are normally divided into three categories:

- Preventive controls aim to stop an attack from succeeding. Examples of preventive controls include border routers, firewalls, and ACLs.
- Detective controls aim to identify malicious activity on the network. Examples of detective controls include audit trails, intrusion detection systems, and honeypots.
- Corrective controls aim to restore a resource to its pre-attack state. Examples of corrective controls include intrusion prevention systems and data backup and recovery mechanisms.

Other common control types include:

- Deterrent controls
- Application controls
- Input controls
- Processing controls
- Output controls
- Change controls
- Test controls

## Data Backups

Data backup is a critical part of any disaster recovery/business continuity plan. Security professionals must ensure that proper backup procedures are in place and effectively carried out.

### Backup Types

There are three primary types of backups:

- Full backups – Create a duplicate copy of all files on the primary media and store them on the backup media.
- Differential backups – Create a duplicate copy of all files that have been modified since the last full backup.
- Incremental backups – Create a duplicate copy of all files that have been modified since the last full or incremental backup (whichever was more recent).

The major differences between differential and incremental backups are their treatment of the archive bit:

- Incremental backups clear the archive bit.
- Differential backups do not clear the archive bit.

The media used for restoring data after a loss depends upon the last type of backup that was performed:

- If the last backup was a full backup, only the full backup must be restored from tape.
- If the last backup was a differential backup, you must restore the last full backup and the most recent incremental backup.
- If the last backup was an incremental backup, you must restore the last full backup and all intervening incremental backups.

There are tradeoffs in time to backup and time to restore:

- Using incremental backups in combination with periodic full backups requires less time to create the backups but requires more time to restore in the event of a disaster.
- Using differential backups in combination with periodic full backups requires more time to create the backups but requires less time to restore in the event of a disaster.

## Auditing

The goal of any audit is to ensure compliance with the security policy. Some audits are against organizational policies whereas others are for compliance with specific legal, regulatory, or accounting standards.

The audit function should always be independent of undue influence.

- In the case of an internal audit, the director of that function should report to a high-ranking official (preferably the CEO or equivalent) who has no direct responsibility for functions being audited.
- In the case of external audit, the firm chosen should have no relationship with the auditee outside of the audit function.

Audit trails should be configured on critical or sensitive systems that record, at a minimum:

- Date and time of each event
- Identity of the user who caused the event
- Details of the event-related activity
- Source of the event (IP, physical location, etc.)

The following are types of evidence that should be reviewed in connection with an audit:

- Physical examination
- Confirmation (response from third party)
- Documentation
- Observation
- Inquiry
- Mechanical accuracy
- Analytical procedures (using comparisons and ratios)

## Data Protection

Redundant Arrays of Inexpensive Disks (RAID) are often used to avoid SPOFs in servers resulting from hardware failures. There are many different levels of RAID that provide different levels of protection. The levels of RAID protection are:

- RAID 0 – Disk striping consists of using several disks to store different pieces of data. It increases performance but offers no added security.
- RAID 1 – Disk mirroring consists of maintaining two disks that are mirror images of each other. This is highly effective in terms of redundancy but also quite slow and wasteful in terms of disk space.
- RAID 5 – Interleave parity uses a minimum of three physical disks and stripes data blocks and a parity block across the disks. It is configured such that the failure of any one disk will not result in the loss of data. The administrator simply needs to replace the disk and regenerate the RAID array.
- RAID 10 – Uses two striped disk sets that are mirror images of each other.

RAID arrays use three different types of drives. The difference is significant in the event of a failure. The drive types include:

- Hot-swappable – Drives may be replaced while the server is running without any downtime.
- Cold-swappable – Drives require a server shutdown for replacement and cause downtime.
- Warm-swappable – Drives require software disablement of the RAID array and render it unavailable but do not require a complete server shutdown for replacement.

## Problem Management

There are a number of different problem action items which should be addressed; these items should be detailed in a way which is executable by most people with minimal assistance. These include:

### System Component Failure

A problem management plan should detail a process of implementing redundant components and the activation of backup items.

### Power Failure

The failure of primary power is an issue that can affect everyone in a company. It is the responsibility of the person in charge to stay aware of the time that a backup source is used on primary failure. It should also be the job of this person to limit the amount of power which is used while on these backup supplies.

