Appendix C

Answers to Review Questions

Chapter 1

1. The following terms are defined from a cybersecurity perspective:

   - **Availability—**The property of a system or a system resource being accessible, or usable, or operational upon demand by an authorized system entity, according to performance specifications for the system. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, and maintaining a correctly functioning operating system environment that is free of software conflicts.

   - **Integrity—**This means maintenance of consistency, accuracy, and trustworthiness of data over its entire life cycle. There should not be any change in data in transit, such as unauthorized people altering data (for example, in a breach of confidentiality). These measures include encryption, file permissions, and user access controls.

   - **Authenticity—**This is simply the property of being genuine and being able to be verified and trusted. It is a technological concept and can be solved by cryptography. Authenticity is about one party, Alice, interacting with another, Bob to convince Bob that some data really comes from Alice.

   - **Non-repudiation—**This is a legal assurance that the sender of information is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. For example, non-repudiation is about Alice showing to Bob a proof that some data really comes from Alice, such that not only is Bob convinced, but Bob also gets the assurance that he could show the same proof to Charlie, and Charlie would be convinced, too, even if Charlie does not trust Bob

   - **Confidentiality—**This, in lay terms, is privacy. It is a set of rules that limits access to information from reaching the wrong people, while making sure that the right people can in fact get it. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs, or soft tokens.

2. Three key challenges in developing an effective cybersecurity system are as follows:

   - **Scale and complexity of cyberspace—**Many telecom companies, such as Ericsson, are working to connect all devices and people to each other to make a fully connected society by next decade. It would cut across wired, wireless, and satellite networks and would consist of mobile devices, PDAs, laptops, wearables, cars, Internet of Things (IOT) devices, the cloud, and so on. The challenges to achieving cybersecurity will change with each technological advancement because new applications of information technology will emerge, which will trigger massive changes in societal norms.

   - **Nature of threat—**It will come from both internal sources and external sources. Common actors involved are vandals, criminals, terrorists, hostile states, and other malevolent actors. The desire to collect, analyze, and store individual information by both government agencies and corporations will create security and privacy risks.

   - **Trade-off between user needs and security implementation—**It is a heavily debated topic that involves huge trade-offs because users wants to use the most recent technology without caring for overall security, whereas an enterprise wants security and continuity at all costs. For example, employees prefer to connect their personal devices to the office network and share content, but this might introduce potent viruses and malware that could infect the whole system in a short time.

3. Big organizations employ a mix of many technologies, such as cryptography, network security protocols, operating system mechanisms, database security schemes, firewall, and antivirus protection.

4. The most significant activity of the ISF is the ongoing development of the Standard of Good Practice for Information Security (SGP). This document is a focused reference guide for enterprises to identify and manage information security risks in their operations and supply chains. This document is well researched, with input from its members, as well as an analysis of the leading standards on cybersecurity, information security, and risk management.

5. The three key activities for information security, according to the SGP, are as follows:

   - Planning for cybersecurity

   - Managing the cybersecurity

   - Assessment of security

6. An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. An ISMS is primarily implemented to

minimize all types of risk and ensure business continuity by proactively limiting the impact of a security breach. An ISMS typically addresses employee behavior and processes as well as data and technology. ISO 27001 is the default standard for establishing and maintaining ISMSs in enterprises.

7. Five core functions mentioned in the NIST framework are as follows:

   - **Identification—**This implies development of organizational understanding of management of cybersecurity risk to systems, assets, data, and capabilities.
   - **Protection—**This implies development and implementation of appropriate safeguards for ensuring delivery of critical infrastructure services.
   - **Detection—**This implies development and implementation of appropriate activities for identification of any occurrence of a cybersecurity event.
   - **Response—**This implies development and implementation of appropriate activities for taking action regarding a detected cybersecurity event.
   - **Recovery—**This implies development and the appropriation of activities needed for maintenance of plans for resilience and for restoration of capabilities or services impaired due to a cybersecurity event.

8. The weakest link in an information security chain is the people employed by or associated with the organization.

Chapter 2

1. Both terms have their own scope and definition. *Security governance* is the system by which an organization directs and controls its overall security, thereby meeting all strategic needs of the organization. *Security management* is concerned with making decisions to mitigate risks by using the information as input and then applying it in the risk management process.

   Governance determines decision-making authority. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Management recommends security strategies, whereas governance ensures that these security strategies are aligned with business objectives and consistent with regulations.

2. The three supplemental factors—internal incident and global vulnerability reports, standards and best practices, and user feedback—are all part of the success of any security management system. Internal security incident reports and global vulnerability reports from various sources illuminate possible security breaches/violations that help define the threat and the level of risk that the organization faces in protecting its information assets. The numerous standards and best practices documents provide guidance on managing risk. User feedback (both internal and external) helps improve the effectiveness of policies, procedures, and technical mechanisms.

3. Primary, or *internal*, stakeholders are parties (either individuals or groups) that actively run the management of the company. They can influence and can be influenced by the success or failure of the entity because they have a vested interest in the organization. Some examples of internal stakeholders of an organization are employees, owners, members of the board of directors, managers, and investors. Secondary, or *external*, stakeholders are interested parties who are not a part of the management but who indirectly affect the company's working and in turn are affected by the outcome. They are the outside parties that form part of the business operation chain. Some examples of external stakeholders of a company are customers, suppliers, creditors, third-party contractors, competitors, society, and government.

4. The two key pillars on which IT strategy planning should be based are mission necessity and enterprise maturity.

5. The three categories of metrics for evaluating an organization's security governance are as follows:

   - **Executive management support—**This is the most critical component for the success of any cybersecurity program. In order for the effect to perpetuate to lower layers, top executives must exhibit an understanding of security issues and take a proactive role in promoting security.

   - **Business and information security relationship—**There has to be a strong and symbiotic relationship between business goals and objectives and information security in any organization. When information security is incorporated into the enterprise planning process, employees feel empowered to secure their assets and view security not as an impediment but as an enabler of success.

   - **Information protection—**This is concerned with the pervasiveness and strength of information security mechanisms. These indicators reflect the degree of awareness of information security issues and the level of enterprisewide preparedness to deal with actual attacks.

6. COBIT 5 enumerates five distinct roles or structures for the security governance body:

   - **Chief information security officer (CISO)—**The CISO carries overall responsibility for the enterprise information security program. The CISO acts as a bridge between executive management and the information security program and effectively communicates and coordinates closely with key business stakeholders to address information protection needs.

   - **Information security steering (ISS) committee—**This committee ensures constant monitoring and review to ensure that good practices in information security are applied effectively and consistently throughout the enterprise. It acts as a watchdog.

   - **Information security manager (ISM)—**The ISM holds overall responsibility for the management of all aspects of information security.

- **Enterprise risk management (ERM) committee—**This is the main decision-making body of the enterprise to assess, control, optimize, finance, and monitor risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.
- **Information custodians/business owners—**They act as intermediaries between the business and information security functions.

7. The acronym RACI stands for *responsible, accountable, consulted, and informed*. It is used in the form of a matrix that explains the levels of responsibilities of all stakeholders in each of the key activities of the work:

   - **Responsible—**The person/group/team that performs the activity and is expected to deliver/submit the assigned work portion within the given deadline. For example, in an office transport system, the driver is responsible.
   - **Accountable—**The person /group/team that has decision-making authority and is expected to ensure the successful completion of the activity. For example, in an office transport system, the manager of the team of drivers is accountable.
   - **Consulted—**The person /group/team that should be included in the decision-making process for the activity because this person's/group's/team's responsibilities cover the outcome of this activity. For example, in an office transport system, the administrative head of the office should be consulted.
   - **Informed—**The person /group/team that needs to know of a decision or an action after it occurs in order to plan things based on the outcome. For example, in an office transport system, the manager of the employees who are using the office transport should be informed.

Chapter 3

1. Fair and accurate risk assessment enables an organization to determine an appropriate budget for security and implement appropriate security controls that optimize the level of protection while not overshooting the budget. Risk assessment enumerates potential security breaches, fair estimates of their cost, and the likelihood of their occurrence. Without risk assessment, an organization cannot formulate a cost-effective strategy to secure itself.
2. Residual risk is the remaining portion of a threat after all efforts to identify and eliminate risk have been made. In other words, residual risk is the output of risk treatment applied on a potential threat. For example, an athlete can transfer residual risk by insuring his body parts.
3. A threat is a capability of a threat source to intentionally or accidentally trigger vulnerability in the system. A vulnerability is a weakness or potential and intentional entry point in a system. Vulnerabilities can be in security procedures, design, implementation, or internal controls. A threat that cashes in on a potent vulnerability will produce a security violation, or breach.

4. The four contributing factors to determine risk in any organization are as follows:

   - **Asset—**Anything that can be a given a monetary value is an asset of an organization. Valuation of an asset is crucial to determine the impact of a risk and its subsequent treatment.
   - **Threat—**Any risk that has a potential to damage an asset is a threat. For any threat, past history is a good indicator of its frequency and possible impact.
   - **Vulnerability—**Any trapdoor or unintended weak point of a system is as vulnerability. A threat can ride on a potential vulnerability and damage a system if not stopped early.
   - **Control—**A control is an action to stop a potential threat from causing damage. A control is specific to the threat and thus needs to be chosen judiciously because this choice has major impacts on cost, functionality, and continuity of the system.

5. A qualitative risk assessment prioritizes the identified risks using a predefined rating scale (1 to 10, 1 to 7, and so on). Risks are scored based on their probability or likelihood of occurring (0 to 1) and the impact on project objectives should they occur. This is grossly subjective and is based on past history, heuristics, and expert judgment. A quantitative risk assessment is a purely mathematical approach to prioritizing risks by calculating/deriving a numerical or quantitative rating for each risk and then summing up and normalizing to arriving at overall risk.

6. Key ingredients of a sample risk analysis worksheet are as follows:

   - **Security issues—**This gives a brief statement of the security issue or area of concern as well as a description of compliance issues.
   - **Likelihood—**This is estimated (by internal experts or using past history or heuristics) likelihood for an occurrence of the linked threat/vulnerability pair.
   - **Impact—**This is the estimated impact (financial/temporal/spatial) for the linked threat/vulnerability pair.
   - **Risk level—**This is assessed according to the matrix shown in Figure 3.8 of Chapter 3.
   - **Recommended security controls—**These are specific security controls recommended by the team.
   - **Control priorities—**These are the relative priorities of the recommended controls.
   - **Comments—**This is a relevant note for the security risk management decision-making process linked with this security issue.

7. The six stages of information security risk management process are described as follows:

   - **Context establishment—**Here you set the basic criteria necessary for information security risk management, define the scope and boundaries, and establish an appropriate organization operating the information security risk management.

- **Risk assessment—**Here you identify the risk to analyze it thoroughly and then to evaluate the risk against establish metrics to categorize it for further action.
- **Risk treatment—**Here you mitigate risk by either stopping/removing the source of risk or change its probability of happening or change its possible impact or hedge the risk with a third party or transfer the risk by outsourcing or living with the risk.
- **Risk acceptance—**The risk post-treatment process should be explicitly communicated to managers/decision makers with the caveat that it cannot be reduced further and should be accepted.
- **Risk communication and consultation—**This is the continual and iterative processes an organization follows to provide, share, or obtain information about the risk and to keep updating or taking feedback from the key stakeholders regarding the management of risk.
- **Risk monitoring and review—**This stage involve continuous monitoring and review of all risk information obtained from the risk management activities.

8. The four risk-related standard documents that are published by Open Group are as follows:

   - The Open Group Standard: Risk Taxonomy (2013)
   - The Open Group Technical Guide : Requirements for Risk Assessment Methodologies (2009)
   - The Open Group Technical Guide: FAIR—ISO/IEC 27005 Cookbook (2010)
   - The Open Group Risk Analysis (O-RA) Technical Standard (2013)

9. FAIR defines the key terms as follows:

   - **Asset—**Any data, device, or other component of the environment that involves information and that can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss
   - **Risk—**The probable frequency and probable impact of future loss
   - **Threat—**Any entity capable of harming an asset and/or organization partially or permanently
   - **Vulnerability—**The probability of an asset's inability to resist actions of a threat agent

   FAIR definitions are much more specific than ISO 27005 definitions pertaining to risk analysis.

10. Regarding risk assessment, you consider the following types of assets:

    - **Hardware assets—**This includes physical servers, workstations, laptops, mobile devices, removable media, PDA devices, television sets, and networking and telecommunications equipment.

- **Software assets—**This includes applications, operating systems and other system software, virtual machine and container virtualization software, software for software-defined networks (SDNs) and network function virtualization (NFV), database management systems (DBMSs), decision support systems (DSS), and analytic engine (AEs).
- **Information assets—**This includes assets directly connected with information or its storage (for example, databases, file systems, cloud storage, routing information). This category of asset depends on the nature of work done by the organization.
- **Business assets—**This category includes all other organization assets (such as human capital, business processes, and factory location) that don't fit in preceding categories of assets. It also includes intangible assets, such as organization control, know-how, reputation, and image of the organization.

11. STRIDE is a threat classification system developed by Microsoft to categorize deliberately planned attacks. It includes identity spoofing, data tampering, repudiation, information disclosure to non-authorized entities, denial-of-service (DoS), privilege elevation, and so on. For example, imagine that a bright engineering team of company X is working on a new high-end mobile phone. The product is announced, and the CEO of X describes it capabilities and fixes its release date. All is going fine until a key member of the design team voluntarily discloses design specifications (for extra money and a better job than his current one) and implementation-level details to the company's key competitor, say Y. As a result, Y improves the specifications, adds more capability, and, following an Agile go-to-market strategy, it announces an earlier release date. This results in X's image being downgraded, its share price crashing, investors losing confidence, and a complete panic in the design team. This is a classic case of involuntary information disclosure.

12. Some common cybersecurity threat forms are malware, virus, worm, ransomware, spam, Trojan horse, trapdoor, exploits, spam programs, flooders, zombies/bots, spyware, adware, DNS attacks, DoS attacks, remote access attacks, phishing, sniffing, website exploit, and password attack.

13. The three key themes in the Threat Horizon report are as follows:

    - **Disruption—**This can be caused by overreliance on existing connectivity and planning processes of doing business.
    - **Distortion—**Once information integrity is lost, the monitoring of access and changes to sensitive information will become critical. This also leads to development of complex incident management procedures.
    - **Deterioration—**This occurs when controls are dictated by regulations and technology bringing a heightened focus on risk assessment and management in light of regulatory changes and the increased prevalence of artificial intelligence in everyday technology.

14. The FAIR risk analysis document groups controls into four categories:

    - **Avoidance controls—**This type of control affects the frequency and/or likelihood of threats encountered. These controls include firewall filters, physical barriers, and relocation of assets and reduction of threat populations.
    - **Deterrent controls—**This type of control affects the likelihood of a threat causing possible damage. These controls include policies, logging and monitoring, and enforcement practices.
    - **Vulnerability controls—**This type of control affects the probability that a threat's action will result in loss. These controls include authentication, access privileges, and patching.
    - **Responsive controls—**This type of control affects the amount of loss that results from a threat's action (that is, loss magnitude). These controls include backup and restore media and processes, forensics capabilities, and incident response processes.

15. ISO 27005 lists four options for treating risk:

    - **Risk reduction or mitigation—**This implies actions taken to lessen the probability and/or negative consequences associated with a risk.
    - **Risk retention—**This implies acceptance of the cost from a risk.
    - **Risk avoidance—**This implies a decision not to become involved in or an action to withdraw from a risk situation.
    - **Risk transfer or sharing—**This implies sharing the burden of loss from a risk with a third party, such as an insurance agency.

16. Three elements define the scope of risk assessment:

    - **Services—**This includes business services, such as sales and marketing, business processes, such as inventory management, and technical services, such as configuration management.
    - **Assets—**This includes human capital, information, physical devices, software, and physical plant assets.
    - **Factors influencing impact ratings—**This includes economic, social, technological, legal, and environmental factors.

Chapter 4

1. The security management function encompasses establishing, implementing, and monitoring and information security program, under the direction of a senior responsible person or specialized team. The organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements.

2. The two key individual roles in security management are as follows:

    - **Chief information security officer (CISO)—**This person holds overall responsibility for the enterprise information security program in the organization. The CISO links executive management with the information security program. The CISO should also communicate and coordinate closely with key business stakeholders to address information protection needs.

    - **Information security manager (ISM)—**This person holds overall responsibility for the management of information security efforts, including application information security, infrastructure information security, access management, threat and incident management, risk management, awareness program, metrics, and vendor assessments.

3. Key security program areas are as follows:

    - **Security planning—**Security planning primarily includes the alignment of information security management and operations with enterprise and IT strategic planning. It also includes more detailed planning for the organization, coordination, and implementation of security.

    - **Capital planning—**Capital planning is meant to facilitate and control the expenditure of the organization's funds. Its main aim is to prioritize potential IT security investments for allocating available funding to maximize profit.

    - **Awareness and training—**Awareness and training programs ensure that all employees of the organization understand their information security responsibilities to properly use and protect the information resources entrusted to them.

    - **Information security governance—**The CISO along with other C-level executives (CEO, CFO, CTO, and so on) and the board develop an effective security governance charter.

    - **System development life cycle—**This is about the development, implementation, and replacement of information systems.

    - **Security products and services acquisition management—**This is about supervision of the acquisition of security-related products and services, including considering the costs involved, the underlying security requirements, and the impact on the organizational mission, operations, strategic functions, personnel, and service provider arrangements.

    - **Risk management—**This is the prediction and evaluation (mostly financial) of risks together with the identification of procedures to avoid or minimize their impact on the organization.

    - **Configuration management—**This implies adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

- **Incident response—**Incident response occurs after the reporting of a security event. It aims to minimize the damage of the event and facilitate rapid recovery.
- **Contingency planning—**Information system contingency planning refers to management policies and procedures designed to maintain or restore business operations, including computer operations (possibly at an alternate location) in the event of emergencies, system failures, or disasters.
- **Performance measures—**Performance measures, a key feedback mechanism for an effective information security program, should be defined and used across the entire organization.

4. The Select/Control/Evaluate framework defines a cyclical process consisting of three steps for deciding which projects to pursue or which investments to make:

   - **Select phase—**Here the organization identifies and analyzes each project's risks and returns to determine financial feasibility before committing significant funds to any project. The organization then selects IT projects that will align best with its future plans. This process should be repeated each time funds are allocated to projects.
   - **Control phase—**Here the organization ensures that, as a project progresses, it continues to meet mission needs at the expected levels of cost and risk. If the project is not meeting expectations or if problems have arisen, steps must be quickly taken to address the deficiencies. If the mission needs have changed, the organization needs to adjust its objectives for the project and appropriately modify expected project outcomes.
   - **Evaluate phase—**Here a comparison is done between actual and expected results after project completion.

5. An information security policy is framed to ensure that all employees in an organization, especially those with responsibility of some sort for one or more assets, understand the security principles in use and their individual security-related responsibilities. Ambiguity in information security policies can defeat the purpose of the security program and may result in significant losses in all aspects. An information security policy is the central tool of an organization to provide management direction and support for information security across the organization. The security policy document defines the ideal expectations and proper behavior for employees, contractors, vendors, and all others who have roles in the organization.

   Some of the documents related to security are the information security plan, strategic plan, security plan, security policy, and acceptable use policy.

