RHEMA UNIVERSITY, ABA

COLLEGE OF BASIC & APPLIED SCIENCES
DEPARTMENT OF COMPUTER SCIENCE

COURSE TITLE
SOFTWARE SECURITY, MAINTENANCE & MANAGEMENT

COURSE CODE
RU- SEN 211

(2 CREDIT UNITS)

DR. MRS. P. C. NWOSU

Course Contents

Information Security in the 21st Century with Special Emphasis on Computer Security, Introduction to System Analysis and Design, Information System Security: modularizing requirements specifications: control analysis and control methods, Security Criteria, System Security Testing, vulnerability identification, Threat-Source Identification,

Information Gathering, Information-Gathering Techniques, overview of Information Security as a risk management function, The Role of ICT in fraud: The clearing case, Elevating Information Security to Business Security. Principles of applied information security management, governance and security policy, threat and vulnerability management, incident management, risk assessment and risk management frameworks, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations. 1SO 27000 series and the Plan Do Check Act model assignment of threats and vulnerabilities, incident response, forensics and investigations dealing with classified sensitive data, legal and regulatory drivers and issues, certification, common criteria, security awareness, education and training, and practical considerations when implementing the framework to address current and future threats.

INFORMATION SECURITY

Information security is a collection of technologies, standards, policies, and management practices that are applied to keep information secure. Due to the proliferation of information on the Internet, and despite it helping disseminate information to all and sundry, there is a need to protect said information. It is, therefore, necessary to put in place policies, protective measures, and compliance mechanisms to prevent unauthorized access, abuse, or misuse of personal or sensitive information.

Information is vital to the success of individuals, organizations, and nations; thus, protecting information from unauthorized access, use, disclosure, or destruction is a fundamental requirement to maintain the economic value of this information. It is key to all sectors of the economy and applies to almost all human activities. For organizations to succeed, they need to take effective management decisions based upon secure information.

Most international organizations realize the importance of information security. Governments have also taken it upon themselves to introduce legislation to force organizations to prevent unauthorized access, use, disclosure, or destruction of information. These measures are mostly relatively recent, and the effectiveness of these measures will need to be tested over time, including the ability of the government to enforce the legislation.

The Information Security Triad: Confidentiality, Integrity, Availability (CIA)

The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions. A comprehensive information security strategy includes policies and security controls that minimize threats to these three crucial components.

Confidentiality: Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data—whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

Integrity: Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended. The integrity of data is maintained only if the data is authentic, accurate, and reliable. Information can lose its integrity through malicious intent, such as when someone who is not authorized makes a change to intentionally misrepresent something. An example of this would be when a hacker is hired to go into the university's system and change a grade.

Availability: This means that systems, networks, and applications must be functioning as they should and when they should. Information is useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should. To ensure availability, organizations can use redundant networks, servers, and applications. For example, power outage or network breach could hamper access to critical systems. Availability can also be compromised through deliberate acts of sabotage, such as the use of denial-of-service (DoS) attacks or ransomware.

INFORMATION SECURITY IN THE 21ST CENTURY: WITH SPECIAL EMPHASIS ON COMPUTER SECURITY

The 21st century's information-based society has more and more opportunities to collect and share information with the utilization of ICT tools. Because of the extreme curious nature of human, people want to access and possess all new information immediately. This is supported by the rapid development of information and communication technology, as the Internet is available and accessible at different locations. This advancement has several benefits as well as disadvantages, because the vulnerability of the human-IT system is also increasing. It is a serious problem that the threats are becoming more sophisticated, more difficult to detect and manage, thus both individual, private and corporate organizations, and government are at risk.

Computer Security

Computers and other digital devices have become essential to business and commerce, they have also increasingly become a target for attacks. In order for any organization or an individual to use a computing device with confidence, there should be guarantee that the devices are not compromised in any way and that all communications are secured.

Computer security in concerned with procedures and controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction. It applies to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet. It covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and are of growing importance in line with the increasing reliance on computer systems of most societies worldwide.