### Telecommunications Failure

The failure of the primary telecommunications line is always a possibility. An alternative should be supplied which enables locations with constant requirements to still have some network access. These backups are typically slower in speed than the primary source, and should be used in accordance to this lower bandwidth availability.

### Physical Break-in

As part of a problem management plan, personnel should be trained to inform local security personnel as well as the local authorities upon awareness of a physical break-in.

### Tampering

The tampering of systems is typically an internal attack and requires the notification of internal security. Care should be taken not to interact with the tampered system or data as this may make it harder for security personnel to locate the offending party.

# Legal, Regulations, Compliance and Investigations

## Information Security Laws

In recent years, a large number of laws affecting the information security profession have been enacted:

- The Electronic Communications Privacy Act of 1986 restricts eavesdropping on electronic communications.
- The Privacy Act of 1974 places restrictions on the types of information that federal agencies may collect from individuals and the ways they may use that information.
- The Health Insurance Portability and Accountability Act (HIPAA) consists of two components:
    - The Security Rule requires covered entities to use reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information.
    - The Privacy Rule requires covered entities to use reasonable and appropriate safeguards to ensure the privacy of protected health information (in either electronic or non-electronic form).
    - Many organizations outside of the healthcare profession may be subject to HIPAA if they work with healthcare information or have a self-insured employee benefits program.
- The Sarbanes-Oxley (SOX) Act requires that publicly traded organizations have security procedures in place to ensure that critical business records are protected and maintained for specified periods of time. It places personal accountability for compliance and accurate reporting in the hands of corporate officers.
- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to take reasonable and appropriate measures to protect personal financial information.
    - Covered organizations must have a written security plan.
    - The Federal Trade Commission's definition of "financial institution" is quite liberal and includes a large number of organizations that may not fall under the traditional definition of the term.

- The Computer Fraud and Abuse Act of 1986 (as amended in 1996) covers crimes against "federal interest" computing systems. It defines the following actions as felonies:
    - Unauthorized use of or access to classified information
    - Committing fraud that involves a computing system
    - Conducting activities intended to damage computing systems
- The National Information Infrastructure Protection Act requires government entities to implement measures to ensure the confidentiality, integrity, and availability of government data.
- The Family Education Rights and Privacy Act (FERPA) grants students and their families specific rights with regard to the dissemination of student data and requires educational institutions to implement safeguards to ensure privacy is maintained.

## Federal Law

There are three ways federal laws may be enacted in the United States:

- Statutory law is enacted by Congress and embodied in the United States Code.
- Administrative law is enacted by agencies of the executive branch and embodied in the Code of Federal Regulations.
- Case law is recognized by the judicial branch and documented in the legal precedents of the courts.

The law is further divided into three categories of law:

- Criminal law provides for punishment by imprisonment and fines for crimes against society.
- Civil law provides for financial damages for crimes against an individual or organization.
- Administrative law provides sanctions for violations of administrative requirements promulgated by regulatory bodies.

Another category of law, common law, is based upon principles handed down through the generations and recognized by the courts, but not codified in a legislative fashion.

## Intellectual Property Laws

Intellectual property may be protected by one or more of the following legal mechanisms:

- Copyrights – Used to protect original works of authorship and last for 70 years after the death of the author.
- Patents – Used to protect novel inventions and generally last for 17 years from the time of invention.
- Trademarks – Used to protect words, symbols, or other markings that identify the source of a product or service
- Trade secrets – Confidential business secrets kept within a business and not released to outsiders. Trade secrets are only protected by law if the owner takes reasonable precautions to ensure that they do not fall into the public domain.

## Evidence

There are two types of evidence, depending upon the circumstances of its intended use:

- In connection with an audit:
  - Physical examination
  - Confirmation (response from third party)
  - Documentation
  - Observation
  - Inquiry
  - Mechanical accuracy
  - Analytical procedures (using comparisons and ratios)
- Relevant to legal proceedings:
  - Best evidence
  - Secondary
  - Direct
  - Circumstantial
  - Conclusive
  - Corroborative
  - Opinion
  - Hearsay

To be admissible in court, evidence must meet three standards:

- It must be relevant, meaning that it must provide information related to the commission of the crime.
- It must be reliable, meaning that it has not been tampered with from the time of collection.
  - Reliability is established through the use of a documented chain of custody.
- It must be legal, meaning that it must have been gathered within the parameters of the law and the subject's rights under the Constitution and other relevant laws.