6. Some common security policies of an organization are as follows:

   - Access control policy
   - Contingency planning policy
   - Data classification policy

- Change control policy
- Wireless policy
- Incident response policy
- Termination of access policy
- Backup policy
- Virus policy
- Retention policy
- Physical access policy
- Security awareness policy
- Audit trail policy
- Firewall policy
- Network security policy
- Encryption policy

7. A prototypical structure of a security document should contain following items:
    - **Overview—**Background information about the issue the policy addresses.
    - **Purpose—**Why the policy is being created.
    - **Scope—**What areas the policy covers.
    - **Targeted audience—**To whom the policy is applicable.
    - **Policy—**A complete but concise description of the policy.
    - **Noncompliance—**Consequences for violating the policy
    - **Definitions—**Technical terms used in the document.
    - **Version—**The version number to control the changes made to the document.
8. The key aspects of a security policy document are as follows:
    1. **Responsibilities—**This aspect identifies:
        - Those responsible for ratifying policy document (for example, the board)
        - Responsibilities of all relevant individuals to comply with the policy
        - Individuals responsible for protecting specific assets
        - That all individuals must confirm the understanding of, acceptance of, and compliance with relevant policies and understand that disciplinary action will follow policy violation

2. **Principles—**This aspect specifies the following:
    - All relevant assets to be identified and classified by value/importance
    - All assets protected with respect to CIA (confidentiality, integrity, and availability) and other security requirements
    - All laws, regulations, and standards are complied with
3. **Actions—**This aspect specifies the following:
    - That all individuals are made aware of the security policy and their responsibilities
    - That all assets are subject to risk assessment periodically and before a major change
    - That all breaches are reported in a systematic fashion
    - That auditing occurs periodically and as needed
    - That policy documents are reviewed regularly and as needed
4. **Acceptable use—**This aspect specifically documents the following:
    - What behaviors are required, acceptable, and prohibited with respect various assets
    - Responsibility for establishing, approving, and monitoring acceptable use policies

9. Information security management performs the following functions:
    - **Consistent organizationwide use of security—**The CISO or other responsible authority should develop, maintain, and regularly review an overall security strategy for the organization and the accompanying policy document.
    - **Support function—**The CISO or other responsible authority should act as a security adviser and a security evangelist in the organization and oversee security aspects in all documents across the organization.
    - **Monitor function—**The CISO or other responsible authority should monitor trends and developments to be aware of how they may affect the organization's security strategy and implementation, including in the area of business trends, new technical developments, security solutions, standards, legislation, and regulation.
    - **Projects function—**The CISO or other responsible authority should be responsible for overseeing security-related projects.
    - **External requirements function—**The CISO or other responsible authority should manage the implications of laws, regulations, and contracts.

10. An acceptable use policy (AUP) is a type of security policy targeted at all employees who have access to one or more organization assets. It defines what behaviors are acceptable and what behaviors are not acceptable. The policy should be clear and concise, and it should be a condition of employment for each employee to sign a form indicating that he or she has read and understood the policy and agrees to abide by its conditions.

Chapter 5

1. The employment life cycle is a human resources model that identifies stages in employees' careers to help guide their management and optimize the company's performance. It is a relationship of the individual to the organization prior to employment, during employment, and post-employment (resignation/termination). One way to define the employment life cycle is to see it as having five stages:

    1. Recruitment
    2. Onboarding
    3. Career planning
    4. Career development
    5. Termination/resignation

2. You can categorize the security problems caused by employees into two divisions:

    - **Unintentional and originating from carelessness—**Some employees, unknowingly or out of sheer carelessness, aid in the commission of security incidents by failing to follow proper procedure, by forgetting security considerations, and by not understanding what results their actions can have. These people have no motive to cause harm. It may be either accidental, when there is no decision to act inappropriately, or it may be negligent, when there is a conscious decision to act inappropriately. In the latter case, someone may take a shortcut to increase productivity or simply to avoid hassle but feels he or she can do so without causing a security incident.

    - **Malicious intent and deliberate—**A minority chunk of employees knowingly violates all controls and procedures to causes or aids in an incident. The security problems caused by such persons can exceed those caused by outsiders, as employees with privileged access are the ones who know the controls and who know what information of value may be present. These incidents are hard to track.

3. General guidelines for checking applicants are as follows:

    - Ask for as much detail as possible about employment and educational history. The more detail that is available, the more difficult it is for the applicant to lie consistently. Check this data with online tools such as LinkedIn to verify authenticity.

    - Investigate the accuracy of the details (using a background or criminal check) to the extent reasonable by outsourcing it to some verification agency.

    - Arrange for experienced staff members to interview candidates face-to-face and try to gauge each candidate's expectations and fit with the proposed profile and company.

- Check the applicant's credit record for evidence of large personal debt and inability to pay it.
- Ask the applicant to obtain bonding for his or her position if the company expects to spend a significant amount in hiring/training this person or sending him or her abroad on a work visa to work on its behalf.

4. Any company can ensure personnel security by following these principles:
   - **Least privilege—**Give each person the minimum access necessary to do his or her job. This restricted access is both logical (access to accounts, networks, programs) and physical (access to computers, backup tapes, and other peripherals). If every user has accounts on every system and has physical access to everything, then all users are roughly equivalent in their level of threat.
   - **Separation of duties—**Carefully separate duties so that people involved in checking for inappropriate use are not also capable of perpetrating such inappropriate use. Having all the security functions and audit responsibilities entrusted to the same person is dangerous. This practice can lead to a case in which the person may violate security policy and commit prohibited acts, yet no other person sees the audit trail or is alerted to the problem.
   - **Limited reliance on key employees—**No one in an organization is irreplaceable. If your organization depends on the ongoing performance of a key employee, then your organization is at risk. Organizations cannot help but have key employees. To be secure, organizations should have written policies and plans established for unexpected illness or departure. As with systems, redundancy should be built into the employee structure. There should be no single employee with unique knowledge or skills.
5. The security officer of Alpha should take the following actions before relieving X from services of Alpha:
   1. Remove X's name from all lists of authorized access.
   2. Explicitly inform guards that X is not allowed into the building without special authorization by named employees.
   3. Take away any car parking sticker, official drawer/cupboard, and so on from X.
   4. If appropriate, change lock combinations, reprogram access card systems, and replace physical locks.
   5. Remove all personal access codes.
   6. Recover all assets, including employee ID card, disks, documents, and equipment.
   7. Check whether all relevant stakeholders have given no objection to Mr. X's termination.
   8. Notify, by memo or email, appropriate departments so that they are aware of the change in employment status.

6. The four levels of the cybersecurity learning continuum are as follows:

   - **Awareness—**A set of activities that explains and promotes security, establishes accountability, and informs the workforce of security news. Participation in security awareness programs is required for all employees.

   - **Cybersecurity essentials—**Intended to develop secure practices in the use of IT resources. This level is needed for those employees, including contractor employees, who are involved in any way with IT systems. It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.

   - **Role-based training—**Intended to provide knowledge and skills specific to an individual's roles and responsibilities relative to information systems. Training supports competency development and helps personnel understand and learn how to perform their security roles.

   - **Education/certification—**Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technological and social).

7. The goals for a security awareness program should include the following:

   - Provide a focused approach for all awareness, training, and educational activities related to information security, with better coordination to make it more effective.

   - Communicate key recommended guidelines or practices required to secure information resources.

   - Provide general and specific information about information security risks and controls to people on a need basis.

   - Make individuals aware of their responsibilities in terms of information security.

   - Motivate individuals to adopt recommended guidelines or practices by giving incentives (corporate goodies).

   - Create a stronger culture of security with individual commitment to information security.

   - Help enhance the consistency and effectiveness of existing information security controls and potentially stimulate the adoption of cost-effective controls.

   - Help minimize the number and extent of information security breaches, thus reducing costs directly (for example, data damaged by viruses) and indirectly (for example, reduced need to investigate and resolve breaches).

8. Impart awareness training by using the following instruments:

   - Brochures, leaflets, and fact sheets

   - Security handbook

- Regular email or newsletter
- Distance-learning web courses
- Workshops and training sessions by both internal and external sources
- Formal classroom coaching
- Online video tutorials
- A separate security website
- Email advisories issued by industry-hosted news groups, academic institutions, or the organization’s IT security office
- Professional organizations and vendors
- Online IT security daily news websites
- Periodicals
- Conferences, seminars, and workshops

9. Bring your own device (BYOD) is a strategy adopted by an organization that allows employees, business partners, and other users to utilize a personally selected and purchased client device to execute enterprise applications and access company data. A BYOD policy usually spans personal laptops, smartphones, and tablets. It can have various options, depending on the level of access and type of devices. Some challenges in implementing a BYOD strategy are as follows:

   - **Data management issues—**With mobile and cloud data storage solutions, it has become difficult to manage and track data, especially when devices have seamless connectivity and huge storage. It is not easy to distinguish between work data and personal data, and often companies have use third-party solutions to monitor data movement.
   - **Data compliance issues—**With the increased incidence of identity theft and phishing scams everywhere, government authorities have come up with strict regulations for data management. These measures increase operation and capital cost of doing business, and BYOD policies increase the complexity.
   - **Malicious applications—**Personal devices are vulnerable to malware and malicious apps. Further, an organization needs to be concerned about unauthorized access to corporate data via mobile apps. When employees download malicious apps on their cellphones, they give outsiders unauthorized access to critical corporate data. It is a headache to impose security software and add updates and patches on these devices.
   - **Lost or stolen devices—**Whenever devices that are registered in a BYOD network are lost or stolen, there is a high probability that sensitive corporate data can fall into the hands of an outsider with malicious intent.

- **Fired/disgruntled outgoing employees—**Employees can easily retain a certain amount of data (by making backups) even after they leave an organization. It is impractical for the HR department to check the data residing on an employee's smartphone, and such information can easily be leaked to a rival organization.
- **Hacking issues—**These days, it is easy to hack mobile devices. When a device is hacked, it can be used to connect to a corporate network to access business-critical information.

10. An ideal cybersecurity program should include following points:
    - Technical points about cybersecurity and its taxonomy, terminology, and challenges, with subtle details
    - Common information and computer system security vulnerabilities
    - Common cyber attack mechanisms, their consequences, and motivations behind them
    - Different types of cryptographic algorithms
    - Intrusion, types of intruders, techniques, and motivation
    - Firewalls and other means of intrusion prevention
    - Vulnerabilities unique to virtual computing environments
    - Social engineering and its implications to cybersecurity
    - Fundamental security design principles and their role in limiting points of vulnerability
11. The following measures are suggested:
    - The organization should have documented procedures in place for protecting physical assets, such as mobile devices, USB drives, and documents. Further, the organization should have in place more stringent procedures for remote access to company servers and databases, as well as cloud services used by the company.
    - There should be support for remote working by imparting adequate training (for example, how to perform backups and encrypt files) and adequate technical support as well as allowing use of secure tools such as VPN access to allow remote access. For sensitive documents, an additional layer of security must be implemented.
    - Additional controls and support, in terms of handling of information and sensitive data, should be provided for employees traveling to high-risk countries.
12. Malicious behavior involves deliberate and conscious attempts to harm an organization by acting inappropriately. Examples include sharing business files with a competitor, insider trading, and destroying project data to cause deliberate loss to the organization.

Negligent behavior is non-intentional but ignorant or lazy action to act inappropriately. It is often devoid of any motive to cause harm. Examples include using unauthorized services or devices to save time, doing personal work during office hours, and downloading movies from unsafe sites using office network.

Accidental behavior is non-intentional and non-deliberate action to act inappropriately. Such actions are usually done on impulse. Examples include emailing sensitive information to unauthorized recipients, opening malicious email attachments, publishing personal information on publicly available servers, and talking about a confidential product launch with a colleague in a public place.

Chapter 6

1. ISF's SGP divides information management into these four topics:

   - **Information classification and handling—**This encompasses methods of classifying and protecting an organization's information assets.
   - **Privacy—**This is broadly concerned with threats, controls, and policies related to the privacy of personally identifiable information (PII).
   - **Document and records management—**This covers the protection and handling of the documents and records maintained by an organization.
   - **Sensitive physical information—**This consists of specific issues related to the security of information assets in physical form.

2. The NIST risk management framework enumerates six steps for managing overall risk:

   1. **Categorization—**Here you identify information that will be transmitted, processed, or stored by the system and define applicable levels of information categorization based on an impact analysis.
   2. **Selection—**Here you select an initial set of baseline security controls for the system, based on the security categorization, and you tailor and supplement the security control baseline as needed.
   3. **Implementation—**Here you implement security controls and document how the controls are used within the system and its environment of operation.
   4. **Assessment—**Here you assess the security controls by using appropriate assessment procedures and try to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
   5. **Authorize—**This is about formal authority by the system to operate or continue to operate based on the results of the security control assessment. This decision is based

on a determination of the risk to organizational operations and assets resulting from the operation of the system and the decision that this risk is acceptable.

6. **Monitor—**Here you persistently monitor security controls to ensure that they are effective over time as changes occur in the system and the environment in which the system operates.

3. FIPS 199 provides the following generic format to define a security category:

   SC information type = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}

4. The four steps in the security categorization process given by NIST SP 800-60 are as follows:

   1. **Identify information types—**In this step, you identify the information types for classification, resulting in an information taxonomy or catalog of information types. The level of detail, or granularity, must be decided by consensus of security governance personnel. They may base their decision on factors such as the size of the organization, its range of activities, and the perceived overall level of risk.
   2. **Select provisional impact levels—**Here you assign security impact levels for the identified information types.
   3. **Review and adjust provisional impact levels—**Here you review the provisional impact levels, allowing a range of managers and information owners to contribute to the process. This results in fine-tuning of impact levels.
   4. **Assign system security category—**Finally, you run the security classification process to assign a security classification for each information type. If you follow SP 800-60, the overall classification of an information type corresponds to its assessed impact, which is the highest of the confidentiality, integrity, and availability impacts.

5. The following three organizational sources, as suggested by SP 800-60, define individual information types.

   - **Mission-based information—**This area encompasses types of information that relate specifically to the mission of the organization. For example, an organization in the healthcare field has information on what healthcare delivery services it provides, fee schedules, insurance arrangements, and policies for providing financial help to clients. A technology company has information about its research and development plans and goals, outside consulting arrangements, and long-range plans for new technology.

   - **Services delivery support functions—**These are types of information that support the operation of the organization and relate to specific services or products offered by the organization. For example, in the area of risk management and mitigation, information types include contingency planning, continuity of operations, and service recovery.

   - **Back office support functions—**These support activities enable the organization to operate effectively. SP 800-60 identifies five main groups of information types in this area: administrative management, financial management, human resource management, information management, and technology management.

6. In the context of information, the term *privacy* usually refers to making valuable private information about an individual unavailable to parties who have no permission (from the legitimate owner) as well as no direct need for that information. Privacy interests attach to the gathering, control, protection, and use of information about individuals and then using it for their own gains. For example, call centers handling credit card accounts leaking credit card details of subscribers to a marketing company would be a blatant violation of privacy.

7. The two terms are related. *Information security* can protect *privacy*. For example, an intruder seeking ostensibly private information (such as personal e-mails or photographs, financial or medical records, phone calling records) may be stymied by good cybersecurity measures. Additionally, security measures can protect the integrity of PII and support the availability of PII. But certain measures taken to enhance cybersecurity can also violate privacy. For example, some proposals call for technical measures to block Internet traffic containing malware before it reaches its destination. But to identify malware-containing traffic, the content of all in-bound network traffic must be inspected. But inspection of traffic by any party other than its intended recipient is regarded by some as a violation of privacy, because most traffic will, in fact, be malware-free. Under many circumstances, inspection of traffic in this manner is also a violation of law.

   Both these terms are very closely related and have a deep symbiotic relationship. *Information security* provides protection for all types of information, in any form, so that the information's confidentiality, integrity, and availability are maintained. *Privacy* assures that personal information is collected, processed (used), protected, and destroyed legally and fairly as per prevailing law of land.

8. Some possible types of threats in the information collection process are as follows:

   - **Surveillance—**This is the watching, listening to, or recording of an individual's activities without his or her consent or knowledge. This can be problematic and a violation of the right to privacy.
   - **Interrogation—**This is the act of pressuring an individual to divulge information by application of force (physical or mental). For example, if certain fields in a form or in an online registration process are required in order to proceed, the individual is compelled, or at least pressured, to divulge information that he or she would prefer not to.

9. Privacy can be violated at the information processing stage in the following ways:

   - **Aggregation—**Aggregation of data about an individual in various databases allows anyone with access to the aggregated data to learn more about an individual than could be learned from separate, and separately protected, data sets.
   - **Identification—**It is possible, with sufficient data, to be able to aggregate data from various sources and use those data to identify persons who are not otherwise identified in the data sets.

- **Insecurity—***Insecurity* refers to the improper protection and handling of PII. Identity theft is one potential consequence of insecurity. Another possible consequence is the dissemination of false information about a person, through alteration of that person's record.
- **Secondary use—**With secondary use, information about a person obtained for one purpose is used or made available for other purposes without consent.
- **Exclusion—**This is the failure to provide individuals with notice and input about their records.

10. Some potential privacy threats while disseminating information are as follows:
    - **Disclosure—**This refers to the public release of authentic personal information about an individual. The potential harm is damage to reputation or position in some form.
    - **Breach of confidentiality—**This is a disclosure that involves the violation of trust in a relationship. An example is the unauthorized release of medical information to a third party.
    - **Exposure —**This involves the exposing to others of certain physical and emotional attributes about a person, such as nude photographs or a video of an operation.
    - **Increased accessibility—**Public information is very easy to get these days, and thus this increases the likelihood of malicious use.
    - **Blackmail—**Blackmail involves the threat of disclosure. Ransomware is an example of blackmail in the cybersecurity context.
    - **Appropriation—**This involves the use of a person's identity or personality for the purpose of another.
    - **Distortion—**This refers to the manipulation of the way a person is perceived and judged by others and involves the victim being inaccurately exposed to the public. Distortion can be achieved by modifying records associated with an individual.
11. Invasion exposes the following types of threats:
    - **Intrusion—**This involves incursions into an individual's personal space. In the context of cybersecurity, intrusion is an act of penetrating into a network or a computer system and achieving some degree of access privilege to get or change some data. Intrusion is a part of a variety of security threats but can also cause a privacy threat. For example, the actual intrusion, or threat of intrusion, into a personal computer can disrupt the activities or peace of mind of the personal computer user.
    - **Decisional interference—**This techno-legal term involves the individual's interest in avoiding certain types of disclosure. To the extent that certain actions, such as registering for a government benefit, might generate data that could potentially be disclosed, the decision to perform those actions is deterred.

12. Some key principles of the EU's GDPR are as follows:

    - **Fair, lawful, and transparent processing—**This is very extensive and bound with legal terms. It includes, for example, an obligation to tell data subjects what their personal data will be used for.
    - **Purpose limitation—**This means that personal data collected for one purpose should not be used for a new, incompatible, purpose.
    - **Data minimization—**Subject to limited exceptions, an organization should only process the personal data that it actually needs to process in order to achieve its purposes.
    - **Accuracy—**Personal data must be accurate and recent. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.
    - **Data retention periods—**Personal data must be kept in a form viable to permit identification of data subjects for no longer than is necessary and for the purposes for which the data were collected or for which they are further processed. Data subjects hold the right to erasure of personal data at any point of time.
    - **Data security—**Technical and organizational measures must be taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, and unauthorized disclosure or access.
    - **Accountability—**The controller is obliged to demonstrate that its processing activities are compliant with the data protection principles.

13. NIST SP 800-53 organizes privacy controls into 8 families, with a total of 24 controls:

    - **Authority and purpose—**This family ensures that organizations identify the legal bases that authorize a particular PII collection or activity that impacts privacy and specify in their notices the purpose(s) for which PII is collected.
    - **Accountability, audit, and risk management—**This family consists of controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.
    - **Data quality and integrity—**The objective of this family is to ensure that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used.
    - **Data minimization and retention—**This family includes minimization of PII, data retention, and disposal and minimization of PII used in testing, training, and research.
    - **Individual participation and redress—**This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII.