Tools for Information Security

In order to ensure the confidentiality, integrity, and availability of information, organizations can choose from a variety of tools. Each of these tools can be utilized as part of an overall information-security policy. They include;

Authentication: Authentication is the process of verifying user's identity to allow access to confidential data or systems. It might involve validating personal identity documents or ensuring that a product or document is not counterfeit. The most common form of authentication today is the user ID and password. A more secure way to authenticate a user is to do multi-factor authentication. By combining two or more of the factors, it becomes much more difficult for someone to misrepresent themselves.

Access Control: Access control determines which users are authorized to read, modify, add, and/or delete information. Several different access control methods, such as Access Control List (ACL). For each information resource that an organization manages, a list of users with the ability to take specific actions can be created. For each user, specific capabilities are assigned, such as read, write, delete, or add. Only users with those capabilities are allowed to perform those functions. If a user is not on the list, they have no ability to even know that the information resource exists.

Encryption: This is the process of transforming information in a way that only authorized parties can decode. During encryption, the original representation of the information known as plain-text is converted into an alternative form known as cipher-text. The encoded text is then decoded (decryption) at the receivers end.

Backup: This is a duplicate copy of computer data and stored elsewhere so that it may be used to restore the original event of data loss event. A good backup plan should consist of several components. Removable storage media such as USB flash drive, external hard drive, cloud storage, etc can be utilizeded . An organization should make a full inventory of all of the information that needs to be backed up and determine the best way back it up.

Hot Sites: Some organizations choose to have an alternate site where an exact replica of their critical data is always kept up to date. When the primary site goes down, the alternate site is immediately brought online so that little or no downtime is experienced. It is recommended for organizations with an extremely heavy reliance on computers.

Firewalls: A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria. It may also be configured to restrict the flow of packets leaving the organization. This may be done to eliminate the possibility of employees watching YouTube videos or using Facebook from a company computer. an organization should use to increase security on its network is a firewall. A firewall can exist as hardware, software or both. A hardware firewall is a device that is connected to the network to filter the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they get to a computer.

Intrusion Detection Systems: Another device that can be placed on the network for security purposes is an intrusion detection system, or IDS. An IDS does not add any additional security; instead, it provides the functionality to identify if the network is being attacked. An IDS can be configured to watch for specific types of activities and then alert security personnel if that activity occurs. An IDS also can log various types of traffic on the network for analysis later. An IDS is an essential part of any good security setup.

Virtual Private Networks: A VPN allows a user who is outside of a corporate network to take a detour around the firewall and access the internal network from the outside. Through a combination of software and security measures, this lets an organization allow limited access to its networks while at the same time ensuring overall security.

Physical Security: Physical security is the protection of the actual hardware and networking components that store and transmit information resources. To implement physical security, an organization must identify all of the vulnerable resources and take measures to ensure that these resources cannot be physically damaged or stolen. These measures include the following.

1. Locking doors: High-value information assets should be secured in a location with limited access. All other security measure becomes meaningless if an intruder can simply walk in and physically remove a computing device.

2. Physical intrusion detection: High-value information assets should be monitored through the use of security cameras and other means to detect unauthorized access to the physical locations where they exist.

3. Environmental monitoring: An organization's servers and other high-value equipment should always be kept in a room that is monitored for temperature, humidity, and airflow. The risk of a server failure rises when these factors go out of a specified range.

4. Employee training: Employees should be trained to secure ICT assets in their possession, especially outside the office. One of the most common ways thieves steal corporate information is to target and steal employee ICT gadgets such as laptops, tablets and mobile phones.

Principles of Information Security

There are five principles of security, they include:

1. Confidentiality: This involves protecting sensitive information so that it is only accessible by authorized individuals. Protection of confidentiality prevents malicious access and accidental disclosure of information. Information that is considered to be confidential is called as sensitive or classified information.

2. Integrity: Involves the accuracy and reliability of data. It ensures that sensitive data is accurate and trustworthy and cannot be created, changed, or deleted without proper authorization.