# References

(ISC)$^2$, (2007). Official (ISC)$^2$ Guide to the CISSP CBK. Boca Raton, FL:Taylor & Francis.

# Practice Questions

## Chapter 1

1. _____________ is what allows you to perform requested actions or denies such actions based on access criteria. Select the best answer.

   ○ A. Authorization
   ○ B. Identification
   ○ C. Authentication
   ○ D. Auditing

2. ACLs on objects are the most common implementation of what form of access control? Select the best answer.

   ○ A. Role based
   ○ B. Mandatory
   ○ C. Nondiscretionary
   ○ D. Discretionary

3. What is a Type 3 authentication factor? Select the best answer.

   ○ A. Something you have
   ○ B. Something you are
   ○ C. Something you know
   ○ D. Something you do

4. What does a Type I biometric error indicate? Select the best answer.

   ○ A. The rate at which authorized users are not granted access
   ○ B. The rate at which authorized users are granted access
   ○ C. The rate at which unauthorized users are not granted access
   ○ D. The rate at which unauthorized users are granted access

## Chapter 2

1. An indication that the integrity of the database has been violated occurs when which of the following includes a null value? Select the best answer.

   ○ A. Primary key
   ○ B. Cell
   ○ C. Tuple
   ○ D. Relation

2. Semantic integrity rules ensure that all structural and semantic rules of the database are not violated. Which of the following is NOT something that these rules would examine? Select the best answer.

   ❍ A. Data type
   ❍ B. Logical value
   ❍ C. Uniqueness constraints
   ❍ D. Relevance

## Chapter 3

1. Which of the following is NOT a reason to test a disaster recovery plan? Select the best answer.

   ❍ A. Testing verifies the accuracy of the procedures
   ❍ B. Testing minimizes legal liability
   ❍ C. Testing trains personnel
   ❍ D. Testing verifies the processing capability of the alternate site

2. Which form of disaster recovery test is an on-paper only walk through of the plan in a group meeting? Select the best answer.

   ❍ A. Full interruption test
   ❍ B. Structured walk through test
   ❍ C. Simulation test
   ❍ D. Parallel test

3. Which of the following is the most often overlooked aspect of disaster recovery? Select the best answer.

   ❍ A. Maintaining employee compensation mechanisms
   ❍ B. Protecting human safety
   ❍ C. Restoring and maintaining critical business functions
   ❍ D. Alternate site selection

## Chapter 4

1. The Escrowed Encryption Standard (EES) is embodied in which of the following? Select the best answer.

   ❍ A. Clipper chip
   ❍ B. Data Encryption Standard (DES)
   ❍ C. A symmetric cryptographic system
   ❍ D. Digital Signature Standard (DSS)

2. Which of the following is NOT true in regards to a one-time pad?
Select the best answer.

○ A. Extremely suitable for modern applications
○ B. Often used as a stream cipher
○ C. True random codes makes one-time pads unbreakable
○ D. The key length is the same as the length of the original message

## Chapter 5

1. When should the final report from an auditor be issued? Select the best answer.

○ A. After interim reports
○ B. During the exit conference
○ C. At the beginning of the auditing process
○ D. After the exit conference

2. The purpose of risk management is? Select the best answer.

○ A. Safeguard evaluation
○ B. Risk mitigation
○ C. Loss estimation
○ D. Remove all risk

3. Which of the following is NOT an accepted response to the results of risk analysis?
Select the best answer.

○ A. Reduce
○ B. Reject
○ C. Assign
○ D. Accept

## Chapter 6

1. Which of the following is NOT a valid means to identify or label computer evidence?
Select the best answer.

○ A. Writing on printouts with permanent markers
○ B. Recording serial numbers
○ C. Writing a contents and ID tag file to a hard drive
○ D. Photographing the contents displayed on the monitor

2. Aspects of the relevance of evidence include all but which of the following?
Select the best answer.

○ A. It has not been altered
○ B. It must show that a crime has been committed
○ C. It shows some aspect of the perpetrator's motives
○ D. It verifies or demonstrates what has occurred

## Chapter 7

1. Emergency response should be planned out before an incident occurs. Which of the following is NOT an aspect of this type of planning? Select the best answer.