- **Security—**This family ensures that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure. These controls are meant to supplement the organization's security controls that may be relevant to privacy.
- **Transparency—**This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities. This includes procedures for notifying individuals of the status of their PII and dissemination of privacy program information.
- **Use limitation—**This family ensures that the scope of PII use is limited to the intended purpose. This includes developing policies and procedures to limit internal access to PII to only those personnel who require and are authorized access, as well as similar policies and procedures for third parties outside the organization.

14. *Document* and *record* are very close in meaning but hold subtle differences when applied to information security. A document may be a record, but not all documents are records. A document is a work-in-progress object, and only authorized users can read, edit, and easily distribute it. A document is editable and therefore doesn't necessarily have to adhere to industry, government, or other regulatory standards. A record is an official file that clearly delineates terms and conditions, statements, or claims and is accepted as valid legal proof of authenticity of information.

15. The life of a record can be divided into three stages:

    1. **Active—**Here a record is used to support the organization's functions and reporting requirements. Generally, active records are referred to often during the regular course of business.
    2. **Semi-active—**Here a record is no longer needed to carry out current activities but must still be retained to meet the organization's administrative, fiscal, legal, or historical requirements.
    3. **Inactive—**Here a record is no longer required to carry out the administrative or operational functions for which it was created and is no longer retrieved or accessed. Such records can either be archived or destroyed.

16. Some supporting technologies that can be used to protect sensitive physical information are as follows:

    - Closed-circuit television (CCTV)
    - Locks
    - Alarms
    - Access control
    - Vaulting

- Intelligence reports
- First responder interfaces
- Facilities management solutions
- Fire protection systems
- Time locks
- Physical access solutions

17. Following are some key issues that can help secure physical information throughout its life cycle:

    - **Identify and document—**Each item of physical information needs to be identified properly, and its existence needs to be documented.
    - **Classification—**Every physical document or other type of media (example, DVD) should be classified according to the security classification policy of the organization.
    - **Label—**An appropriate security classification label must be affixed to or incorporated into the document itself.
    - **Storage—**Secure storage is needed for all physical assets. This may be a safe, a secure area of the facility, or other physical means of restricting and controlling access.
    - **Secure transport—**If sensitive information is to be sent by a third party, such as a courier or shipping service, policies and procedures must be in place to ensure that this is done securely.
    - **Disposal—**Some kind of retention and disposal policy should be implemented across the organization for physical assets.

Chapter 7

1. ISF's SGP divides physical asset management into four topics:

    - **Hardware life cycle management—**This encompasses the management of the entire life cycle of hardware that is used to support enterprise information systems. This includes product selection, testing, deployment, assessment, and decaying.
    - **Office equipment—**This covers peripheral devices such as printers, scanners, fax machines, and multifunction devices (MFD).
    - **Industrial control systems—**This covers security issues related to systems that monitor or control physical activities such as temperature, pressure, and velocity.

- **Mobile computing—**This deals with security issues related to the use of mobile devices in an enterprise information system.

2. ISF's SGP includes physical assets (for example, access gates at the entry to an office), embedded software within a physical asset (for example, embedded software on the employer's access gate), and operating systems that support any embedded software (for example, RTLinux).

3. Any organization should adopt a well-drafted hardware life cycle management policy, considering the following reasons:

   - The hardware asset should be retained until the cost of operating it is lower than the cost of low productivity, increased downtime, worker safety, and elevated levels of user dissatisfaction. A systematic approach to life cycle management can provide guidance on when to replace particular equipment.

   - Organizations not following any hardware asset management are often frustrated by the communication gaps that allow assets to be lost, acquisitions to be made when spares are in the warehouse, or upgrades failing due to incomplete information. All this swells operation cost and hits the top business line.

   - Hardware life cycles are vendor dependent; some vendors might follow a three-year cycle, while others might follow a five-year cycle. Hence, the organization should centralize this information in a configuration management database (CMDB).

   - Every hardware asset brings its own set of threats. An organization can reduce risk by having and using the tools to properly track and manage its hardware.

   - There is a need to map hardware with the applications installed on that hardware for software compliance management and reporting. For example, the organization should know how many bar code readers were not used for past three months and what version of firmware is installed on them to prepare for upgrade.

4. An organization should follow these steps to acquire any hardware asset:

   1. **Request and approval—**This includes application of standards, redeployment, and initiation of a purchase, if appropriate.
   2. **Vendor relationships—**This includes creation of contracts and management of vendor relationships.
   3. **Acquisition—**This includes contract negotiations and contract execution.
   4. **Receipt—**This triggers initiating payment of invoices and creating an incident to configure and deliver to the correct individual/location/department.

5. After deployment, equipment can be managed in several ways:

   - The best way to maintain it is by doing preventive maintenance. Depending on the nature of the work, usage, and asset type, proper monitoring must be done and, based on that, the service schedule should be decided.

- Another way is to track key hardware assets. Technology such as RFID and geotagging can help organizations ensure that critical assets, such as essential information system components, remain in authorized locations.
- All hardware must be properly monitored and measured on all key parameters.
- Hardware should be serviced on a regular basis, and it must be assessed on safety norms after each service.

6. There are three potential vulnerability sources in an MFD:

   - **Print, fax, and copy/scan logs—**With print logs, there is the threat of exposure of sensitive document names, network usernames, and URLs of websites users have printed from. Fax numbers indicate with whom an organization does business, and long-distance codes/long-distance credit-card numbers may show up with dialed numbers. Copy/scan logs can expose email addresses of recipients and logon information for FTP file uploads.
   - **Address books—**Some MFDs allow the user to create address books as distribution or destination lists. This may expose internal and customer email addresses and fax numbers, long-distance codes and credit-card numbers, and server addresses and usernames for FTP sites.
   - **Mailboxes—**Mailboxes are used to store scans, faxes, or templates on an MFD. Unless it is password protected, a mailbox could provide an attacker with entire faxes or scanned documents containing sensitive information.

7. Media sanitization a process of rendering access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort. Three increasingly secure actions for sanitization are defined:

   - **Clear—**Here you apply logical techniques to sanitize data in all user-addressable storage locations for protection against simple noninvasive data recovery techniques; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
   - **Purge—**Here you apply physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques. This can be achieved by performing multiple overwrites. For a self-encrypting drive, cryptographic erasure can be used. If the drive automatically encrypts all user-addressable locations, then all that is required is to destroy the encryption key, which could be done with multiple overwrites.
   - **Destroy—**This method renders target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data. Typically the medium is pulverized or incinerated at an outsourced metal destruction or licensed incineration facility.

8. The elements of an ICS are as follows:

    - **Sensor—**A sensor measures some phenomenon of a physical, chemical, or biological domain and delivers an electronic signal proportional to the observed characteristic, either in the form of an analog voltage level or a digital signal.
    - **Actuator—**An actuator receives an electronic signal from a controller and responds by interacting with its environment to induce a change in behavior of a physical, chemical, or biological entity.
    - **Controller—**The controller interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators. The controller is devoid of intelligence and needs a human–machine interface for direction.
    - **Human–machine interface—**Operators and engineers use human interfaces to monitor and configure set points, control algorithms, and adjust and establish parameters in the controller. The human interface also gives GUI displays about status and health of the system.
    - **Remote diagnostics and maintenance—**Diagnostic and maintenance utilities are used to prevent, identify, and recover from abnormal operations or failures.

9. An IT system is non-real time, whereas an ICS is hard real time. IT systems need a consistent response and tolerate some delay, but an ICS wants responses under scheduled time. High delay and jitter are not acceptable for an ICS, whereas they may be acceptable in an IT system. IT systems are not usually designed for critical emergency responsiveness, and usually an ICS is designed for that very reason. Finally, security can restrict access to an IT system and may affect its functionality, whereas an ICS need to be strictly controlled but not at the expense of hampering its functionality.

10. Some common security threats to an ICS are as follows:

    - Disruption of service due to blocked or delayed flow of information through ICS networks.
    - Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment; create environmental impacts; and/or endanger human life.
    - Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects.
    - ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.

- Financial losses due to interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Danger to human life due to interference with the safety operation.

11. A typical mobile device technology stack has four layers:

- **Hardware—**The base layer of the technology stack is termed hardware. This includes an application processor and a separate processor that runs the cellular network processor, typically referred to as the baseband processor. There are other chips, such as system clock, Wi-Fi controller, and USB controller. Further, there may be hardware-encryption modules and other security modules. The hardware layer also includes the peripherals incorporated into the device, such as a camera and SIM card. Vulnerabilities at this level can serve as attack vectors.
- **Firmware—**The firmware is needed to boot the mobile operating system (that is, the boot loader) and verify additional device initialization code, device drivers used for peripherals, and portions of the mobile operating system prior to the user actually using the device.
- **Mobile operating system—**Common operating systems for the mobile device are Android, iOS, and Symbian. The operating system lies between hardware and applications and helps the applications perform. It also isolates third-party applications in some manner to prevent unexpected or unwanted interaction between the system, its applications, and the applications' respective data (including user data). Vulnerabilities are routinely discovered in mobile device operating systems. However, the development of patches and the update of the software are beyond the control of the enterprise and in the hands of the operating system provider.
- **Application—**This layer includes third-party applications, utility apps, games, and services provided by the mobile device vendor and facilities for defining permissions.

12. According to SP 800-14, major security concerns for mobile devices are as follows:

- **Lack of physical security controls—**Mobile devices are mostly under the complete control of the user (password protection, biometric lock) and are used and kept in a variety of locations outside the organization's control, such as employee's home. Even if a device is required to remain on premises, the user may move the device within the organization between secure and insecure locations, thereby exposing it to theft and tampering threats. The threat is twofold: A malicious party may attempt to recover sensitive data from the device itself or may use the device to gain access to the organization's resources
- **Use of untrusted mobile devices—**Apart from official assets, virtually all employees have personal smartphones and/or tablets. The organization must assume that these devices are not trustworthy; the devices may not employ encryption and either the user or a third party may have installed a bypass to the built-in restrictions on security, operating system use, and so on.

- **Use of untrusted networks—**An employee's mobile device can connect to organization resources over the organization's own in-house wireless networks. However, for off-premises use, the user will typically access organizational resources via Wi-Fi or cellular access to the Internet and from there to the organization. Thus, traffic that includes an off-premises segment is potentially susceptible to eavesdropping or man-in-the-middle types of attacks.
- **Use of applications created by unknown parties—**It is very convenient to find and install third-party applications on mobile devices. This poses the obvious risk of installing malicious software since the user unintentionally may give complete access to mobile/PDA data to the new app.
- **Interaction with other systems—**All smartphones and tablets can automatically synchronize data, apps, contacts, photos, and so on with other computing devices and with cloud-based storage without paying much attention to security aspects. Unless an organization has control of all the devices involved in synchronization, there is considerable risk of the organization's data being stored in an unsecured location, and there is also a risk of the introduction of malware.
- **Use of untrusted content—**Mobile devices may access and use content in unique ways. Here the vulnerability is twofold: The content is untrustable, and the access method is not foolproof. An example is the Quick Response (QR) code, which is a two-dimensional barcode. QR codes are designed to be captured by a mobile device camera and used by the mobile device. A QR code translates to a URL, and a malicious QR code could direct mobile devices to malicious websites.
- **Use of location services—**The GPS capability on mobile devices can be used to track the physical location of the device to the nearest cell. This can be a security risks as an attacker can use the location information to determine where the device and user are located, which may be of use to the attacker.

13. NIST has developed a tool called AppVet that provides automated management support of the app testing and app approval or rejection activities. AppVet facilitates the app vetting workflow by providing an intuitive user interface for submitting and testing apps, managing reports, and assessing risk.

Chapter 8

1. The initiation phase typically consists of the following tasks:
   - **Strategy—**This task involves ensuring that the system release is fully aligned to all master strategy and intent.
   - **Research—**This task involves determining opportunities and solution options that meet requirements.

- **Feasibility—**This task involves ensuring that if the overall strategy is acceptable to management, then the team takes the next step to examine the viability of the system in terms of economic, financial, technology, operations, social, and organization factors.
- **Planning—**This task includes activities such as detailing what will actually go into the systems release (for example, new features and break-fixes), creating initial project plans, and improving budget estimates.
- **Requirements—**This task is primarily focused on developing the requirements specification of what needs to be accounted for in downstream design and implementation activities.

2. The development/acquisition phase typically involves two types of testing:
    - **Integration testing—**This type of testing takes as scope all interfaces of the system (to other entities). Here all data and technology connections are tested for a specific system moving through the SDLC and all its upstream system dependencies (user layer) and all its downstream system targets (service layer).
    - **User acceptance testing—**This takes as scope the entire system and tests system functions that end users will be able to execute while operating in the final production environment.
3. The changeover is implemented by running the new system with the data from one or more of the previous periods for the whole system or part of it. The results are compared with the old system results, and the old system is replaced if and only if the results prove better. It is less expensive and risky than the parallel run approach. This strategy builds confidence, and the errors are traced easily, without affecting the operations at all.
4. The DevOps methodology rests on the joint effort of all participants—including business unit managers, developers, operations staff, security staff, and end user groups—in creating a product or system collaborating from the beginning. DevOps can be defined as the practice of operations and development engineers participating together in the entire service life cycle, from design through the development process to active production support. The techniques can range from using source control to debugging to testing and to participating in an Agile development process.
5. Major stages in the life cycle of an application/system are as follows:
    1. **Development—**Developers build and deploy code in a test environment, and the development team tests the application at the most basic level. The application must meet certain criteria for advancement to the next phase.
    2. **System integration testing—**The application is tested to ensure that it works with existing applications and systems. The application must meet the criteria of this environment before it can move to the next phase.

3. **User acceptance testing—**The application is tested to ensure that it provides the required features for end users. This environment is usually production-like. The application must pass these requirements to move to the next phase.
4. **Production—**The application is made available to users. Feedback is captured by monitoring the application's availability and functionality. Any updates or patches are introduced in the development environment to repeat this cycle.

6. The four phases of the DevOps reference architecture are as follows:

   1. **Plan and measure—**This activity focuses on business units and their planning process. The planning process relates business needs to the outcomes of the development process. This activity can start with small, limited portions of the overall plan, identifying outcomes and resources needed to develop the required software. The plan must include developing measures that are used to evaluate software, adapt and adjust continually, relate to customer needs, and continually update the development plan and the measurement plan.
   2. **Develop and test—**This activity focuses on collaborative development, continuous integration of new code, and continuous testing of the system. It focuses on catching the synergies of development and testing teams. Useful tools are automated tracking of testing against measured outcomes and virtualized test beds that enable testing in an isolated but real-world environment.
   3. **Release and deploy—**This activity provides a continuous delivery pipeline that automates deployment to test and production environments using variety of tools. Releases are managed centrally in a collaborative environment that leverages automation. Deployments and middleware configurations are automated and then matured to a self-service model that gives individual developers, teams, testers, and deployment managers the capability to continuously build, provision, deploy, test, and promote.
   4. **Monitor and optimize—**This activity includes the practices of continuous monitoring, customer feedback, and optimization to monitor how applications are performing, allowing businesses to adapt their requirements as needed.

7. The two key foundations on which DevOps rests are collaboration and automation. Collaboration begins with management policy to encourage and require the various actors in the software development and deployment process to work together. Automation consists of tools that support that collaboration and are designed to automate as much as possible this cyclic process.

8. Control gates are decision points at the end of each phase when the system needs be evaluated and management needs to determine whether the project should continue as is, change direction, or be discontinued. Typical examples of control gates are performance review, code review, and financial feasibility analysis.

9. Key security considerations that exist throughout the SDLC are as follows:

    - **Secure concept of operations—**There should be an operations or business continuity document for secure development that contains a contingency plan for the code repository as well as documents as both are the predominant work products of software and system development and should be preserved in the event of interruption to the development environment.

    - **Standards and processes—**These play the role of a guide and help decide and document appropriate security processes for the assurance level required by the system.

    - **Security training for development team—**Additional security training may be needed for key developers to understand the current threats and potential exploitations of their products as well as training for secure design and coding techniques, based on the prevailing standards and need.

    - **Quality management—**This includes planning, assurance, and control that are keys to ensuring minimal defects in and proper execution of the information system.

    - **Secure environment—**The development environment—including workstations, servers, network devices, and code repositories—needs to meet the organization's security requirements. A secure development environment is a prerequisite for developing secure software and systems.

    - **Secure code practices and repositories—**These should be religiously followed. Special attention should be placed on code repositories, with an emphasis on systems that support distributed code contribution with check-in/check-out functionality. Role-based access should apply to accessing the code repository, and logs should be reviewed regularly as part of the secure development process. When possible, completed software components that have passed security certification should be retained as reusable components for future software development and system integration.

10. Some of the control gates at the development/acquisition phase are as follows:

    1. **Architecture/design review—**Here you do review of the security architecture and design that evaluates its integration with other systems and the overall enterprise architecture.
    2. **Performance review—**Here you evaluate whether the system meets the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use.
    3. **Functional test review—**Here you ensure that functional requirements are sufficiently detailed and are testable after deployment.
    4. **Risk management review—**Here you review the risk management decisions made up to that point and their impact on the system or its security controls.
    5. **Mid-project status and financial review—**Here you determines if there have been changes in the planned level of effort and evaluate the effect on costs and benefits.

11. The key activities for disposal phase are:

    - **Create disposal/transition plan—**This plan makes all stakeholders aware of the future plan for the system and its information. The plan should document all the planned steps for disposal.
    - **Ensure information protection—**Any information that is to be archived or otherwise retained must be accessible by appropriate hardware in the future. If the information is encrypted, appropriate key management functions must be invoked.
    - **Sanitize media—**The procedures of SP 800-88 or similar standards should be followed to ensure thorough sanitization.
    - **Dispose of hardware and software—**Hardware and software can be sold, given away, destroyed, or discarded, as provided by applicable law or regulation.
    - **Close system—**The information system is formally shut down and disassembled at this point.

12. According to the International Foundation for Information Technology, best practices for managing the SDLC are as follows:

    - **Ownership—**Assign full, unambiguous accountability for system development management to key individuals, committees, or departments.
    - **Inventory—**Religiously maintain a central database of all items related to the management of system development, including requirements, deliverables, and the status of control gates.
    - **Terminology—**Be consistent in the use of standard terminology for the various aspects of system development.
    - **Data centralization—**Maintain core data—that is, data that is required by or is useful for stakeholders involved in system development in a central repository.
    - **Metrics—**Ensure that management discuss and agree on a set of performance metrics that can be defined, tracked, and analyzed to assess progress in system development.
    - **Standards and best practices—**Follow, to the maximum extent possible, industry standards and best practices for system development. This helps in interoperability and legal compliance.
    - **Transparency—**Strive to make any and all system development management data transparent to all other appropriate stakeholders, at a minimum, and often to the entire enterprises.

13. The International Foundation for Information Technology defines the following environments for system development:

    - **Research—**This environment is used as an isolated sandbox for researching the viability of technologies and solutions, often implemented in the form of a proof of concept, a study, or an experiment.