3. Authentication: Authentication mechanism helps in establishing proof of identification. It is designed to establish validity of transmission of message by verification of individual's identity to receive specific category of information.

4. Non-repudiation: Non-repudiation is a security and legal concept that prevents a party from denying their involvement in a communication or transaction. It provides proof of the origin and integrity of data, and helps to prevent fraud and disputes. It ensures that sender or receiver cannot deny fact that they are part of data transmission.

5. Availability: It means that assets are accessible to authorized parties at appropriate times. It guarantees reliable and constant access to sensitive data only by authorized users. It involves measures to sustain access to data in spite of system failures and sources of interference.

INTRODUCTION TO SYSTEM ANALYSIS AND DESIGN

Systems Analysis a process of collecting and interpreting facts, identifying the problems, and decomposition of a system into its components. System analysis is conducted for the purpose of studying a system or its parts in order to identify its objectives. It is a problem solving technique that improves the system and ensures that all the components of the system work efficiently to accomplish their purpose.

Systems Design on the order hand is a process of planning a new business system or replacing an existing system by defining its components to satisfy the specific requirements. Before planning, the old system is thoroughly analyzed to determine what to incorporate into the new system for better performance. System design focuses on how to accomplish the objective of the system.

System Analysis and Design basically deals with software development activities and guarantees that user requirements and business needs are well represented. It focuses on:

- System: Interdependent components that are integrated to work together in order to achieve a specific goal.
- Process: The activity that transform input into output.
- Technology: The scientific knowledge, principles and methods that are applied to achieve specific goals.

System Development Life Cycle (SDLC)

Systems Development Life Cycle (SDLC) is a standard framework that identifies all the activities required to design and build high-quality software. It generates a structure for designing, creating and delivering quality software based on customer requirements. Its primary goal is to minimize project risks through advance planning to produce high-quality products that are effective and efficient. It involves different phases that comprise a detailed plan that describes how to develop, replace and maintain a system. Each phase builds on the results of the previous one. Adhering to the SDLC enhances development speed and minimizes project risks and costs associated with alternative methods of software development. The phases of SDLC include:

1) **Problem Analysis:** This is involves a detailed analysis of the problem in order to provide a solution. It is important that the problem is clearly identified and stated because the programmer must understand the problem and how to solve it. What is expected of the solution must be clearly understood, i.e. the nature of the output and the input to consider so as get the output. It is also important to understand the ways of solving the problem and the relationship between the input and the expected output.

2) **Design:** This stage of system development involves building a model of the system; it is an essential precursor to the actual development. It is involves extensive prototyping, it is sometimes referred to as logical design. It is common to use design tools such as UML diagrams, data flow diagram, flowchart, pseudo code, etc to depict the system design, these

tools help to ensure that best practices are rigorously adhered to. It produces a logical design of the system.

3) **Implementation/Coding:** This is the stage where the design is translated into code using programming languages. This involves writing instructions for the system, which is the program that carry out tasks, equally referred to as **coding.** The programs coordinate the data movements and control the entire process in a system. Developers choose the right programming language based on the project specifications and requirements.

4) **Testing and Debugging:** This involves running the program to identify and remove likely bugs. The functionality of the entire system is tested to ascertain that the system works according to user requirements specified in the design. This process continues until the software is stable, bug-free and working according to the business requirements of the system.

5) **Deployment:** At this stage, the new system is integrated into its environment and installed in the actual machines that they are intended to be used. It entails installation of the new system, in addition to all the hardware and software required to operate the system. It also involves training the users of the system, file conversion and employing appropriate change over method to ensure that the new system meets user's expectations.

6) **Maintenance:** Maintenance starts during the effective use of a new system by end-users. Obtaining feedback from end-users guarantees that likely issues are highlighted and taken care of. It involves modifications of the system after release to better match the needs of users by providing updates. Features could be added or modified to guarantee better performance and increased efficiency of the new system.