○ A. What constitutes a federal crime
○ B. What is considered an incident
○ C. To whom should incidents be reported
○ D. Who should handle the response to an incident

2. Clipping levels are useful for detecting all but which of the following? Select the best answer.

○ A. Repetitive mistakes
○ B. Individuals exceeding their authorized privileges
○ C. Serious intrusion attempts
○ D. Slow low-traffic attacks

## Chapter 8

1. The radiation generated by the difference in power of the hot and neutral wires of a circuit is known as? Select the best answer.

○ A. Transient noise
○ B. Traverse mode noise
○ C. Common mode noise
○ D. Brownout

2. What is the ideal operating humidity for a data center room? Select the best answer.

○ A. 20 - 40%
○ B. 40 - 60%
○ C. 60 - 80%
○ D. 80 - 100%

3. What type of flame or fire detector is considered the most expensive but also the fastest in detecting fires? Select the best answer.

○ A. Smoke actuated
○ B. Fixed temperature, heat actuated
○ C. Rate of rise heat actuated
○ D. Flame actuated

## Chapter 9

1. Which of the following is NOT an element of life cycle assurance as defined by the Orange Book? Select the best answer.

   ❍ A. Design specification and testing
   ❍ B. Configuration management
   ❍ C. Trusted distribution
   ❍ D. System architecture

2. For security to be effective, which of the following must NOT be true? Select the best answer.

   ❍ A. Security is added to a product after its initial development
   ❍ B. Security is integrated into a product at the design stage
   ❍ C. Security is engineered into the product
   ❍ D. Security is implemented by default in the product

3. The Information Technology Security Evaluation Criteria (ITSEC) evaluates what two attributes separately that Trusted Computer System Evaluation Criteria (TCSEC) evaluates together? Select the best answer.

   ❍ A. Confidentialty and integrity
   ❍ B. Functionality and assurance
   ❍ C. Availability and authentication
   ❍ D. Accountability and non-repudiation

## Chapter 10

1. A dynamic packet filtering firewall is known as what generation of firewall? Select the best answer.

   ❍ A. Fifth
   ❍ B. Fourth
   ❍ C. Third
   ❍ D. Second

2. Starting counting from the Physical layer, the third layer of the OSI model is? Select the best answer.

   ❍ A. Session
   ❍ B. Transport
   ❍ C. Network
   ❍ D. Data Link

# Answers & Explanations

## Chapter 1

### 1. Answers: A

**Explanation A**. Authorization is what allows you to perform requested actions or denies such actions based on access criteria.

Explanation B. Identification is the "who" that a subject claims to be.

Explanation C. Authentication is the verification of the subject's identity with one or more authentication factors, such as a password.

Explanation D. Auditing enables the activities of subjects to be tracked in order to sustain accountability.

### 2. Answers: D

Explanation A. Role based or nondiscretionary access controls are based on job descriptions and work tasks. Role based access control uses labels on subjects rather than ACLs on objects.

Explanation B. Mandatory access control is based on data classification. Mandatory access control uses labels on subjects rather than ACLs on objects.

Explanation C. Role-based or nondiscretionary access controls are based on job descriptions and work tasks. Nondiscretionary access control uses labels on subjects rather than ACLs on objects.

**Explanation D**. ACLs on objects are the most common implementation of discretionary access control.

### 3. Answers: B

Explanation A. Something you have is a Type 2 authentication factor. An example of a something you have factor is a smart card.

**Explanation B**. Something you are is a Type 3 authentication factor. An example of a something you are factor is a fingerprint.

Explanation C. Something you know is a Type 1 authentication factor. An example of a something you know factor is a password.

Explanation D. Something you do is a Type 4 authentication factor. An example of a something you do factor is signing your name on a digital pad.

### 4. Answers: A

**Explanation A**. A False Rejection Rate (Type I) error of a biometric device indicates the rate at which authorized users are not granted access.

Explanation B. Granting authorized users access is not an error.

Explanation C. Preventing unauthorized users from gaining access is not an error.

Explanation D. A False Acceptance Rate (a Type II) error of a biometric device indicates the rate at which unauthorized users are granted access.

## Chapter 2

### 1. Answers: A

**Explanation A.** If the primary key contains a null value, then integrity has been violated.

Explanation B. A cell, as long as it is not within the primary key, can have a null value without violating integrity.

Explanation C. A tuple, as long as it is not the primary key, can have a null value without violating integrity.

Explanation D. A relation, as long as it is not within the primary key, can have a null value without violating integrity.