- **Developer work space—**This environment accommodates the activities associated with the private or localized implementation that is performed by a single or individual resource, such as a software coder or an engineer, to provide an isolated working area that provides the flexibility to work freely without interference with or from other environments where other resources may be working.
- **Centralized build—**This environment accommodates the activities associated with centralized or merged builds. In this environment, the individual developer products are brought together to create a single, unified build.
- **Integration testing—**An isolated environment is used to test the integrations (that is, the data communications connections, channels, and exchanges) between the product, system, or software release being worked on and those of other products, systems, or instances of software that the release is intended to work with and communicate with during its operation in other downstream environments, such as production.
- **User acceptance testing—**This environment enables human interaction with the system for the purpose of obtaining final approval and sign-off for the features and functions of the release.
- **Production—**This environment is the final targeted environment where a product, system, or software release operates for business use. This environment is deemed to be the most critical, as failures in this environment can potentially disturb or even shut down a line of business, depending on the importance of the product, system, or software being used by its end users.

Chapter 9

1. Application management (AM), in a nutshell, is the process of managing the operation, maintenance, versioning, and upgrading of an application throughout its life cycle. It includes best practices, techniques and procedures that are critical for any deployed application's optimal operation, performance, and efficiency throughout the enterprise and back-end IT infrastructure.
2. The key stakeholders of application management are as follows:
    - **Application owners—**These are key business executive personnel who view AM in terms of business productivity, revenue, and control.
    - **Application developers/managers—**These are key IT enterprise personnel responsible for application development, deployment, and maintenance.
    - **Application testers—**These are key IT enterprise personnel responsible for testing, validating, and certifying an application for production.

- **Application users—**These are end users of an application. For them, AM is measured according to security, privacy, versioning, and overall control of application processes and modules.

3. Application life cycle management typically has following stages.

    1. **Gather requirements—**Here the business units identify the functional and business process requirements for the change or new application.
    2. **Design—**In this phase, the design team translates the requirements into a technical solution. IT infrastructure planners, solution architects, and so on typically get involved at this step, and simulation tools help them effectively assess long-term requirements. This ensures that IT infrastructure resources are available to support ongoing operations of the new application.
    3. **Build, integrate, test—**In this phase, all the components and flows are developed and tested both individually and in integration with the system to uncover any functional and process flaws. Detecting adverse impacts early in the development process helps developers take appropriate actions quickly.
    4. **Implement, deploy—**This covers the rollout of the new application. The application modules are first put into production libraries. Then any customer training required to effectively and efficiently use the new facilities is provided.
    5. **Operate—**Here you monitor and measure the application in the following areas:

        - Addressing changes in regulatory requirements
        - Fixing flaws uncovered in the application
        - Monitoring service levels (and addressing problems in missed service levels)
        - Measuring and reporting on application performance

    6. **Optimize—**Here IT management uses past measurement and in-house heuristics to seek ways to optimize existing applications. Areas of concern include performance, capacity utilization, and user satisfaction and productivity.

4. Total cost of ownership (TCO), in a generic sense, is an analysis to determine all the lifetime costs that follow from owning certain kinds of assets. From an applications point of view, it is a detailed analysis of information technology (IT) or other costs across enterprise boundaries over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses, and the opportunity costs of downtime, training, and other productivity losses.

5. According to Gartner, an effective APM strategy consists of following steps:

    1. **End-user experience monitoring—**The first step is to capture both qualitative and quantitative elements of user experience. It is a precursor to determining how end-to-end performance impacts the user and identifies any problem. This step is the most important.

2. **Runtime application architecture discovery, modeling, and display—**The second step is to study the software and hardware components involved in application execution, as well as their communication paths, to establish the potential scope of the problem. In this step, you get to know the specific components (hardware or software) fueling the application's performance. For example, a database server may be broken down into components such as processor, memory, disk, query execution time, and so forth.
3. **User-defined transaction profiling—**In this step, you record user-defined transactions and analyze them to identify the source of the problem. Here the concern is not so much with the total transaction time but rather with what portions of the application are spending time processing the transaction.
4. **Component deep-dive monitoring in an application context—**The fourth step is about conducting deep-dive monitoring of the resources consumed by and events occurring within the components found in step 2.
5. **Analytics—**Finally, you use analytics to crunch the data generated in the first four steps, discover meaningful and actionable patterns, pinpoint the root cause of the problem, and ultimately anticipate future issues that may impact the end user.

6. COTS stands for commercial-off-the-shelf (COTS), and it refers to a software or hardware item that is commercially available for leasing, licensing, or sale to the general public in its original form, without any (major) need for a modification or maintenance over the life cycle of the product to meet the needs of the procuring agency (for example, Windows 10, MATLAB, or BlueJ IDE for Java development).

7. ModSecurity is an open source software web application firewall (WAF). A WAF is a firewall that monitors, filters, or blocks data packets as they are transiting from a web application. It can be run as a standalone server in a premises network or as a server plug-in or as a cloud service. The key role of a WAF is to inspect each packet and use a rule table (application logic) to analyze and filter out potentially harmful traffic.

   Some of its salient features are as follows:

   - **Real-time application security monitoring and access control—**Full-duplex HTTP traffic sieves through ModSecurity, where it is thoroughly inspected and filtered. ModSecurity also has a persistent storage mechanism, which enables tracking of events over time to perform event correlation.

   - **Virtual patching—**This is the ability to apply web application patching without making any direct modifications to the application. Virtual patching is applicable to applications that use any communication protocol, but it is particularly useful with HTTP because the traffic can generally be well understood by an intermediary device.

   - **Complete bidirectional HTTP traffic logging—**Unlike many other web services, ModSecurity has the ability to log events, including raw transaction data, which is essential for forensics. In addition, the system manager gets to choose which transactions are logged, which parts of a transaction are logged, and which parts are sanitized.

- **Web application hardening—**This is a method of attack surface reduction in which the system manager selectively narrows down the HTTP features that will be accepted (for example, request methods, request headers, and content types).

8. Some of the benefits of EUDAs are as follows:

    - **Convenience and ease of use—**EUDAs can be developed easily and quickly by non-IT staff to meet the requirements of the end users. EUDAs allow businesses and users to quickly deploy solutions in response to shifting market and economic conditions, industry changes, or evolving regulations.

    - **Powerful tools and technology-aware end users—**End-user tools offer rich functionality, including the ability to connect to corporate data sources. As a result, technology-savvy users can perform powerful data processing from their desktops. This can help plug functionality gaps for business systems.

    - **Demand for more and more information—**Traditionally, managers were often constrained by standard reports in IT systems that failed to meet all management information and reporting requirements. The lack of flexibility in these systems and increasing demand for different views of the data have resulted in an increase in the level of end-user computing in organizations.

9. There are a number of disadvantages and risks to EUDAs:

    - **Errors—**Errors can occur at nearly any stage, such as at data entry, within formulas, within application logic, or with links to other applications or data sources. Without a sound SDLC discipline, such errors are bound to occur, and they could result in poor decision making or inaccurate financial reporting.

    - **Poor version and change control—**EUDAs do not follow a standard method of development and thus they can be more difficult to control than more traditional IT-developed applications.

    - **Poor documentation—**EUDAs generally have very poor or no documentation. Files that have not been properly documented may be used incorrectly after a change in ownership of the EUDA, or they may just be improperly used in general. Again, this can lead to unintended and undetected errors.

    - **Lack of security—**Users are more interested in getting their problems solved than in evaluating security. Hence, they generally exchange files in an insecure manner. This can lead to increased errors, or it might allow sensitive and confidential information to be seen by unauthorized users. An EUDA could possibly be used to perpetuate fraud or hide losses.

- **Lack of audit trail—**EUDAs are mostly unaudited. The ability to audit and control changes to key data is essential both for internal governance and for compliance with external regulation. For critical applications, managing this risk effectively is crucial and in many instances requires monitoring and controlling changes at a detailed level.
- **Regulatory and compliance violations—**A host of regulations deal with security and privacy for which the enterprise is responsible.
- **Unknown risk—**The greatest operational risk with the use of EUDAs is not knowing the magnitude and severity of a potential problem. The use of EUDAs is so widespread that it may be extremely difficult to assess just how many exist, how many are used in critical business applications, how they are linked together, and where data is fed into or extracted from other IT applications. To quantify this risk, it is necessary to carry out a full inventory of EUDA usage and a detailed risk assessment of all business-critical spreadsheets.
- **Opportunity cost—**Scarce resources (money or employee time) may be wasted on developing these applications, which would otherwise be utilized in work that provides a financial returns.

10. There are four key elements of the EUDA security framework:

    - **Governance—**As part of good governance, senior executives must define what constitutes a EUDA. This involves distinguishing EUDAs from IT-developed and supported applications and specifying which types of EUDAs should be placed under management control.
    - **People—**It is the duty key stakeholders to properly manage and control EUDAs, and thus there should be a proper process to identify them. Once the key stakeholders are identified, the next step is to establish the roles and responsibilities. Stakeholder roles include the program sponsor, central program group, steering committee, business unit representatives, EUDA users, and internal auditors.
    - **Process—**There should be a proper process for assessing the security of an EUDA. Management's top concern with respect to EUDAs is the potential risks of any given application. For each EUDA, the EUDA owner can apply a risk model to determine which EUDAs should be placed under formal management control. Furthermore, there should be an inventory or register of all EUDAs that are under management control, with details concerning the application, including security-related aspects.
    - **Technology—**From a technology point of view, an organization should perform an assessment to identify tools and techniques needed to support the development of EUDAs. Specific EUDA management software tools can be deployed, or native functionality (such as Microsoft SharePoint) can be used; various degrees of functionality are available in different products.

Chapter 10

1. The term AAA stands for authorization, authentication, and access control. Authorization implies granting of access rights of system resources to a user, program, or process. Authorization comes after successful authentication and defines possible actions for an authenticated user or agent. Authentication is the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Access control is the process of granting or denying specific requests, such as accessing and using information and related information processing services and or entering specific physical facilities.

2. There are two main functions involved in user authentication:

   - **Identification—**This involves presenting an identifier to the security system to verify the identity with respect to the system.

   - **Verification—**This involves presenting or generating authentication information that corroborates the binding between the entity and the identifier.

3. The NIST 800-63 digital identity model involves three pivotal concepts:

   - **Digital identity—**The digital identity is the unique representation of a subject engaged in an online transaction. The representation consists of an attribute or set of attributes that uniquely describe a subject within a given context of a digital service but does not necessarily uniquely identify the subject in all contexts.

   - **Identity proofing—**This process establishes that a subject is who he or she claims to be to a stated level of certitude. This process involves collecting, validating, and verifying information about a person.

   - **Digital authentication—**This process involves determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate.

4. NIST's digital identity model involves six entities:

   - **Credential service provider (CSP)—**This refers to a trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.

   - **Verifier—**This refers to an entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators, using an authentication protocol.

   - **Relying party (RP)—**This refers to an entity that relies on the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

- **Applicant—**This refers to a subject undergoing the processes of enrollment and identity proofing.
- **Claimant—**This refers to a subject whose identity is to be verified using one or more authentication protocols.
- Subscriber**—**This refers to a party who has received a credential or an authenticator from a CSP.

5. There are three authentication factors in user identity authentication:

   - **Knowledge factor—**This is something that is partly or fully known by an individual. It requires the user to demonstrate knowledge of hidden information. Normally, it is used in single-layer authentication processes in the form of passwords, passphrases, PINs, or answers to secret questions. Examples include a password, a personal identification number (PIN), or answers to a prearranged set of questions.
   - **Possession factor—**This is something possessed by the individual. It is normally a physical entity possessed by the authorized user to connect to the client computer or portal. This type of authenticator is referred to as *hardware token*, of which there are two types. Connected hardware tokens are items that physically connect to a computer in order to authenticate identity, and disconnected hardware tokens are items that do not directly connect to the client computer but instead require input from the individual attempting to sign in.
   - **Inherence factor—**This is something intrinsically present in the individual. It refers to the characteristics, called biometrics, that are unique or almost unique to the individual. These include static biometrics, such as fingerprint, retina, and face; and dynamic biometrics, such as voice, handwriting, and typing rhythm.

6. Common attacks on password-based authentication along with their mitigation steps are as follows:

   - **Offline dictionary attack—**In this type of attack, an attacker bypasses system controls and gains access to the password file. The attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker can gain access by using that ID/password combination. Countermeasures include controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords in the event that the password file is compromised.
   - **Specific account attack—**This is a variation of the preceding attack type, but here the attacker uses a popular password and tries it against a wide range of user IDs. A user's tendency is to choose a password that is easily remembered; this unfortunately makes the password easy to guess. Countermeasures include policies to inhibit the selection by users of common passwords and scanning the IP addresses of authentication requests and client cookies for submission patterns.

- **Password guessing against a single user—**Here the attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password. Countermeasures include training in and enforcement of password policies that make passwords difficult to guess. Such policies address the secrecy, minimum length of the password, character set, prohibition against using well-known user identifiers, and length of time before the password must be changed.
- **Workstation hijacking—**Here the attacker waits until a logged-in workstation is unattended. The standard countermeasure is automatically logging the user out of the workstation after a period of inactivity. Intrusion detection schemes can be used to detect changes in user behavior.
- **Exploiting user mistakes—**This type of attack exploits users' mistakes. A user may intentionally share a password to enable a colleague to share files, for example. Also, attackers are frequently successful in obtaining passwords by using social engineering tactics that trick the user or an account manager into revealing a password. Countermeasures include user training, intrusion detection, and simpler passwords combined with another authentication mechanism.
- **Exploiting multiple password use—**Here the attacker can harm more than one system as the user has set the same password for multiple systems. Countermeasures include a policy that forbids using the same or similar password on particular network devices.
- **Electronic monitoring—**Here the attack can snoop the network traffic to extract a password that is transmitted over a network. Simple encryption will not fix this problem because the encrypted password is, in effect, the password and can be observed and reused by an adversary.

7. The salt value serves three purposes in terms of hashing:

   - It makes duplicate passwords invisible in the password file. Even if two users choose the same password, those passwords will be assigned different salt values. Hence, the hashed passwords of the two users will differ.
   - It makes offline dictionary attacks significantly difficult. For a salt of length b bits, the number of possible passwords is increased by a factor of 2b, increasing the difficulty of guessing a password in a dictionary attack because and exponential order algorithm takes years of computation to solve.
   - It becomes nearly impossible to find out whether a person with passwords on two or more systems has used the same password on all of them.

8. The major vulnerabilities of password file protection are as follows:

   - A hacker may be able to exploit a software vulnerability in the operating system to bypass the access control system long enough to extract the password file. Alternatively, the hacker may find a weakness in the file system or database management system that allows access to the file.

- An accident of protection or a manual slip might render the password file readable, thus compromising all the accounts.
- Some users may have accounts on other machines in other protection domains, for which they might use the same password. Thus, if the passwords could be read by anyone on one machine, a machine in another location might be compromised.
- A lack of or weakness in physical security may aid a hacker. Sometimes there is a backup to the password file on an emergency repair disk or archival disk. Access to this backup enables the attacker to read the password file. Alternatively, a user may boot from a disk running another operating system such as Linux and access the file from that operating system.
- Instead of capturing the system password file, another approach to collecting user IDs and passwords is through sniffing network traffic when a user is trying to log in to an unsecured channel.

9. The potential drawbacks of using a memory card as an authentication device are as follows:
    - **Requirement of special reader—**this Increases the cost of using the hardware token and creates the requirement to maintain the security of the reader's hardware and software.
    - **Hardware token loss—**This event can temporarily prevent the owner of a lost token from gaining system access. Thus, there is an administrative cost in replacing the lost token. In addition, if the token is found, stolen, or forged, then an adversary now need only determine the PIN to gain unauthorized access.
    - **User dissatisfaction—**Users may find using memory cards for computer access inconvenient, unnecessary, and futile.
10. You can categorize authentication protocols used in a smart grid in the following manner:
    - **Static—**With a static protocol, the user authenticates himself or herself to the token, and then the token authenticates the user to the computer. The latter half of this protocol is similar to the operation of a memory token.
    - **Dynamic password generator—**Here both the token and the computer system are actively involved. The token generates a unique password periodically—say every minute. This password is then entered into the computer system for authentication, either manually by the user or electronically via the token. The token and the computer system must be initialized and kept synchronized so that the computer knows the password that is current for this token.
    - **Challenge-response—**In this case, the computer system generates a challenge, such as a random string of numbers. The smart token generates a response based on the challenge.
11. A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. OTP tokens are usually

pocket-size fobs with a small screen that displays a number. The number changes periodically, say every 30 or 60 seconds, depending on how the token is configured. An OTP is more secure than a static password and has the potential to replace authentication login information or may be used to add another layer of security.

12. Possible threats to possession-based authentication are as follows:

    - **Theft—**An attacker can steal a token device. If a second factor is required, such as a PIN, the attacker must also use some means to obtain or guess the PIN. If the second factor is biometric, the attacker must come up with some way of forging the biometric characteristic.
    - **Duplication—**The attacker gains access to the device and clones it. Again, if a second factor is required, the attacker's task is more formidable.
    - **Eavesdropping/replaying—**The authenticator secret or authenticator output is revealed to the attacker as the subscriber is authenticating. This captured information can be used later. If there is a time-sensitive aspect to the exchange, such a nonce or the use of an OTP, this latter attack can be thwarted.
    - **Replay—**If the attacker can interpose between the token device and the server, this constitutes a man-in-the-middle attack, in which the attacker assumes the role of the client to the server and the server to the client.
    - **Denial of service—**The attacker makes repeated failed attempts to access the server, which may cause the server to lock out the legitimate client.
    - **Host attack—**The attacker may gain sufficient control of the authentication server to enable the attacker to be authenticated to an application.

13. A biometric authentication system uses unique physical characteristics of an individual to authenticate the user. These include static characteristics, such as fingerprints, hand geometry, facial characteristics, and retinal and iris patterns; and dynamic characteristics, such as voiceprint, signature, and gait movement. Internally biometrics is based on pattern recognition, and biometric authentication is both technically complex and expensive compared to other methods.

14. Major criteria in designing a biometric system are as follows:

    - **Universality—**A very high percentage of the population should have the characteristic. For example, virtually everyone has recognizable fingerprints, but there are rare exceptions.
    - **Distinctiveness—**No two people should have identical characteristics. For some otherwise acceptable characteristics, identical twins share virtually the same patterns, such as facial features and DNA, but not other features, such as fingerprints and iris patterns.

- **Permanence—**The characteristic should not change with time. For otherwise acceptable characteristics, such as facial features and signatures, periodic reenrollment of the individual may be required.
- **Collectability—**Obtaining and measuring the biometric feature(s) should be easy, non-intrusive, reliable, and robust, as well as cost-effective for the application.
- **Performance—**The system must meet a required level of accuracy, perform properly in the required range of environments, and be cost-effective.
- **Circumvention—**The difficulty of circumventing the system must meet a required threshold. This is particularly important in an unattended environment, where it would be easier to use such countermeasures and a fingerprint prosthetic or a photograph of a face.
- **Acceptability—**The system must have high acceptance among all classes of users. Systems that are uncomfortable to the user, appear threatening, require contact that raises hygienic issues, or are non-intuitive are unlikely to be acceptable to the general population.

15. The false match rate (FMR) is an important measure of biometric authentication system performance. The FMR is the rate at which a biometric process mismatches biometric signals from two distinct individuals as coming from the same individual.

16. Presentation attack detection (PAD) involves methods created to directly counter spoof attempts at the biometric sensor and are of two kinds: artifact detection and liveness detection. Artifact detection attempts to determine the originality of the sample. For example, for a voice detector, an artificial detector will attempt to determine if it is a human voice or produced by a voice synthesizer. Liveness detection attempts to determine the actuality of the sample. For instance, it will answer the question "Is the biometric sample at the sensor from a living human presenting a sample to be captured?" For example, is it a fingerprint sensed from the user's finger, or is it a fingerprint presented by the lift of a fingerprint onto a printed surface?