CONTROL ANALYSIS

Control analysis refers to the process of evaluating the effectiveness of current and planned controls in order to assess the likelihood of a vulnerability being exploited by a threat source. It is the foundational to assessing threats and risk to an enterprise. It helps to avoid, detect, counteract or minimize security risks to physical properties, information, computer systems or other assets. It is impossible to prevent all threats, control seeks to decrease the risk by reducing the chances that a threat will exploit a vulnerability.

It also helps to determines if the controls are implemented correctly, operating as intended, producing the desired outcome, and meeting the security requirements for the system. Control analysis is a compliance tool, that is used to test control requirements to guarantee security.

Classification of Security Controls

1. Technical Security Controls: This is also known as logic controls; it employs various technological solutions to protect sensitive information and systems from unauthorized access, security breaches, and other potential threats. It involves hardware, software, or firmware components that protect the system against threats and vulnerability. Automated software tools are installed and configured to protect these assets. Examples of technical controls include:

- Encryption
- Antivirus and Anti-Malware Software
- Firewalls

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Identification and authentication mechanisms

2. Administrative Security Controls: Administrative security controls refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organization’s security goals. An organization may have an acceptable policy that specifies the conduct of users, including not visiting malicious websites. The security control to monitor and enforce could be in the form of a web content filter, which can enforce the policy and log simultaneously. Users are instructed to review and acknowledge the security policy of an organization and by acknowledging the policies as a new user/hire, there is an obligation to adhere to the corporate policy of the organization.

3. **Physical Security Controls:** Physical controls are the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. Examples of physical controls are:

- Closed-circuit surveillance cameras
- Motion or thermal alarm systems
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors
- Biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods used to recognize individuals)

Security Criteria

Security criteria are rules with a set of security properties that can be used to assess a security function or security objective. They are constraints that a system, application, or process must meet to ensure the protection of its data, resources, and users. These requirements are typically defined during the early stages of the software development life cycle and are integral to the design, development, and operation of secure systems. It tests whether a security function has desired security properties.

Security requirements can vary depending on the nature of the system and the sensitivity of the data it handles. However, their primary goal is to mitigate risks and vulnerabilities that could lead to unauthorized access, data breaches, or other security incidents.

Security Testing

Security testing is an important aspect of software testing that is focused on identifying and addressing security vulnerabilities in a software application. It aims to ensure that the software is secure from malicious attacks, unauthorized access, and data breaches. Security testing involves verifying the software's compliance with security standards, evaluating the security features and mechanisms, and conducting penetration tests to identify weaknesses and vulnerabilities that might be exploited by malicious actors.

The goal of security testing is to identify security risks and offer recommendations for remediation to improve the overall security of the software application. Testers simulate attacks to check existing security mechanisms and look for new vulnerabilities.

Types of Security Testing

- **Vulnerability Scanning:** This test scans a system or network assets, such as servers, routers, and endpoints, to find potential security vulnerabilities. It is a crucial first step in securing a network. Before implementing a countermeasure or control, it is usually performed to ensure the security feature is implemented to address the vulnerability. A vulnerability scan seeks for any missing security patches, weak passwords in the system, malware and report the potential exposure of treasure box when it is scanning. This type of Scanning is automated and can also be scheduled weekly, monthly, quarterly depending on the organization.

- **Penetration Testing:** This is a type of security testing that attempts to find and exploit potential vulnerabilities in the system. This practice tests for any possible threats by simulating an attack from a malicious hacker. The purpose of a penetration test is not just to see whether or not specific vulnerabilities exist within a system but also to determine the level of risk posed by these vulnerabilities. Therefore, a penetration test performed by security professionals should reveal all the potential risks and offer mitigation strategies against such threats.

- **Network Security Testing:** Network security testing is a critical component of a comprehensive information security program. It is a broad means of testing network security controls across a network to identify and demonstrate vulnerabilities and determine risks. The testing medium can vary like wireless, IoT, ethernet, hardware, phishing emails, etc.