### 2. Answers: D

Explanation A. The semantic integrity rules would address or examine data type, logical value, and uniqueness constraints.

Explanation B. The semantic integrity rules would address or examine data type, logical value, and uniqueness constraints.

Explanation C. The semantic integrity rules would address or examine data type, logical value, and uniqueness constraints.

**Explanation D**. The semantic integrity rules would not address or examine the relevance of the data.

## Chapter 3

### 1. Answers: B

Explanation A. Testing verifies the accuracy of the procedures.

**Explanation B**. Testing alone does not minimize legal liability, rather the overall act of designing and implementing a plan minimizes legal liability.

Explanation C. Testing trains personnel.

Explanation D. Testing verifies the processing capability of the alternate site.

### 2. Answers: B

Explanation A. A full interruption test performs all activities of the plan up to the point of terminating processing at the primary site.

**Explanation B**. A structured walk through test is an on-paper only walk through of the plan in a group meeting.

Explanation C. A simulation test performs all activities of the plan up to but not including point of starting processing at the alternate site.

Explanation D. A parallel test performs all activities of the plan but processing at the primary facility continues.

### 3. Answers: A

**Explanation A**. The most often overlooked aspect of disaster recovery is maintaining a mechanism by which to continue issuing employee paychecks.

Explanation B. Human safety is well-known to be the most important factor and is rarely overlooked in disaster recovery planning.

Explanation C. Restoring and maintaining critical business functions is the key purpose Business Continuity and Disaster Recovery Planning 28 of disaster recovery planning and is rarely overlooked.

Explanation D. Selecting an alternate site is a key factor of restoring and maintaining critical business functions, thus it is rarely overlooked.

## Chapter 4

### 1. Answers: A

**Explanation A**. The Escrowed Encryption Standard (EES) is embodied in the clipper chip.

Explanation B. The Escrowed Encryption Standard (EES) is not embodied in Data Encryption Standard (DES). DES is a symmetric 56-bit key cryptographic system.

Explanation C. The Escrowed Encryption Standard (EES) is not a symmetric cryptographic system, it is an asymmetric cryptographic system.

Explanation D. The Escrowed Encryption Standard (EES) is not embodied in Digital Signature Standard (DSS). DSS is the formalized collection of hashing mechanisms.

### 2. Answers: A

**Explanation A**. One-time pads are not suitable for modern applications, primarily due to the inability for a computer to create truly non-repeating random codes and the problem of securely exchanging the pad with communication partners.

Explanation B. One-time pads are often used as a stream cipher.

Explanation C. One-time pads are unbreakable if the codes are truly random.

Explanation D. One-time pads use a key length that is the same length as the original message.

## Chapter 5

### 1. Answers: D

Explanation A. The final report should be issued after the exit conference. Interim reports are used to inform the client of issues that need immediate attention. Interim reports are not the trigger to initiate the final report.

Explanation B. The final report should be issued after the exit conference. The exit conference is held to discuss important items from the audit, but the final report is not given to the client at this time.

Explanation C. The final report should be issued after the exit conference. The final audit report can only be written after the auditng process, not at its beginning.

**Explanation D**. The final report should be issued after the exit conference.

### 2. Answers: B

Explanation A. Safeguard evaluation is the goal of risk analysis, which is part of risk management. However, safeguard evaluation is not the goal of risk management.

**Explanation B**. The purpose of risk management is risk mitigation. However, even in the most successful implementation, there is always some level of risk.

Explanation C. Loss estimation is the goal of risk analysis, which is part of risk management. However, loss estimation is not the goal of risk management.

Explanation D. It is not possible to remove all risk without the organization ceasing to exist.

### 3. Answers: B

Explanation A. Reducing risk is an accepted response to the results of risk analysis.

**Explanation B**. Rejecting risk is not an accepted response to the results of risk analysis.

Explanation C. Assigning risk is an accepted response to the results of risk analysis.

Explanation D. Accepting risk is an accepted response to the results of risk analysis.

## Chapter 6

### 1. Answers: C

Explanation A. Writing on printouts is a valid means to label evidence.

Explanation B. Recording serial numbers is a valid means to label evidence.

**Explanation C**. Writing a file to the hard drive may alter the evidence and therefore is an invalid means to label evidence.

Explanation D. Photographing a monitor is a valid means to collect/label data.