17. NIST SP 800-63 provides a useful way of characterizing the risk of an authentication system by using the concept of authentication assurance level (AAL). The AAL describes the degree of confidence in the registration and authentication processes. A higher level of AAL indicates that an attacker must have better capabilities and expend greater resources to successfully subvert the authentication process.

18. There are three levels of AAL.

    1. **AAL1—**This level provides some assurance that the claimant controls an authenticator bound to the subscriber's account. It requires either single-factor or multifactor authentication, using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

2. **AAL2—**This level provides high confidence that the claimant controls the authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s).
3. **AAL3—**This level provides very high confidence that the claimant controls the authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication requires use of a hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance.

19. An out-of-band device is a physical device with a unique address and that can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel. The device is possessed and controlled by the claimant and supports private communication over this secondary channel, separate from the primary channel for e-authentication.

20. Customer access refers to the access to business applications by individuals such as end users of an online ecommerce site, or subcontractors of a manufacturing companies, or vendors of a semiconductor company. Customer access presents additional considerations and security challenges beyond those involved with system access for employees. Before providing customers with access to specific applications and information resource, a risk assessment needs to be carried out and the required controls identified. An individual or a group within the organization should be given responsibility for authorizing each customer access arrangement. Furthermore, there should be approved contracts between the organization and the customer that cover security arrangements. Any customer access to system resources should be subject to the same types of technical controls as with employees. It is a big legal and ethical responsibility of an organization to protect data about the customer.

Chapter 11

1. According to SGP, system management is divided into two areas: system configuration and system maintenance. The objective of *system configuration* is to develop and enforce consistent system configuration policies that can cope with current and protected workloads and protect systems and the information they process and store against malfunction, cyber attack, unauthorized disclosure, and loss. The objective of *system maintenance* is to provide guidelines for the management of the security of systems by performing backups of essential information and software, applying a rigorous change management process, and monitoring performance against agreed service level agreements.

2. NIST SP 800-123 mentions the following common security threats to servers:

   - Malicious entities may exploit software bugs in the server or its underlying operating system to gain unauthorized access to the server. Further, they may attack other entities after compromising a server. These attacks can be launched directly (for example, from the compromised host against an external server) or indirectly (for example, placing malicious content on the compromised server that attempts to exploit vulnerabilities in the clients of users accessing the server).

- Denial-of-service (DoS) attacks may be directed to the server or its supporting network infrastructure, denying or hindering valid users from making use of its services.
- Sensitive information on the server may be read by unauthorized individuals or changed in an unauthorized manner.
- Sensitive information transmitted unencrypted or weakly encrypted between the server and the client may be intercepted.
- Malicious entities may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the server.

3. The SANS Institute describes the following general requirements for server security:
   - All internal servers deployed at the organization must be owned by an operational group that is responsible for system administration.
   - Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the CISO.
   - Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the CISO. Specifically, the following items must be met:
     - Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
       - Server contact(s) and location and a backup contact
       - Hardware and operating system/version
       - Main functions and applications, if applicable
     - Information in the corporate enterprise management system must be kept up-to-date.
     - Configuration changes for production servers must follow the appropriate change management procedures.
4. Virtualization is the process of creating a non-real (or virtual) representation of an entity. It is a technology that provides an abstraction of the computing resources used by some software, which thus runs in a simulated environment called a virtual machine (VM). Virtualization improves efficiency in the use of the physical system resources compared to what is typically seen using a single operating system instance. Virtualization can also provide support for multiple distinct operating systems and associated applications on the one physical system. It can be a very cost-effective solution to a firm that wants to launch its product in a short time and on a small budget.

5. A hypervisor is software that runs on top of hardware and gives services to the VMs by acting as a resource broker. It allows multiple VMs to safely coexist on a single physical server host and share that host's resources. The virtualizing software provides abstraction of all physical resources (such as processor, memory, network, and storage) and thus enables multiple computing stacks, called virtual machines, to be run on a single physical host. Principal functions of hypervisor are as follows:

   - **Execution management of VMs—**This includes scheduling VMs for execution, virtual memory management to ensure VM isolation from other VMs, and context switching between various processor states. It also includes isolation of VMs to prevent conflicts in resource usage and emulation of timer and interrupt mechanisms.
   - **Device emulation and access control—**This is all about emulating all network and storage (block) devices that different native drivers in VMs are expecting, mediating access to physical devices by different VMs.
   - **Execution of privileged operations by hypervisor for guest VMs—**In certain cases, operations are invoked by guest operating systems, instead of being executed directly by the host hardware, and they may have to be executed by the hypervisor because of their privileged nature.
   - **Management of VMs (also called VM life cycle management) —**This is about configuring guest VMs and controlling VM states (for example, start, pause, stop).
   - **Administration of hypervisor platform and hypervisor software—**This involves setting parameters for user interactions with the hypervisor host as well as hypervisor software.

6. There are two types of hypervisors based on the presence of the operating system between the hypervisor and the host. A type 1 hypervisor is loaded as a software layer directly onto a physical server; this is referred to as *native virtualization*. The type 1 hypervisor can directly control the physical resources of the host. A type 2 hypervisor exploits the resources and functions of a host operating system and runs as a software module on top of the operating system; this is referred to as *hosted virtualization*. It relies on the operating system to handle all the hardware interactions on the hypervisor's behalf.

7. In container virtualization, a software piece known as a *virtualization container* runs on top of the host operating system kernel and provides an isolated execution environment for applications. Unlike hypervisor-based VMs, containers do not aim to emulate physical servers. Instead, all containerized applications on a host share a common operating system kernel. This eliminates the need for resources to run a separate operating system for each application and can greatly reduce overhead. For containers, only a small container engine is required as support for the containers. The container engine sets up each container as an isolated instance by requesting dedicated resources from the operating system for each container. Each container app then directly uses the resources of the host operating system.

8. The three categories of network storage systems are as follows:

   - **Direct attached storage (DAS)—**This is internal server hard drives that are generally captive to the attached server.
   - **Storage area network (SAN)—**A SAN is a dedicated network that provides access to various types of storage devices, including tape libraries, optical jukeboxes, and disk arrays. To servers and other devices in the network, a SAN's storage devices look like locally attached devices.
   - **Network attached storage (NAS)—**NAS systems are networked appliances that contain one or more hard drives that can be shared with multiple, heterogeneous computers. Their specialized role in networks is to store and serve files. NAS disk drives typically support built-in data protection mechanisms, including redundant storage containers or redundant arrays of independent disks (RAID). NAS enables file-serving responsibilities to be separated from other servers on the network and typically provides faster data access than traditional file servers.

9. A service level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the performance standards the provider is obligated to meet. SLAs are output based, with the sole purpose of specifically defining what service the customer will receive. Companies that establish SLAs include IT service providers, managed service providers, and cloud computing service providers. Three important types of SLAs are as follows:

   - **Network provider SLA—**A network SLA is a contract between a network provider and a customer that defines specific aspects of the service that is to be provided.
   - **Computer security incident team SLA—**A computer security incident response team (CSIRT) SLA typically describes the response to an incident, preventive actions to stop such incidents, and steps takes to beef up security of the system.
   - **Cloud service provider SLA—**An SLA for a cloud service provider should include security guarantees such as data confidentiality, integrity guarantees, and availability guarantees for cloud services and data.

10. An organization can ensure effective backup by following these policies:

    - Backups of all records and software must be retained such that computer operating systems and applications are fully recoverable. The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data. At a minimum, backup copies must be retained for 30 days.
    - Tri level or, better, *N* level redundancy must be maintained at the server level.
    - At a minimum, one fully recoverable version of all data must be stored in a secure offsite location. An offsite location may be in a secure space in a separate building or with an approved offsite storage vendor.

- Derived data should be backed up only if restoration is more efficient than re-creation in the event of failure.
- All data information accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to allow for backup. Data located directly on workstations, laptops, or other portable devices should be backed up to networked file server drives.
- Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.
- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- Recovery procedures must be tested on an annual basis.

11. FIPS 199 describes three types of sites for backup:
    - **Cold site—**This is a backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from the main computing location to an alternate site
    - **Warm site—**This is an environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.
    - **Hot site—**This constitutes a fully operational offsite data processing facility, equipped with hardware and software, with prime use in the event of an information system disruption.
12. The following are some useful guidelines for developing a change management strategy:
    - **Communication—**Adequate advance notice should be given, especially if a response is expected and a proper response matrix with contact details is known.
    - **Maintenance window—**A maintenance window is a defined period of time during which maintenance, such as patching software or upgrading hardware components, can be performed. Clearly defining a regular maintenance window can be advantageous as it provides a time when users should expect service disruptions
    - **Change committee—**The change committee reviews change requests and determine whether the changes should be made. In addition, it may determine that certain changes to the proposed plan for implementing the change must be made in order for it to be acceptable.

- **Critical changes—**There must be provision to accommodate critical changes that are needed to be rushed into production, creating an unscheduled change.
- **Plan the change—**All aspects associated with the change (who what, when, and so on) must be carefully planned.
- **Document change requests—**A change request form provides detailed information about the change and is appropriate for changes affecting data classified as confidential (highest, most sensitive) where protection is required by law and where the asset risk is high and involves information that provides access to resources, physical or virtual.
- **Test the change—**The change should be tested prior to implementation.
- **Execute the change—**The change should be properly executed.
- **Keep a record of the change—**A log or other record of all changes should be kept to supplement the change request document.

Chapter 12

1. Key functions of network management are as follows:
    - **Fault management—**This refers to facilities that enable the detection, isolation, and correction of abnormal operation of the OSI environment.
    - **Accounting management—**This refers to facilities that enable charges to be established for the use of managed objects and costs to be identified for the use of those managed objects.
    - **Configuration management—**This refers to facilities that exercise control over, identify, collect data from, and provide data to managed objects for the purpose of assisting in providing for continuous operation of interconnection services.
    - **Performance management—**This refers to facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities.
    - **Security management—**This refers to aspects of OSI security that are essential to operate OSI network management correctly and to protect managed objects.
2. Some of the key tasks performed by a network management entity or NME are as follows:
    1. Collect statistics on communications and network-related activities.
    2. Store of statistics locally.
    3. Respond to commands from the network control center, including commands to do the following:
        - Transmit collected statistics to the network control center
        - Change a parameter (example, a timer used in a transport protocol)

        - Provide status information (example, parameter values, active links)
        - Generate artificial traffic to perform a test
    4. Send messages to the NCC when local conditions undergo a significant change.

3. In a decentralized network management scheme, there may be multiple top-level management stations, called *management servers*. Each such server might directly manage a portion of the total pool of agents. However, for many of the agents, the management server delegates responsibility to an intermediate manager. The intermediate manager plays the role of manager to monitor and control the agents under its responsibility. It also plays an agent role in providing information and accepting control from a higher-level management server. This scheme reduces total network traffic and distributes the processing burden.

4. According to Cisco, the network management architecture has three layers:

    - **Element management layer—**This layer provides an interface to the network devices and communications links in order to monitor and control them. This layer captures events and fault occurrences through a combination of direct polling and unsolicited notification by network elements. Management function modules provide interfaces to specific elements, allowing elements from different manufacturers to be incorporated under a single management control.

    - **Network management layer—**This layer provides a level of abstraction that does not depend on the details of specific elements. In terms of event management, this layer takes input from multiple elements, correlates the information received from the various sources (also referred to as root-cause analysis), and identifies the event that has occurred.

    - **Service management layer—**The service management layer is responsible for adding intelligence and automation to filtered events, event correlation, and communication between databases and incident management systems.

5. Firewalls use four techniques to control access and enforce the site's security policy:

    - **Service control—**A firewall determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; it may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a web or mail service.

    - **Direction control—**A firewall determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

    - **User control—**A firewall controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as that provided by IPsec.

- **Behavior control—**A firewall controls how particular services are used. For example, the firewall may filter email to eliminate spam, or it may enable external access to only a portion of the information on a local web server.

6. Principal types of firewalls are:
   - Packet filtering firewall
   - Stateful inspection firewalls
   - Application-level gateway
   - Circuit-level gateway
7. Packet filters have following weaknesses:
   - A packet filtering firewall cannot prevent attacks that employ application-specific vulnerabilities or functions as these firewalls do not examine upper-layer data.
     For example, if a packet filtering firewall cannot block specific application commands and if a packet filtering firewall allows a given application, all functions available within that application will be permitted.
   - The logging functionality present in packet filtering firewalls is limited as these firewalls have access to limited information.
   - Most packet filtering firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality.
   - Packet filtering firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Many packet filtering firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered.
   - Packet filtering firewalls are susceptible to security breaches caused by improper configurations. This means it is easy to accidentally configure a packet filtering firewall to allow traffic types, sources, and destinations that should be denied based on an organization’s information security policy.
8. Some of the important characteristics of automated network device configuration management tools are as follows:
   - **Multivendor device support—**The solution should support all device types from all popular vendors.
   - **Discovery capability for device addition—**The solution should have provision for discovering the devices in the network and automatically adding them, in addition to other device addition options.
   - **Communication protocols—**The solution should support a wide range of protocols to establish communication with the device and transfer configuration files.

- **Secure storage—**The configuration data should be stored in encrypted form and protected against intrusion.
- **Inventory—**The solution should provide an informative inventory of the devices being managed. It should provide various details, such as serial numbers, interface details, chassis details, port configurations, IP addresses, and hardware properties of the devices.
- **Configuration operations and schedules—**The solution should provide simple, intuitive options in the GUI to carry out various configuration operations, such as configuration retrieval and viewing, editing, and uploading configurations back to the device.
- **Configuration versioning—**A version number should be associated with the configuration of each device and incremented with each change.
- **Baseline configuration—**The solution should have provision for labeling the trusted configuration version of each device as a baseline version to enable administrators to roll back configurations to the baseline version in the event of a network outage.
- **Access control—**An attribute-based or role-based access control scheme should be used to provide security when multiple users have access to configuration tools.
- **Approval mechanism—**The security policy in an enterprise may require certain types of changes carried out by certain levels of users to be reserved for review and approval by top administrators prior to the deployment of the changes.

9. A TIA-942 compliant data center has following functional areas:

   - **Computer room—**This is the portion of the data center that houses date processing equipment.
   - **Entrance room—**This area houses external network access provider equipment and provides an interface between the computer room equipment and the enterprise cabling systems.
   - **Main distribution area—**This is a centrally located area that houses the main cross-connect as well as core routers and switches for LAN and SAN infrastructures.
   - **Horizontal distribution area (HDA)—**The HDA serves as the distribution point for horizontal cabling and houses cross-connects and active equipment for distributing cable to the equipment distribution area.
   - **Equipment distribution area (EDA)—**The EDA houses equipment cabinets and racks, with horizontal cables terminating with patch panels.
   - **Zone distribution area (ZDA)—**This is an optional interconnection point in the horizontal cabling between the HDA and EDA. The ZDA can act as a consolidation point for reconfiguration flexibility or for housing freestanding equipment, such as mainframes.

10. Some of the main risks associated with wireless access are as follows:

    - **Insufficient policies, training, and awareness—**Wireless security controls must include policies and user awareness training specifically for wireless access. These should include procedures regarding uses of wireless devices and an understanding of relevant risks.
    - **Access constraints—**Wireless access points repeatedly send out signals to announce themselves so that users can find them to initiate connectivity. This signal transmission occurs when beacon frames containing the access points' service set identifiers (SSIDs) are sent unencrypted. SSIDs are names or descriptions used to differentiate networks from one another. This signal transmission makes it easy for unauthorized users to learn the network name and attempt an attack or intrusion.
    - **Rogue access points—**Rogue access points are APs that users install without coordinating with IT. Access controls, encryption, and authentication procedures enable IT to maintain control.
    - **Traffic analysis and eavesdropping—**An eavesdropper can snoop the communication and interpret the communication. To counter this threat, it is necessary to use a strong user authentication technique and to encrypt all traffic.
    - **Insufficient network performance—**Poor performance may be due to an imbalance in the use of access points, insufficient capacity planning, or a denial-of-service (DoS) attack.
    - **Hacker attac**ks**—**Hackers attempt to gain unauthorized access over wireless networks. Intrusion detection systems, antivirus software, and firewalls are mitigation techniques.
    - **Physical security deficiencies—**This is in the domain of physical security. Both network devices and mobile devices should be subject to physical security policies and procedures.

11. SP 800-41 defines firewall planning and implementation phases in the following manner:

    1. **Plan—**The first phase of the process involves identifying all requirements for an organization to consider when determining what firewall to implement to enforce the organization's security policy.
    2. **Configure—**The second phase involves all facets of configuring the firewall platform. This includes installing hardware and software as well as setting up rules for the system.
    3. **Test—**The next phase involves implementing and testing a prototype of the designed solution in a lab or test environment. The primary goals of testing are to evaluate the functionality, performance, scalability, and security of the solution and to identify any issues—such as interoperability—with components.
    4. **Deploy—**When testing is complete and all issues are resolved, the next phase focuses on deployment of the firewall into the enterprise.

5. **Manage—**After the firewall has been deployed, it is managed throughout its life cycle, including component maintenance and support for operational issues. This life cycle process is repeated when enhancements or significant changes need to be incorporated into the solution.

12. In general, email security threats can be classified as follows:

    - **Authenticity-related threat—**This threat arises from not being able to verify authenticity. It could result in unauthorized access to an enterprises' email system. Another threat in this category is deception, in which the purported author isn't the actual author.
    - **Integrity-related threat—**This threat could result in unauthorized modification of email content.
    - **Confidentiality-related threat—**This threat could result in unauthorized disclosure of sensitive information.
    - **Availability-related threat—**This threat could prevent end users from being able to send or receive email.

13. ISO 27002 advocates the following ways to protect email:

    - Protecting messages from unauthorized access, modification, or denial of service commensurate with the classification scheme adopted by the organization.
    - Ensuring correct addressing and transportation of the message.
    - Ensuring reliability and availability of the service.
    - Giving legal consideration, such as requirements for electronic signatures.
    - Obtaining approval prior to using external public services such as instant messaging and social networking.
    - Using file sharing instead of sending sensitive data unencrypted over email.
    - Using stronger levels of authentication to control access from publicly accessible networks.

14. The two main types of infrastructure equipment that support VoIP are as follows:

    - **IP PBX—**This is designed to support digital and analog phones and connect to IP-based networks using VoIP, as well as provide, if needed, a connection to the public switched telephone network using traditional technology.
    - **Media gateway—**This connects different physical networks in order to provide end-to-end connectivity. An important type of media gateway connects a VoIP network to a circuit-switched telephone network, providing the necessary conversion and signaling.

15. Some of the key threats for VoIP usage are as follows:

    - **Spam over Internet telephone (SPIT)—**Unsolicited bulk messages may be broadcast over VoIP to phones connected to the Internet. Although marketers already use voicemail for commercial messages, IP telephony makes a more effective channel because the sender can send messages in bulk instead of dialing each number separately.
    - **Eavesdropping—**Interception of control packets enables an adversary to listen in on an unsecured VoIP call.
    - **Theft of service—**This type of attack involves capturing access codes, allowing the adversary to get into the VoIP provider network and then use the facility.
    - **Man-in-the middle attack—**This type of attack involves an adversary inserting as a relay point between two ends of a VoIP call. In addition to eavesdropping, the adversary could divert a call to a third party or generate simulated voice content to create misleading impressions or cause operational errors.

16. The Standards Customer Council defines the following key components of a cloud service agreement (CSA):

    - **Customer agreement—**This section describes the overall relationship between the customer and the provider. Its terms include how the customer is expected to use the service, methods of charging and paying, reasons a provider may suspend service, termination, and liability limitations.
    - **Acceptable use policy—**This section prohibits activities that providers consider to be improper or outright illegal uses of their service. Conversely, the provider usually agrees not to violate the intellectual property rights of the customer.
    - **Cloud service level agreements—**These agreements define a set of service level objectives. These objectives may concern availability, performance, security, and compliance/privacy. The SLA specifies thresholds and financial penalties associated with violations of these thresholds. Well-designed SLAs can significantly contribute to avoiding conflict and can facilitate the resolution of an issue before it escalates into a dispute.
    - **Privacy policies—**These policies describe the different types of information collected; how that information is used, disclosed, and shared; and how the provider protects that information.

Chapter 13

1. ICT, which stands for information communication technology, comprises a collection of devices, networking components, applications, and systems that together allow people and organizations to interact in the digital world. ICT is generally used to represent a broader, more comprehensive list of all components related to computer and digital technologies than IT.

2. A supply chain is an end-to-end network of all the individuals, organizations, resources, activities, and technology involved from the creation to the sale of a product or service. It typically starts from the delivery of source materials from the supplier to the manufacturer and goes through to eventual delivery to the end user. In this traditional use, the term applies to the entire chain of production and use of physical products. An ICT supply chain is a linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer.

3. Three types of flows are associated with a supply chain:

   - **Product/service flow—**This refers to the flow of intermediate products or services. A key requirement is a smooth flow of an item from the provider to the enterprise and then on to the internal user or external customer.

   - **Information flow—**This comprises the request for key information items such as quotations, purchase orders, monthly schedules, engineering change requests, quality complaints, and reports on supplier performance from the customer side to the supplier. From the producer's side to the consumer's side, the information flow consists of the presentation of the company, offer, confirmation of purchase order, reports on action taken on deviation, dispatch details, report on inventory, invoices, and so on.

   - **Money flow—**This refers to the actual flow of money or currency from client to seller. On the basis of the invoice raised by the producer, the clients examine the order for correctness. If the claims are correct, money flows from the clients to the respective producer. Flow of money is also observed from the producer side to the clients, in the form of debit notes.

4. Key elements of a supply chain management are as follows:

   - **Demand management—**This function meets all demands for goods and services to support the marketplace. It involves prioritizing demand when supply is lacking. Proper demand management facilitates the planning and use of resources for profitable business results.

   - **Supplier qualification—**This refers to ability to provide an appropriate level of confidence that suppliers, vendors, and contractors are able to supply consistent quality of materials, components, and services, in compliance with customer and regulatory requirements.

   - **Supplier negotiation—**This is a formal process of communication in which two or more people come together to seek mutual agreement over an issue(s). Negotiation is particularly appropriate when issues besides price are important for the buyer or when competitive bidding will not satisfy the buyer's requirements on those issues.

- **Sourcing, procurement, and contract management—**Sourcing refers to the selection of a supplier(s). Procurement is the formal process of purchasing goods or services. Contract management is a strategic management discipline employed by both buyers and sellers whose objectives are to manage customer and supplier expectations and relationships, control risk and cost, and contribute to organizational profitability/success.
- **Logistics and inventory control—**Here logistics refers to the process of strategically managing the procurement, movement, and storage of materials, parts, and finished inventory (and the related information flows) through the organization and its marketing channels. Inventory control is the tracking and accounting of procured items.
- **Invoice, reconciliation, and payment—**This is about payment of goods and services.
- **Supplier performance monitoring—**This includes the methods and techniques used to collect information that can be used to measure, rate, or rank a supplier's commitment to honor commitments and enterprise objectives on a continuous basis.

5. According to SP 800-161, the three tiers of risk management model that are defined in SP 600-39 are as follows:
   - **Tier 1—**This tier is engaged in the development of the overall ICT SCRM strategy, determination of organization-level ICT SCRM risks, and setting of the organizationwide ICT SCRM policies to guide the organization's activities in establishing and maintaining organizationwide ICT SCRM capability
   - **Tier 2—**This tier is engaged in prioritizing the organization's mission and business functions, conducting mission-/business-level risk assessment, implementing Tier 1 strategy, establishing an overarching organizational capability to manage ICT supply chain risks, and guiding organizationwide ICT acquisitions and their corresponding SDLCs.
   - **Tier 3—**This tier is involved in specific ICT SCRM activities to be applied to individual information systems and information technology acquisitions, including integration of ICT SCRM into these systems' SDLCs.
6. Key external risks of a supply chain are as follows:
   - **Demand—**This relates to potential or actual disturbances to the flow of product, information, and cash emanating from within the network between the focal firm and its market. For example, disruptions in the cash resource within the supply chain can have a major impact on the operating capability of organizations.
   - **Supply—**This is the upstream equivalent of demand risk; it relates to potential or actual disturbances to the flow of product or information emanating within the network upstream of the focal firm. The disruption of key resources coming into the organization can have a significant impact on the organization's ability to perform.
   - **Environmental—**This refers to the risk associated with external and, from the firm's perspective, uncontrollable events. The risks can impact the firm directly or through its

suppliers and customers. Environmental risk is broader than just natural events such as earthquakes or storms. It also includes, for example, changes created by governing bodies such as changes in legislation or customs procedures, as well as changes in the competitive climate.

7. Key internal risks of a supply chain are as follows:

   - **Processes—**This refers to the sequences of value-adding and managerial activities undertaken by the firm. Process risk relates to disruptions to key business processes that enable the organization to operate. Some processes are key to maintaining the organization's competitive advantage, and others underpin the organization's activities.
   - **Control—**This refers to the assumptions, rules, systems, and procedures that govern how an organization exerts control over the processes and resources. In terms of the supply chain, this may be order quantities, batch sizes, safety stock policies, and so on, plus the policies and procedures that govern asset and transportation management.
   - **Mitigation—**This refers to a hedge against risk built in to the operations themselves. Mitigation needs to be considered during the supply chain design process; if it is not undertaken, the risk profile can be increased. Contingency is the existence of a prepared plan and the identification of resources that can be mobilized in the event of a risk being identified. This requires all stakeholders in the supply chain to understand what resources can be mobilized and the procedures to do this.

8. SP 800-161 organizes security controls for SCRM into the following categories:

   - Access control
   - Awareness and training
   - Audit and accountability
   - Security assessment and authorization
   - Configuration management
   - Contingency planning
   - Identification and authentication
   - Incident response
   - Maintenance
   - Media protection
   - Physical and environmental protection
   - Planning
   - Program management

- Personnel security
- Provenance
- Risk assessment
- System and services acquisition
- System and communications protection
- System and information security

9. The three security controls of the provenance family are as follows:

   - **Provenance policy and procedures—**This provides guidance for implementing a provenance policy.
   - **Tracking provenance and developing a baseline—**This provides details concerning the tracking process.
   - **Auditing roles responsible for provenance—**This indicates the role auditing plays in an effective provenance policy.

10. Cloud computing is a model for enabling ubiquitous, convenient, on-demand, and scalable network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

11. The key characteristics of cloud computing are as follows:

    - **Broad network access—**This refers to wide network coverage over a range of devices. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, laptops, PDAs) as well as other traditional or cloud-based software services.
    - **Rapid elasticity—**This refers to the ability to expand and reduce resources according to specific service requirements. For example, there may be a need for large number of server resources for the duration of a specific task. After that task, those resources can be released.
    - **Measured service—**Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
    - **On-demand self-service—**By this tenant, a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. Because the service is on demand, the resources are not permanent parts of the IT infrastructure.

- **Resource pooling—**The provider's computing resources may be pooled to serve multiple consumers, using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

12. The three service models of cloud computing, according to NIST, are as follows:

    - **Software as a service (SaaS)—**In this model, the consumer can use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains these functions from the cloud service. SaaS eliminates the complexity of software installation, maintenance, upgrades, and patches. Examples of services at this level are Gmail, Google's email service, and Salesforce.com, which helps firms keep track of their customers.

    - **Platform as a service (PaaS)—**In this model, the consumer can deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. PaaS often provides middleware-style services such as database and component services for use by applications.

    - **Infrastructure as a service (IaaS)—**In this model, the consumer is provided with processing, storage, network, and other fundamental computing resources where the consumer is able to deploy and run software, which can include operating systems and applications. IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems in a short period of time.

13. NIST defines four deployment models:

    - **Public cloud—**Here the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The cloud provider is responsible for both the cloud infrastructure and the control of data and operations within the cloud.

    - **Private cloud—**Here the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premises or off premises. The cloud provider is responsible only for the infrastructure and not for the control.

    - **Community cloud—**Here the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, security requirements, policy, compliance considerations). It may be managed by the organization or a third party and may exist on premises or off premises.

    - **Hybrid cloud—**Here the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (for example, cloud bursting for load balancing between clouds).

14. NIST's cloud computing reference architecture defines the following central elements:

    - **Cloud consumer—**This refers to a person or an organization that maintains a business relationship with, and uses service from, cloud providers.
    - **Cloud provider—**This refers to a person, an organization, or an entity responsible for making a service available to interested parties.
    - **Cloud auditor—**This refers to a party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
    - **Cloud broker—**This refers to an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.
    - **Cloud carrier—**This refers to an intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.

15. Some of the threats to cloud service users are as follows:

    - **Responsibility ambiguity—**This arises from the fact that cloud service users consume delivered resources through service models, thereby making the customer-built IT system dependent on those services. The lack of a clear definition of responsibility among cloud service users and providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomalies or incidents.
    - **Loss of governance—**This refers to reduction on full control of IT systems. The decision by an enterprise to migrate a part of its own IT system to a cloud infrastructure implies giving partial control to the cloud service providers. This loss of governance depends on the cloud service models. For instance, IaaS delegates only hardware and network management to the provider, while SaaS also delegates operating system, application, and service integration in order to provide a turnkey service to the cloud service user.
    - **Loss of trust—**It is sometimes difficult for a cloud service user to recognize the provider's trust level due to the black-box feature of the cloud service. There is no measure to obtain and share the provider's security level in a formalized manner.
    - **Service provider lock-in—**This refers to tight binding with the cloud service provider. Loss of governance could result in lack of freedom in how to replace one cloud provider with another. This could be the case if a cloud provider relies on nonstandard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.
    - **Insecure cloud service user access—**As most of the resource deliveries are through remote connections, non-protected APIs (mostly management APIs and PaaS services)

are among the easiest attack vectors. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities may achieve results.

- **Lack of information/asset management—**Because the physical assets are not hosted at the user's premises, a cloud service user may have serious concerns about lack of information/asset management from cloud service providers, such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), and disaster recovery. Furthermore, cloud service users also may have important concerns about exposure of data to foreign governments and compliance with privacy laws.
- **Data loss and leakage—**This threat may be strongly related to the preceding item. However, loss of an encryption key or a privileged access code will bring serious problems to cloud service users. Accordingly, lack of cryptographic management information, such as encryption keys, authentication codes, and access privilege, will lead to sensitive damages, such as data loss and unexpected leakage to the outside.

16. The Standards Customer Council defines the following key components of a cloud service agreement (CSA):

    - **Customer agreement—**This section describes the overall relationship between the customer and the provider. Its terms include how the customer is expected to use the service, methods of charging and paying, reasons a provider may suspend service, termination, and liability limitations.
    - **Acceptable use policy—**This section prohibits activities that providers consider to be improper or outright illegal uses of their service. Conversely, the provider usually agrees not to violate the intellectual property rights of the customer.
    - **Cloud service level agreements—**These agreements define a set of service level objectives. These objectives may concern availability, performance, security, and compliance/privacy. The SLA specifies thresholds and financial penalties associated with violations of these thresholds. Well-designed SLAs can significantly contribute to avoiding conflict and can facilitate the resolution of an issue before it escalates into a dispute.
    - **Privacy policies—**These policies describe the different types of information collected; how that information is used, disclosed, and shared; and how the provider protects that information.

Chapter 14

1. Technical security controls are safeguards or countermeasures designed for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system (for example, biometric controls).

2. Security architecture is a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. Its key characteristics are as follows:

   - It consists of a transparent and coherent overview of models, principles, starting points, and conditions that give a concrete interpretation of the information security policy, usually without speaking in terms of specific solutions.
   - It reduces a complex problem into models, principles and subproblems that can be understood.
   - The models and principles show where to take which type of measures, when the principles are applicable, and how the principles connect with other principles.

3. The SABSA model consists of six layers:

   1. **Contextual security architecture—**This layer describes the key business issues, starting with the assets, the motivation for providing security, the business processes, the organization, geographical dispersion, and key time-related considerations in these processes.
   2. **Conceptual security architecture—**This layer considers the security characteristics of each of the business drivers. The SABSA ICT Business Attribute Taxonomy, a set of attributes described in business language that reflect security characteristics, has been developed for this. The standard taxonomy has 50 attributes in addition to the traditional security attributes confidentiality, availability, and integrity. By associating a set of attributes with each business driver, it is possible to define a security architecture in a way that provides full traceability to business needs.
   3. **Logical security architecture—**This layer provides a design layer view, focusing on the delivery of services and information to meet the security concept.
   4. **Physical security architecture—**This layer takes care of the delivery of tangible items to support the logical services.
   5. **Component security architecture—**This layer defines the hardware and tools to deliver the physical design and provides a mapping to conform to standards.
   6. **Security service management architecture—**This layer takes care of issues related to how the organization manages the architecture

4. The two-way traceability is as follows:

   - **Completeness—**Completeness answers the question “Has every business requirement been met?” The layers and matrix allow you to trace every requirement through to the components that provide a solution.
   - **Justification—**Justification answers the question “Is every component of the architecture needed?” When someone questions “Why are we doing it this way?” the rationale is plain if you trace back to the business requirements that drive the specific solution.

5. Some common types of malware are as follows:
    - Adware
    - Auto-rooter
    - Backdoor/trapdoor
    - Exploit
    - Downloader
    - Dropper
    - Flooder
    - Keylogger
    - Kit (virus generator)
    - Logic bomb
    - Malware as a Service
    - Mobile code
    - Potentially unwanted program (PUP)
    - Ransomware
    - Remote access Trojan or RAT
    - Rootkit
    - Spammer program
    - Spyware
    - Trojan horse
    - Virus
    - Web drive-by
    - Work
    - Zombie/bot
6. SP 800-83 indicates that good malware software has the following capabilities:
    - It must scan critical host components, such as startup files and boot records.
    - It must watch real-time activities. Good anti-malware software should be configured to perform real-time scans of each file as it is downloaded, opened, or executed, which is known as on-access scanning.

- It must monitor common applications, such as email, instant messaging software, email clients, and Internet browsers. Good anti-malware software monitors activity involving the applications most likely to be used to infect hosts or spread malware to other hosts.
- It must scan each file for known malware. Anti-malware software on hosts should be configured to scan all hard drives regularly to identify any file system infections and, optionally, depending on organization security needs, to scan removable media inserted into the host before allowing its use.
- It must be capable of identifying common types of malware as well as attacker tools.
- It must be capable of disinfecting and quarantining files. Disinfecting files refers to removing malware from within a file, and quarantining files means storing files containing malware in isolation for future disinfection or examination.

7. Identity and access management (IAM) is a framework for business processes that facilitates the management of electronic or digital identities. The framework includes the organizational policies for managing digital identity as well as the technologies needed to support identity management. Typically, these policies fall into two categories:

   - **Provisioning process—**Provides users with the accounts and access rights they require to access systems and applications
   - **User access process—**Manages the actions performed each time a user attempts to access a new system, such as authentication and sign-on

   There are three ways to deploy it:

   - **Centralized—**All access decisions, provisioning, management, and technology are concentrated in a single physical or virtual location. Policies, standards, and operations are pushed out from this single location.
   - **Decentralized—**Local, regional, or business units make the decisions for all access choices, provisioning, management, and technology.
   - **Federated—**Each organization subscribes to a common set of policies, standards, and procedures for the provisioning and management of users. Alternatively, the organizations can buy a service from a supplier.

8. Some of the best practices for avoiding common security mistakes with IAM are as follows:

   - Proactively train staff to spot warning signs of phishing attacks and social engineering.
   - Patch promptly to guard against attacks.
   - Sensibly encrypt data.
   - Deploy multifactor authentication judiciously.
   - Implement least-privilege access controls by giving access to systems only when it is needed.

- Implement controls and monitoring tools to access privileged systems and data.
- Protect your mobile and cloud applications.
- Stop breaches that start on endpoints by granting access to apps and infrastructure from trusted and secured endpoints.
- Implement portals for accessing the web as SaaS applications using single sign-on (SSO).

9. An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Typically, it detects and reports all types of anomalies. There are two types of IDSs:

   - **Host-based IDS—**This monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Host-based IDSs can determine exactly which processes and user accounts are involved in a particular attack on the operating system.
   - **Network-based IDS—**This monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

10. Two generic approaches to intrusion detection are as follows:

    - **Misuse detection—**Misuse detection is based on rules that specify system events, sequences of events, or observable properties of a system that are believed to be symptomatic of security incidents. Misuse detectors use various pattern-matching algorithms, operating on large databases of attack patterns, or signatures. An advantage of misuse detection is that it is accurate and generates few false alarms. A disadvantage it that it cannot detect novel or unknown attacks.
    - **Anomaly detection—**Anomaly detection is based on detection of activity that is different from the normal behavior of system entities and system resources. An advantage of anomaly detection is that it is able to detect previously unknown attacks based on an audit of activity. A disadvantage is that there is a significant trade-off between false positives and false negatives.

11. Some common ways to recognize sensitive data in real time are as follows:

    - **Rule-based—**Regular expressions, keywords, and other basic pattern-matching techniques are best suited for basic structured data, such as credit card numbers and Social Security numbers. This technique efficiently identifies data blocks, files, database records, and so on that contain easily recognized sensitive data.
    - **Database fingerprinting—**This technique searches for exact matches to data loaded from a database, which can include multiple-field combinations, such as name, credit card number, and CVV number.

- **Exact file matching—**This technique involves computing the hash value of a file and monitoring for any files that match that exact fingerprint. This is easy to implement and can be used to check whether a file has been accidentally stored or transmitted in an unauthorized manner.
- **Partial document matching—**This technique looks for a partial match on a protected document. It involves the use of multiple hashes on portions of the document, such that if a portion of the document is extracted and filed elsewhere or pasted into an email, it can be detected.

12. Principal users of DRM system are as follows:
    - **Content provider—**The content provider holds digital rights to the content and wants to protect these rights (for example, a music record label, a movie studio).
    - **Distributor—**The distributor provides distribution channels, such as an online shop or a web retailer. For example, an online distributor receives the digital content from the content provider and creates a web catalog that presents the content and rights metadata for the content promotion (for example, IndiaCast).
    - **Consumer—**The consumer uses the system to access the digital content by retrieving downloadable or streaming content through the distribution channel and then paying for the digital license (for example, Netflix users).
    - **Clearinghouse—**The clearinghouse handles the financial transaction for issuing the digital license to the consumer and pays royalty fees to the content provider and distribution fees to the distributor accordingly (for example, PCH/Media).
13. Cryptography is a method of converting ordinary plaintext into unintelligible text and vice versa. It is a way of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication. It is useful in the following processes:
    - **Data encryption—**Data encryption is a powerful and cost-effective means of providing data confidentiality and data integrity. Once data are encrypted, the ciphertext does not have to be protected against disclosure. Further, if ciphertext is modified, it does not decrypt correctly.
    - **Data integrity—**Data integrity is established by cryptographic algorithms that can provide an effective way to determine whether a block of data (for example, email text, message, file, database record) has been altered in an unauthorized manner.
    - **Data signature—**The digital signature, or electronic signature, is the electronic equivalent of a written signature that can be recognized as having the same legal status as a written signature. Furthermore, digital signature algorithms can provide a means of linking a document with a particular person, as is done with a written signature.