### 2. Answers: A

**Explanation A**. Whether evidence has been altered is not an aspect of relevance but an aspect of reliability.

Explanation B. An aspect of the relevance of evidence is that it must show that a crime has been committed.

Explanation C. An aspect of the relevance of evidence is that it must show some aspect of the perpetrator's motives.

Explanation D. An aspect of the relevance of evidence is that it must verify or demonstrate what has occurred.

## Chapter 7

### 1. Answers: A

**Explanation A**. Determining the criteria for a federal crime is the responsibility of the federal government, not your organization's emergency response planning team.

Explanation B. Deciding what is an incident is an aspect of emergency response planning.

Explanation C. Deciding to whom to report incidents is an aspect of emergency response planning.

Explanation D. Deciding who will respond to incidents is an aspect of emergency response planning.

### 2. Answers: D

Explanation A. Repetitive mistakes are easily detected through the use of clipping levels.

Explanation B. Individuals exceeding their authorized privileges are easily detected through the use of clipping levels.

Explanation C. Serious intrusion attempts are easily detected through the use of clipping levels.

**Explanation D**. Slow low-traffic attacks are typically not detected through the use of clipping levels. Slow low-traffic attacks are lost in the bulk of normal expected activity.

## Chapter 8

### 1. Answers: B

Explanation A. A transient noise is a short duration of an interfering disturbance in the power line.

**Explanation B**. Traverse mode noise is the radiation generated by the difference in power of the hot and neutral wires of a circuit.

Explanation C. Common mode noise is the radiation generated by the difference in power of the hot and ground wires of a circuit.

Explanation D. A brownout is an extended loss of voltage, not a form of interference.

### 2. Answers: B

Explanation A. Too little humidity can cause static electricity buildup.

**Explanation B**. The ideal operating humidity for a data center room is 40 - 60%.

Explanation C. Too much humidity can result in corrosion.

Explanation D. Extremely high levels of humidity can result in corrosion and pooling condensation.

### 3. Answers: D

Explanation A. Smoke actuated fire detectors are the most common; however, they are inexpensive and not the fastest detection method.

Explanation B. Fixed temperature, heat actuated detectors do not detect fires quickly, but only after the room's temperature reaches a pre-determined level. That level needs to be high enough not to be triggered falsely by the heating system or a failure of the A/C.

Explanation C. Rate of rise heat actuated cause many false alarms.

**Explanation D**. Flame actuated fire detectors are considered the most expensive but also the fastest in detecting fires.

## Chapter 9

### 1. Answers: D

Explanation A. Security testing, design specification and testing, configuration management, and trusted distribution are all elements of Life cycle assurance as defined by the Orange book.

Explanation B. Security testing, design specification and testing, configuration management, and trusted distribution are all elements of Life cycle assurance as defined by the Orange book.

Explanation C. Security testing, design specification and testing, configuration management, and trusted distribution are all elements of Life cycle assurance as defined by the Orange book.

**Explanation D**. System architecture, system integrity, covert channel analysis, trusted facility management, and trusted recovery are all elements of operational assurance as defined by the Orange book.

### 2. Answers: A

**Explanation A**. Adding security as an afterthought is not an effective means to provide adequate, functional, or even reliable security.

Explanation B. Security should be integrated into a product at the design stage.

Explanation C. Security should be engineered into the product.

Explanation D. Security should be implemented by default in the product.

### 3. Answers: B

Explanation A. ITSEC evaluates functionality and assurance separately while TCSEC evaluates them together.

**Explanation B**. ITSEC evaluates functionality and assurance separately while TCSEC evaluates them together.

Explanation C. ITSEC evaluates functionality and assurance separately while TCSEC evaluates them together.

Explanation D. ITSEC evaluates functionality and assurance separately while TCSEC evaluates them together.

## Chapter 10

### 1. Answers: B

Explanation A. A fifth generation firewall is a kernel proxy.

**Explanation B**. A fourth generation firewall is a dynamic packet filtering firewall.

Explanation C. A third generation firewall is a stateful inspection firewall.

Explanation D. A second generation firewall is an application level firewall.

### 2. Answers: C

Explanation A. The Session layer is the fifth layer of the OSI model.

Explanation B. The Transport layer is the fourth layer of the OSI model.

**Explanation C**. The Network layer is the third layer of the OSI model.

Explanation D. The Data Link layer is the second layer of the OSI model.