- **User authentication—**Cryptography is a powerful authentication tool. Instead of communicating passwords over an open network, authentication can be performed by demonstrating knowledge of a cryptographic key. A one-time password, which is not susceptible to eavesdropping, can be used.

14. Symmetric encryption has the following five ingredients:

    - **Plaintext—**This refers to the original message or data block that is fed into the algorithm as input.
    - **Encryption algorithm—**This performs various substitutions and transformations on the plaintext.
    - **Secret key—**This is one of the main inputs to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
    - **Ciphertext—**This refers to the scrambled message produced as output. It depends on the plaintext and the secret key. For a given data block, two different keys produce two different ciphertexts.
    - **Decryption algorithm—**This is the inverse of the encryption algorithm: It uses the ciphertext and the secret key and produces the original plaintext.

15. A public key encryption scheme has following ingredients:

    - **Plaintext—**This is the readable message or data block that is fed into the algorithm as input.
    - **Encryption algorithm—**This performs various transformations (mainly mathematical operations) on the plaintext.
    - **Public and private key—**This refers to a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.
    - **Ciphertext—**This refers to the scrambled message produced as output. It depends on the plaintext and the secret key. For a given data block, two different keys will produce two different ciphertexts.
    - **Decryption algorithm—**This is inverse of the encryption algorithm: It accepts the ciphertext and the matching key and produces the original plaintext.

16. SP 800-57 classifies key types as follows:

    - **Private and public signature keys—**An asymmetric key pair is used to generate and verify digital signatures.
    - **Symmetric authentication key—**This key is used for message authentication.
    - **Private and public authentication keys—**These keys are used to provide assurance of the identity of an originating entity (that is, source authentication) when establishing an authenticated communication session.

- **Symmetric data encryption key—**This key is used to provide data confidentiality by encryption/decryption.
- **Symmetric key-wrapping key—**This key, also called a key-encryption key, is used to encrypt/decrypt other keys.
- **Symmetric random number generation key—**This key is used with a random number generation algorithm.
- **Symmetric master key—**This key is used to derive other symmetric keys (for example, data-encryption keys or key-wrapping keys) using symmetric cryptographic methods.
- **Private and public key-transport keys—**These keys are used to establish keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors).
- **Symmetric key-agreement key—**This key is used to establish keys (for example, key wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors) using a symmetric key-agreement algorithm.
- **Private and public static key-agreement key—**This is a long-term key pair used to establish keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (for example, initialization vectors).
- **Private and public ephemeral key-agreement key—**This short-term key pair is used only once to establish one or more keys (for example, key-wrapping keys, data-encryption keys, message authentication keys) and, optionally, other keying material (example, initialization vectors).
- **Symmetric authorization key—**This key is used to provide privileges to an entity. The authorization key is known by the entity responsible for monitoring and granting access privileges for authorized entities and by the entity seeking access to resources.
- **Private and public authorization key—**This key is used to provide and verify privileges.

17. You should not use a key for a prolonged period of time because it becomes vulnerable to the following types of error:

    - **Brute-force attacks—**With the increase in raw processing power and parallel computing, a given key length becomes increasingly vulnerable, and longer key lengths are advised. Any shorter keys still in use need to be retired as quickly as possible and longer key lengths employed.
    - **Cryptanalysis—**Over time, flaws discovered in a cryptographic algorithm make it feasible to "break" the algorithm. An example of this is the original NIST standard hash algorithm, SHA-1, which was used in Digital Signature Algorithm. Once the weaknesses were discovered, NIST migrated to SHA-2 and SHA-3.

- **Other security threats—**There are direct as well as indirect methods of attack. This includes attacks on the mechanisms and protocols associated with the keys, key modification, and achieving unauthorized disclosure. The longer a particular key is used for encryption and decryption, the greater the chance that some means of learning the key will succeed.

18. A public key certificate is a set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, called a certification authority, thereby binding the public key to the entity. Public key certificates are designed to provide a solution to the problem of public key distribution.

19. Common architectural components of a PKI system are as follows:

    - **End entity—**This refers to an end user; a device, such as a router or server; a process; or any other item that can be identified in the subject name of a public key certificate.

    - **Certification authority (CA)—**This refers to an authority trusted by one or more users to create and assign public key certificates. Optionally the certification authority may create the subjects' keys. CAs digitally sign public key certificates, which effectively binds the subject name to the public key.

    - **Registration authority—**This optional component can be used to offload many of the administrative functions that a CA ordinarily assumes. The RA is normally associated with the end entity registration process.

    - **Repository—**This denotes any method for storing and retrieving PKI-related information, such as public key certificates and CRLs. A repository can be an X.500-based directory with client access via Lightweight Directory Access Protocol (LDAP).

    - **Relying party—**This refers to any user or agent that relies on the data in a certificate in making decisions.

Chapter 15

1. A technical vulnerability is a hardware, software, or firmware weakness or design deficiency that leaves an information system open to assault, harm, or unauthorized exploitation, either externally or internally, thereby resulting in unacceptable risk of information compromise, information alteration, or service denial. Five key steps are involved in vulnerability management:

    1. **Plan vulnerability management—**This first step in managing technical vulnerabilities involves many things, such as integration with asset inventory, establishment of clear authority to review vulnerabilities, proper risk and process integration, and integration of vulnerabilities with the application/system life cycle.

2. **Discover known vulnerabilities—**This involves monitoring sources of information about known vulnerabilities to hardware, software, and network equipment.
3. **Scan for vulnerabilities—**Apart from regular monitoring, enterprises should regularly scan software, systems, and networks for vulnerabilities and proactively address those that are found.
4. **Log and report—**After the vulnerability scan, the results should be logged to verify the activity of the regular vulnerability scanning tools.
5. **Remediate vulnerabilities—**The enterprise should deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. As a good practice, patches should be applied to all systems.

2. Key sources that are used to discover vulnerabilities are as follows:

   - **National Vulnerability Database (NVDB)** is a comprehensive list of known technical vulnerabilities in systems, hardware, and software.
   - **Computer emergency response team (CERT) or computer emergency readiness team—**Such a team is a cooperative venture that collects information about system vulnerabilities and disseminates it to systems managers. Hackers also routinely read CERT reports. Thus, it is important for system administrators to quickly verify and apply software patches to discovered vulnerabilities. One of the most useful of these teams is the U.S. Computer Emergency Readiness Team, which is a partnership between the Department of Homeland Security and the public and private sectors, intended to coordinate responses to security threats from the Internet. Another excellent resource is the CERT Coordination Center, which grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency.
   - **Packet Storm—**Packet Storm provides around-the-clock information and tools to help mitigate both personal data and fiscal loss on a global scale.
   - **SecurityFocus—**This site maintains two important resources: BugTraq and the SecurityFocus Vulnerability Database. BugTraq is a high-volume, full-disclosure mailing list for detailed discussion and announcement of computer security vulnerabilities. The SecurityFocus Vulnerability Database provides security professionals with up-to-date information on vulnerabilities for all platforms and services.
   - **Internet Storm Center (ISC)—**The ISC (maintained by the SANS Institute) provides a free analysis and warning service to thousands of Internet users and organizations and is actively working with Internet service providers to fight back against the most malicious attackers.

3. An enterprise needs to address two challenges involved in scanning:

   - **Disruptions caused by scanning—**The scanning process can impact performance. IT operations staff need to be in the loop. They should be made aware of the importance and relevance of scans. Also, timing needs to be resolved to ensure that scanning does not conflict with regular maintenance schedules.
   - **Huge amounts of data and numerous false positives—**Technical vulnerability management practices can produce very large data sets. It is important to realize that even though a tool indicates that a vulnerability is present, frequently follow-up evaluations are needed validate these findings.

4. Three types of patch management techniques are commonly used:

   - **Agent-based scanning—**Requires an agent to be running on each host to be patched, with one or more servers managing the patching process and coordinating with the agents. Each agent is responsible for determining what vulnerable software is installed on the host, communicating with the patch management servers, determining what new patches are available for the host, installing those patches, and executing any state changes needed to make the patches take effect.
   - **Agent-less scanning—**Uses one or more servers that perform network scanning of each host to be patched and determine what patches each host needs. Generally, agentless scanning requires that servers have administrative privileges on each host so that they can return more accurate scanning results and so they have the ability to install patches and implement state changes on the hosts.
   - **Passive network monitoring—**Monitors local network traffic to identify applications (and, in some cases, operating systems) that are in need of patching. Unlike the other techniques, this technique identifies vulnerabilities on hosts that don't permit direct administrator access to the operating system, such as some Internet of Things (IoT) devices and other appliances.

5. A security event is any occurrence during which private company data or records may have been exposed. If a security event was proven to have resulted in a data or privacy breach, that event is deemed a security incident. For example, a delay in patching a security weakness in vital company software would be an event. It would only be deemed an incident after the security monitoring team confirms a resulting data breach by hackers who capitalized on the weakness.

6. You should log the following events:

   - **Operating system logs—**This includes successful user logon/logoff; failed user logon; user account change or deletion; service failure; password changes; service started or stopped; and object access denied.

- **Network device logs—**These logs comprise traffic allowed through firewall, traffic blocked by firewalls, bytes transferred, protocol usage, detected attack activity, user account changes, and administrator access.
- **Web servers—**This is about excessive access attempts to nonexistent files, code (SQL, HTML) seen as part of the URL, attempted access to extensions not implement on the server, web service stopped/started/failed messages, failed user authentication; invalid request, and internal server errors.

7. You can do the following analysis on cleaned SEM data:

    - **Pattern matching—**You can look for data patterns within the fields of stored event records. A collection of events with a given pattern may signal a security incident.
    - **Scan detection—**Attacks often begins with scans of IT resources by the attacker, such as port scans, vulnerability scans, or other types of pings. If a substantial number of scans are found from a single source or a small number of sources, this may signal a security incident.
    - **Threshold detection—**You can detect threshold crossing. For example, if the number of occurrences of a type of event exceeds a given threshold in a certain time period, that can constitute an incident.
    - **Event correlation—**Correlation consists of using multiple events from a number of sources to infer that an attack or suspicious activity has occurred. For example, if a particular type of attack proceeds in multiple stages, the separate events that record those multiple activities need to be correlated in order to see the attack. Another aspect of correlation is to correlate particular events with known system vulnerabilities, which results in a high-priority incident.

8. You can categorize threat sources in following manner:

    - **Adversarial—**This type of threat comes from individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources.
    - **Accidental—**This type of threat is spawned by erroneous actions taken by individuals in the course of executing their everyday responsibilities.
    - **Structural—**This type of threat originates from failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters.
    - **Environmental—**This type of threat arises from natural disasters and failures of critical infrastructures on which the organization depends but that are outside the control of the organization.

9. An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there, undetected, for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT

attacks target organizations in sectors with high-value information, such as national defense, manufacturing, and the financial industry. A typical APT attack has the following pattern:

1. Conduct background research to find potential targets
2. Execute the initial attack on the chosen target(s)
3. Establish a foothold in the target environment
4. Enable persistent command and control over compromised computers in the target environment
5. Conduct enterprise reconnaissance to find the servers or storage facilities holding the targeted information
6. Move laterally to new systems to explore their contents and understand to what new parts of the enterprise can be accessed from the new systems
7. Escalate privileges from local user to local administrator to higher levels of privilege in the environment
8. Gather and encrypt data of interest
9. Exfiltrate data from victim systems
10. Maintain persistent presence

10. A variety of technical tools can be used to prevent delivery, such as the following:

    - **Antivirus software (AVS)—**AVS is a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. Continuously running AVS can identify, trap, and destroy incoming known viruses. If a virus is detected, the AVS can be configured to trigger a scan of the rest of the IT infrastructure for indicators of compromise associated with this outbreak.
    - **Firewall—**A firewall can block delivery attempts from known or suspected hostile sources.
    - **Web application firewall (WAF)—**A WAF is a firewall that monitors, filters, or blocks data packets as they travel to and from a web application.
    - **Intrusion prevention system (IPS)—**An IPS is a system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. This is similar to an intrusion detection system but is proactive in attempting to block the intrusion

11. You can counteract exploits by adopting following methods:

    - **Host-based intrusion detection system (HIDS)—**When the exploit is inside the enterprise network and attacking hosts, a HIDS can detect and alert on such an attempt.
    - **Regular patching—**Patching discovered vulnerabilities can contain the damage.
    - **Data restoration from backups—**After an exploit is discovered and removed, it may be necessary to restore a valid copy of data from a backup.

12. ISO 27035-1 lists the following objectives for security incident management:

    - Information security events are detected and dealt with efficiently. This involves deciding when they should be classified as information security incidents.
    - Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.
    - The adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response.
    - A link with relevant elements from crisis management and business continuity management through an escalation process is established.
    - Information security vulnerabilities are assessed and dealt with appropriately to prevent or reduce incidents.
    - Lessons are learned quickly from information security incidents, vulnerabilities, and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

13. Key capabilities of a typical SIEM are as follows:

    - **Data aggregation—**The aggregator serves as a consolidating resource before data is sent to be correlated or retained.
    - **Data normalization—**This is the process of resolving different representations of the same types of data into a similar format in a common database.
    - **Correlation—**Event correlation is the function of linking multiple security events or alerts, typically within a given time window and across multiple systems, to identify anomalous activity that would not be evident from any singular event.
    - **Alerting—**After data that trigger certain responses, such as alerts or potential security problems, are gathered or identified, SIEM tools can activate certain protocols to alert users, such as notifications sent to the dashboard, an automated email, or a text message.
    - **Reporting/compliance—**Protocols in a SIEM can be established to automatically collect data necessary for compliance with company, organizational, and government policies. Both custom reporting and report templates (generally for common regulations such as Payment Card Industry Data Security Standards [PCI DSS] and the U.S. Sarbanes-Oxley Act) are typically part of a SIEM solution.
    - **Forensics—**This is the ability to search log and alert data for indicators of malicious or otherwise anomalous activities is the forensic function of the SIEM. Forensics, which is supported by the event correlation and normalization processes, requires highly customizable and detailed query capabilities and drill-down access to raw log files and archival data.

- **Retention—**This refers to storing data for long periods so that decisions can be made based on more complete data sets.
- **Dashboards—**This refers to the primary interface to analyze and visualize data in an attempt to recognize patterns or target activity or data that does not fit into a normal pattern.

14. ISO 27035 classifies security incidents in the following way:
    - **Emergency—**Severe impact. These are incidents that:
        - Act on especially important information systems and
        - Result in especially serious business loss or
        - Lead to especially important social impact
    - **Critical—**Medium impact. These are incidents that:
        - Act on especially important information systems or important information systems and
        - Result in serious business loss or
        - Lead to important social impact
    - **Warning—**Low impact. These are incidents that:
        - Act on especially important information systems or ordinary information systems and
        - Result in considerable business loss or
        - Lead to considerable social impact
    - **Information—**No impact. These are incidents that:
        - Act on ordinary information systems and
        - Result in minor business loss or no business loss or
        - Lead to minor social impact or no social impact
15. Typical phases in a digital forensics process are as follows:
    1. **Preparation—**This refers to the planning and policy-making activities related to forensic investigation. SP 800-86 recommends the following considerations:
        - Organizations should ensure that their policies contain clear statements addressing all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures.
        - Organizations should create and maintain procedures and guidelines for performing forensic tasks, based on the organization's policies and all applicable laws and regulations.

- Organizations should ensure that their policies and procedures support the reasonable and appropriate use of forensic tools. Organizations should ensure that their IT professionals are prepared to participate in forensic activities.

2. **Identification—**This phase is initiated when there is a request for a forensic analysis. This phase involves understanding the purpose of the request and the scope of the investigation, such as type of case, subjects involved, and system involved. The identification phase determines where the data of interest are stored and what data can be recovered and retrieved.
3. **Collection—**When the location or locations of data are identified, the forensic process ensures that the data are collected in a manner that preserves the integrity of the evidence.
4. **Preservation—**Several actions comprise the preservation of data process, including the following:
    - Creating a log that documents when, from where, how, and by whom data were collected
    - Storing the data in a secure fashion to prevent tampering or contamination
    - Logging each access to the data made for forensic analysis
5. **Analysis—**Examples of analysis tasks include:
    - Checking for changes to the system such as new programs, files, services, and users
    - Looking at running processes and open ports for anomalous behavior
    - Checking for Trojan horse programs and toolkits
    - Checking for other malware
    - Looking for illegal content
    - Looking for indicators of compromise
    - Determining the who, when, where, what, and how details of a security incident
6. **Reporting—**This phase involves publishing a report resulting from a forensic investigation. SP 800-86 lists the following factors that affect reporting for any type of investigation.
    - **Alternative explanations:** The available information may not provide a definitive explanation of the cause and nature of an incident. The analyst should present the best possible conclusions and highlight alternative explanations.
    - **Audience consideration:** An incident requiring law enforcement involvement requires highly detailed reports of all information gathered and can also require copies of all evidentiary data obtained. A system administrator might want to see network traffic and related statistics in great detail. Senior management might simply want a high-level overview of what happened, such as a simplified visual representation of how the attack occurred and what should be done to prevent similar incidents.

- **Actionable information:** Reporting also includes identifying actionable information gained from data that allows an analyst to collect new sources of information. For example, a list of contacts may be developed from the data that can lead to additional information about an incident or a crime. Also, information that is obtained might help prevent future events, such as learning about a backdoor on a system that is to be used for future attacks, a crime that is being planned, a worm scheduled to start spreading at a certain time, or a vulnerability that could be exploited.

Chapter 16

1. Key elements of a security profile are as follows:

   - **Individuals—**Each local environment should have one or more staff members with specific information security responsibilities, as discussed subsequently. The profile should detail the types of users at the location, in terms of their application and data usage, level of security awareness training, security privileges, and whether they use mobile devices and, if so, what type.
   - **Business processes and information—**This area includes the types of information used and whether any sensitive information is accessible. The profile should include descriptions of business processes that involve user information access, as well as descriptions of any external suppliers (for example, cloud service providers).
   - **Technology use—**The profile should provide a description of the location housing the users and equipment. The profile should indicate to what degree the location is accessible to the public or to others who are not part of the organization, whether the physical space is shared with other organizations (for example, an office building or park), and any particular environmental hazards (for example, tornado zone).

2. Key responsibilities of a security coordinator are as follows:

   - Develop the local environment profile.
   - Determine the best way to implement enterprise security policy in the local environment.
   - Provide oversight of implementation of information security policy in the local environment.
   - Ensure that physical security arrangements are in place and adequate.
   - Assist with communicating security policies and requirements to local end users and local management.
   - Keep enterprise security executives and management informed of security-related developments.

- Oversee or coordinate end-user awareness training.
- Coordinate area response to information security risk assessments.
- Coordinate area response to information security risk audit requests as directed.
- Ensure completion and submission of required documentation.

3. The following infrastructure items demand a high level of physical security:
    - **Information system hardware—**This includes data processing and storage equipment, transmission and networking facilities, and offline storage media, as well as supporting documentation.
    - **Physical facility—**This includes buildings and other structures housing the system and network components.
    - **Supporting facilities—**These facilities underpin the operation of the information system. This category includes electrical power, communication services, and environmental controls (heat, humidity, and so on).
    - **Personnel—**This refers to humans involved in the control, maintenance, and use of the information systems.

4. Key environmental threats to physical security are as follows:
    - **Natural disasters—**These are the source of a wide range of environmental threats to data centers, other information processing facilities, and personnel. These are potentially the most catastrophic of physical threats.
    - **Inappropriate temperature/humidity—**Computers and related equipment are designed to operate within a certain temperature range. Most computer systems should be kept between 10 and 32 degrees Celsius (between 50 and 90 degrees Fahrenheit). Outside this range, resources might continue to operate but may produce undesirable results. If the ambient temperature around a computer gets too high, the computer cannot adequately cool itself, and internal components can be damaged.
    - **Fire and smoke—**Fire is a serious threat to human life and property. The threat is not only from direct flame but may also come from heat, release of toxic fumes, water damage from fire suppression, and smoke damage.
    - **Water—**Water and other stored liquids in proximity to computer equipment pose an obvious threat of electrical short-circuit and subsequent fire. Moving water—such as in plumbing and weather-created water from rain, snow, and ice—also poses threats. Another common and catastrophic threat is floodwater.
    - **Chemical, radiological, and biological hazards—**Chemical, radiological, and biological hazards pose a growing threat, both from intentional attack and from accidental discharge. In general, the primary risk of these hazards is to human life. Radiation and chemical agents can also cause damage to electronic equipment.

- **Dust—**Dust is a prevalent threat that is often overlooked. Even fibers from fabric and paper are abrasive and mildly conductive, although generally equipment is resistant to such contaminants. Larger influxes of dust can result from a number of incidents, such as a controlled explosion of a nearby building and a windstorm carrying debris from a wildfire. A more likely source of influx comes from dust surges that originate within the building due to construction or maintenance work.
- **Infestation—**This covers damage from a broad range of living organisms, including mold, insects, and rodents. High-humidity conditions can lead to the growth of mold and mildew, which can be harmful to both personnel and equipment. Insects, particularly those that attack wood and paper, are also a common threat.

5. Power utility problems can be broadly grouped into three categories:

   - **Undervoltage and power outages—**Undervoltage events range from temporary dips in the voltage supply, to brownouts (prolonged undervoltage), to power outages.
   - **Overvoltag**e**—**Overvoltage is bigger threat than undervoltage. A surge of voltage can be caused by a utility company supply anomaly, by some internal (to the building) wiring fault, or by lightning. Damage is a function of intensity and duration, as well as the effectiveness of any surge protectors between IT equipment and the source of the surge.
   - **Noise—**Power lines can also be a conduit for noise. In many cases, spurious signals can endure through the filtering circuitry of the power supply and interfere with signals inside electronic devices, causing logical errors.

   Noise along a power supply line causes electromagnetic interference (EMI). This noise can be transmitted through space as well as through nearby power lines. Another source of EMI is high-intensity emissions from nearby commercial radio stations and microwave relay antennas. Even low-intensity devices, such as cellular telephones, can interfere with sensitive electronic equipment.

6. The following are some of the human-caused physical threats:

   - **Unauthorized physical access—**Information assets such as servers, mainframe computers, network equipment, and storage networks are generally located in a restricted area, with access limited to a small number of employees. Unauthorized physical access can lead to other threats, such as theft, vandalism, or misuse.
   - **Theft—**This threat includes theft of equipment and theft of data by copying. Eavesdropping and wiretapping also fall into this category. Theft can be at the hands of an outsider who has gained unauthorized access or by an insider.
   - **Vandalism—**This threat includes destruction of equipment and data.

7. Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multilayered defense system than to penetrate a single barrier.

Defense in depth is appropriate and effective for physical security. The protective measures could include fences, gates, locked doors, electronic access (such as via smart card), armed guards, surveillance systems, and more. An appropriate first step is drawing a map of the physical facility and identifying the areas and entry points that need different rules of access or levels of security. These areas might have concentric boundaries, such as site perimeter, building perimeter, computer area, computer rooms, and equipment racks. There may also be side-by-side boundaries, such as visitor area, offices, and utility rooms. For concentric boundaries, physical security that provides access control and monitoring at each boundary provides defense in depth.

8. Important measures that are effective in addressing technical threats are as follows:

    - **Brief power interruptions—**It is advised to use an uninterruptible power supply (UPS) for each piece of critical equipment. A UPS is a battery backup unit that can maintain power to processors, monitors, and other equipment for a period of minutes. UPS units can also function as surge protectors, power noise filters, and automatic shutdown devices when the battery runs low.

    - **Longer blackouts or brownouts—**It is advisable to connect critical equipment to an emergency power source, such as a generator. For reliable service, management needs to address a range of issues, including product selection, generator placement, personnel training, and testing and maintenance schedules.

    - **Electromagnetic interference—**The organization should use a combination of filters and shielding. The specific technical details depend on the infrastructure design and the anticipated sources and nature of the interference.

9. An organization can counter human-caused physical threats by adopting following measures:

    - **Unauthorized physical access—**Physical access should be strictly on a need basis. Preventive measures include using locks and other hardware, card entry system, and proximity/touch access systems. Deterrence and response measures include intrusion alarms, sensors, and surveillance systems.

    - **Theft—**The measures to counter unauthorized physical access apply to the threat of theft as well. In addition, an organization should secure objects from being moved by bolting them down. For movable objects, an organization can incorporate a tracking device and provide an automated barrier that triggers an alarm when tagged objects cross the barrier.

    - **Vandalism—**Vandalism may involve environmental threats such as fire or technical threats such as interrupting or surging power, and the corresponding countermeasures apply.

10. The SGP divides the local environment management category into two areas and five topics. These are the areas:

    - **Local environments—**This area deals with security issues in end-user environments and other local environments. It is subdivided into local environment profile and local security coordination topics.
    - **Physical and environmental security—**This area deals with the security of critical facilities against targeted cyber attack, unauthorized physical access, accidental damage, loss of power, fire, and other environmental or natural hazards. It is subdivided into three categories: physical protection, power supplies, and hazard protection.

Chapter 17

1. Business continuity is the ability of an organization to maintain essential functions during and after a disaster has occurred. Business continuity includes three key elements:

    - **Resilience—**Critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions (for example, through the use of redundancy and spare capacity).
    - **Recovery—**Arrangements have to be made to recover or restore critical and less critical business functions that fail for some reason.
    - **Contingency—**The organization must establish a generalized capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen.

2. Natural disasters threats that hamper business continuity are as follows:

    - **Accidental fire—**Sources include wildfires, lightning, wastebasket fires, and short-circuits.
    - **Severe natural event—**This category includes damage resulting from earthquake, hurricane, tornado, or other severe weather, such as extreme heat, cold, humidity, wind, or drought.
    - **Accidental flood—**Flood causes include pipe leakage from air-conditioning equipment, leakage from a water room on the floor above, fire nozzle being open, accidental triggering of sprinkler systems, broken water main, and open window during rainstorm.
    - **Accidental failure of air conditioning—**Failure, shutdown, or inadequacy of the air-conditioning service may cause assets requiring cooling or ventilation to shut down, malfunction, or fail completely.
    - **Electromagnetic radiation—**This can originate from an internal or external device, such as radar, radio antenna, or electricity generating station. This can interfere with proper functioning of equipment or quality of service of wireless transmission and reception.

- **Air contaminants—**This is caused by other disasters that produce a secondary problem by polluting the air for a wide geographic area. Natural disasters such as flooding can also result in significant mold or other contamination after the water has receded.

3. Human-caused disasters that hamper business continuity are as follows:

    - Theft of equipment
    - Deliberate fire
    - Deliberate flood
    - Deliberate loss of power supply
    - Deliberate failure of air conditioning
    - Destruction of equipment or media
    - Unauthorized use of equipment
    - Vandalism

4. Four key business components critical to maintaining business continuity are as follows:

    - **Management—**Management continuity is critical to ensure continuity of essential functions. The organization should have a detailed contingency plan indicating a clear line of succession so that designated backup individuals have the authority needed to maintain continuity when key managers are unavailable.
    - **Staff—**All staff should be trained on how to maintain continuity of operations or restore operations in response to an unexpected disruption. In addition, the organization should develop guidelines for vertical and cross training so that staff can take on functions of peers and those above and below them in the reporting hierarchy, as needed.
    - **ICT systems—**Communication systems and technology should be interoperable, robust, and reliable. An organization should identify critical IT systems and have backup and rollover capabilities tested and in place.
    - **Buildings and equipment—**This component includes the buildings where essential functions are performed. Organizations should have separate backup locations available where management and business process functions can continue during disruptions that in some way disable the primary facility. This component also covers essential equipment and utilities.

5. Key steps of business impact analysis are as follows:

    - Inventory key business elements such as business processes, information systems/applications, assets, personnel, and suppliers.
    - Develop intake forms to gather consistent information. Interview key experts throughout the business. Get information from inventories.

- Assess and prioritize all business functions and processes, including their interdependencies.
- Identify the potential impact of business disruptions resulting from uncontrolled, nonspecific events on the institution's business functions and processes.
- Identify the legal and regulatory requirements for the institution's business functions and processes. For each business process, determine the maximum tolerable downtime (MTD).
- For each business process, determine a reasonable recovery time objective (RTO) and recovery point objective (RPO). The processes with the shortest MTD or RTO are the most critical business processes. Get agreement from senior management.

6. According to ISO 22301, three key areas to be considered while developing business continuity strategy are as follows:
   - **Protecting prioritized activities—**For activities deemed significant for maintaining continuity, the organization should look at the general strategic question of how each activity is carried out. The goal is to determine a strategy that reduces the risk to the activity.
   - **Stabilizing, continuing, resuming, and recovering prioritized activities and their dependencies and supporting resources—**The next step is to provide more detailed options for managing each prioritized activity during the business continuity process.
   - **Mitigating, responding to, and managing impacts—**In this step, the organization should spell out the strategies that attempt to contain the damage to the organization from disasters.
7. The key objectives of a business continuity awareness program are as follows:
   - Establish objectives of the business continuity management (BCM) awareness and training program.
   - Identify functional awareness and training requirements.
   - Identify appropriate internal and external audiences.
   - Develop awareness and training methodology.
   - Identify, acquire, or develop awareness tools.
   - Identify external awareness opportunities.
   - Oversee the delivery of awareness activities.
   - Establish the foundation for evaluating the effectiveness of the program.
   - Communicate the implications of not conforming to BCM requirements.

- Ensure continual improvement of BCM.
- Ensure that personnel are aware of their roles and responsibilities in the BCM program.

8. Business resilience is the ability of an organization to quickly adapt to disruptions while still maintaining continuous business operations and safeguarding people, assets, and overall brand equity. Business resilience has a wider scope than disaster recovery. Business resilience offers post-disaster strategies to avoid costly downtime, to shore up vulnerabilities, and to maintain business operations in the face of additional, unexpected breaches

9. Five sets of organizational continuity controls are as follows:

   - **Business continuity management—**This includes controls that require the organization's business strategies to routinely incorporate business continuity considerations.
   - **Business continuity policy, plans, and procedures—**This requires an organization to have a comprehensive set of documented, current business continuity policies, plans, and procedures that are periodically reviewed and updated.
   - **Test business continuity plan—**This plan incorporates security controls in order to complete a test simulation of the continuity plan to ensure its smooth running if the time comes to implement it.
   - **Sustain business continuity management—**This includes controls that require staff members to understand their security roles and responsibilities. Security awareness, training, and periodic reminders should be provided for all personnel.
   - **Service providers/third parties business continuity management—**This includes security controls that enforce documented, monitored, and enforced procedures for protecting the organization's information when working with external organizations.

10. Some improvement exercises for participants, as mentioned in an ideal BCP, are as follows:

   - **Seminar exercise (or plan walkthrough)—**The participants are divided into groups to discuss specific issues.
   - **Tabletop exercise—**Participants are given specific roles to perform, either as individuals or groups.
   - **Simple exercise—**This task is a planned rehearsal of a possible incident designed to evaluate the organization's capability to manage that incident and to provide an opportunity to improve the organization's future responses and enhance the competence of those involved.
   - **Drill—**A drill consists of a set of coordinated, supervised activities usually employed to exercise a single specific operation, procedure, or function in a single agency.
   - **Simulation—**This is a type of exercise in which a group of players, usually representing a control center or management team, react to a simulated incident notionally happening elsewhere.

- **Live play—**This is an exercise that enables an organization to safely practice the expected response to a real incident.

11. Good business continuity metrics have the following characteristics:

    - Help senior managers (and/or their target audience) quickly see the performance of the response and recovery solutions based on risk to the organization's products and services
    - Convey information that is important to senior managers
    - Focus on performance rather than exclusively on activities
    - Help senior managers identify problem areas to focus attention and remediation efforts

12. In response to a disruptive event, the business continuity process proceeds in three overlapping phases:

    1. **Emergency response—**This phase is focused on arresting or stabilizing an event.
    2. **Crisis management—**This phase is focused on safeguarding the organization.
    3. **Business recovery/restoration—**This phase is focused on fast restoration and recovery of critical business processes.

Chapter 18

1. A security audit is an independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. The key objective of a security audit is to assess the security of the system's physical configuration and environment, software, information handling processes, and user practices.

   A security audit trail is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a security-relevant transaction from inception to final results. Its key objective is to provide a historical record of progression based on a sequence of events to provide proof of compliance and operational integrity.

2. Key elements of the X.816 model for security audit's relationship with security alarms are as follows:

   - **Event discriminator—**This logic embedded into the software of the system monitors system activity and detects security-related events that it has been configured to detect.
   - **Audit recorder—**For each detected event, the event discriminator transmits the information to an audit recorder. The model depicts this transmission as being in the form of a message. The audit could also be done by recording the event in a shared memory area.

- **Alarm processor—**Some of the events detected by the event discriminator are defined to be alarm events. For such events, an alarm is issued to an alarm processor. The alarm processor takes some action based on the alarm events and this action is an auditable event that is recorded in the audit recorder.
- **Security audit trail—**The audit recorder creates a formatted record of each event and stores it in the security audit trail.

3. Some of the auditable items suggested in the X.816 model of security audits and alarms are as follows:
    - Security-related events related to a specific connection, such as connection request/confirmation.
    - Security-related events related to the use of security services, such as security service requests.
    - Security-related events related to management, such as management operations/notifications.
    - Events such as access denials, authentication, and attribute changes.
    - Individual security services such as authentication results, access control results, non-repudiation, and integrity responses.
4. There are four types of audit trails:
    - **System-level audit trail—**This type of audit trail is generally used to monitor and optimize system performance but can serve a security audit function as well. The system enforces certain aspects of security policy, such as access to the system itself. A system-level audit trail should capture data such as login attempts, both successful and unsuccessful, devices used, and operating system functions performed.
    - **Application-level audit trail—**Application-level audit trails may be used to detect security violations in an application or to detect flaws in the application's interaction with the system. For critical applications or those that deal with sensitive data, an application-level audit trail can provide the desired level of detail to assess security threats and impacts.
    - **User-level audit trail—**A user-level audit trail traces the activity of individual users over time. It can be used to hold a user accountable for his or her actions. Such audit trails are also useful as input to an analysis program that attempts to define normal versus anomalous behavior.
    - **Physical access audit trail—**This type of audit trail can be generated by equipment that controls physical access and is then transmitted to a central host for subsequent storage and analysis. Examples include card-key systems and alarm systems.

5. An external security audit is an independent audit of the security aspects of an organization that is carried out by an external party such as an outsider auditor. Its key objectives are as follows:
   - Assess the process of the internal audit.
   - Determine the commonality and frequency of recurrence of various types of security violations.
   - Identify the common causes.
   - Provide advisory and training inputs to tackle the neglect of procedures.
   - Review and update the policy.
6. The SGP defines the security performance function as follows:
   - **Security monitoring and reporting—**This consists of monitoring security performance regularly and reporting to specific audiences, such as executive management.
   - **Information risk reporting—**This consists of producing reports related to information risk and presenting reporting to executive management on a regular basis.
   - **Information security compliance monitoring—**This consists of information security controls derived from regulatory and legal drivers and contracts used to monitor security compliance.
7. NIST IR 7564 defines the following three broad uses of security metrics:
   - **Strategic support—**Assessments of security properties can be used to aid in different kinds of decision making, such as program planning, resource allocation, and product and service selection.
   - **Quality assurance—**Security metrics can be used during the software development life cycle to eliminate vulnerabilities, particularly during code production, by performing functions such as measuring adherence to secure coding standards, identifying likely vulnerabilities, and tracking and analyzing security flaws that are eventually discovered.
   - **Tactical oversight—**Monitoring and reporting of the security status or posture of an IT system can be carried out to determine compliance with security requirements (for example, policies, procedures, regulations), gauge the effectiveness of security controls and manage risk, provide a basis for trend analysis, and identify specific areas for improvement.
8. The three key processes for the COBIT 5 Monitor, Evaluate, and Assess domain are as follows:
   - **Performance and conformance—**Collect, validate, and evaluate business, IT, and process goals and metrics. Monitor to ensure that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.

- **System of internal control—**Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize, and maintain standards for internal control assessment and assurance activities.
- **Compliance with external requirements—**Evaluate whether IT processes and IT-supported business processes are compliant with laws, regulations, and contractual requirements. Obtain assurance that the requirements were identified and complied with and integrate IT compliance with overall enterprise compliance.

9. COBIT 5 defines the following steps for the performance and conformance process:
    1. **Establish a monitoring approach—**Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope, and method for measuring business solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.
    2. **Set performance and conformance targets—**Work with stakeholders to define, periodically review, update, and approve performance and conformance targets within the performance measurement system.
    3. **Collect and process performance and conformance data—**Collect and process timely and accurate data aligned with enterprise approaches.
    4. **Analyze and report performance—**Periodically review and report performance against targets, using a method that provides a succinct all-around view of IT performance and fits within the enterprise monitoring system.
    5. **Ensure the implementation of corrective actions—**Assist stakeholders in identifying, initiating, and tracking corrective actions to address anomalies.
10. SP 800-55 provides the following view of implementing the monitoring and reporting function based on the security performance metrics:
    1. **Prepare for data collection—**This step involves the metrics development process.
    2. **Collect data and analyze results—**The analysis should identify gaps between actual and desired performance, identify reasons for undesired results, and identify areas that require improvement.
    3. **Identify corrective actions—**Based on step 2, determine appropriate corrective actions and prioritize them based on risk mitigation goals.
    4. **Develop business case—**This involves developing a cost model for each corrective action and making a business case for taking that action.
    5. **Obtain resources—**Obtain the needed budget and resource allocation.
    6. **Apply corrective actions—**These actions may include adjustments in management, technical, and operational areas.

11. ISACA's guidance on information risk reporting is based on the following two concepts of COBIT 5:

    - **Process—**This is defined as a collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs, and produces outputs (for example, products, services). Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.

    - **Activity—**This is the main action taken to operate the process. It provides guidance to achieving management practices for successful governance and management of enterprise IT. It involves describing a set of necessary and sufficient action-oriented implementation steps to achieve a governance practice or management practice.

12. The generic steps for security compliance monitoring are as follows:

    1. Identify key stakeholders and/or partners across the organization who regularly deal with institutional compliance issues (for example, legal, risk management, privacy, audit).
    2. Identify key standards, regulations, contractual commitments, and other areas that address specific requirements for security and privacy.
    3. Perform a high-level gap analysis of each compliance requirement that is applicable to determine where progress needs to be made.
    4. Develop a prioritized action plan to help organize remedial efforts.
    5. Develop a compliance policy, standard, roles and responsibilities, and/or procedures in collaboration with other key stakeholders.