- **API Testing:** Since IT industry has shifted towards the cloud, there is an increased use of Application Programming Interface (API) targeting the cloud, bringing new risks for organizations. These risks to API include improper configuration, exploitation of authentication mechanisms, and API misuse to launch attacks. API security testing performs numerous functions that help identify any irregularity in an API. API also covers network security services. They aid in assisting developers in finding vulnerabilities to resolve the existing loopholes. The interfaces provide access to valuable and sensitive data that hackers can use to their absolute advantage.

- **Security Auditing:** Security audit is an in-depth look at the information security defenses of an organization. For example, a company performing a security audit will protect information from hacking and its systems from malicious code. Audits can be done regularly to ensure security flaws are easily identified and eliminated. Audits act as a standard that organizations can use to validate their security policies and procedures held for the company. Companies will conduct a security audit that will encompass whether or not they have the proper security in place, ensuring they are compliant with the industry standards.

- **Posture Assessment:** A security posture assessment is a method used to analyze the current state of an organization’s security controls. The evaluation can also help identify existing risk areas and recommend changes or improvements that will improve the overall security of protected assets. Posture assessments vary in scope and depth and is usually performed by external security or IT professionals.

- **Risk Assessments:** Risk Assessment is a technique used to identify and prioritize potential risks to an organization or project. Risk assessment is performed by identifying threats that could affect the project's success. By performing a risk assessment for an operation, techniques such as threat modeling can be used to determine the capabilities of a threat to exploit weaknesses in the environment. This information can then be used to prevent against the most likely threats or accept residual risk from less likely ones. It is a best practice to perform this assessment regularly because risk continues to emerge, change, and recede.

- **Ethical Hacking:** Ethical hacking is critical since it's impossible to find all the vulnerabilities within a system through technical or manual testing alone. It is vital to have a fresh pair of eyes review a system before it goes live, and hackers are a good bet to exploit any weakness they discover. Unlike malicious hacking, ethical hacking does not try to damage or destroy anything, and hence it is often known as white hat hacking. Ethical hackers specifically hack into computer systems to expose flaws, not steal, or expose data.

Vulnerability Identification

Vulnerability is a flaw or weakness in a system's design, implementation, or operation that can be exploited to violate the system's security policy. It weakens systems and opens the door to malicious attacks. These can take various forms, such as buffer overflow, unpatched and outdated software, wrong system configurations, etc.

Vulnerability identification is vital to proactively protect IT system rather than actively cleaning up after an attack. The vulnerability identification process enables identification and understanding the weaknesses in the system, underlying infrastructure, support systems, and major applications. The main goal of vulnerability identification is to discover and address potential security gaps before they can be exploited by attackers, ultimately improving the overall security and resilience of the system.

Vulnerability Testing Methods

Vulnerability testing methods can be broadly categorized based on the approach taken to identify vulnerabilities; they are:

a) **Active testing:** This is a vulnerability testing method in which testers interact directly with the target system, network, or application to identify potential security weaknesses. It typically involves sending inputs, requests, or packets to the target and analyzing the responses to discover vulnerabilities. Active testing can be intrusive and may cause disruptions or performance issues in the target system, but it is usually more effective in finding vulnerabilities than passive testing. Examples of active testing include:

   - Port scanning to identify open ports and services running on a network.
   - Fuzz testing, which involves sending malformed or unexpected inputs to applications to discover vulnerabilities related to input validation and error handling.

b) **Passive Testing:** Passive testing is a non-intrusive vulnerability testing method that involves observing and analyzing the target system, network, or application without directly interacting with it. Passive testing focuses on gathering information about the target, such as network traffic, configuration settings, or application behavior, to identify potential vulnerabilities. This method is less likely to cause disruptions or performance issues but may be less effective in finding vulnerabilities compared to active testing. Examples of passive testing include:

- Traffic monitoring to identify patterns or anomalies that may indicate security weaknesses.
- Configuration reviews to assess security settings and identify improper configurations.

c) **Network Testing:** Network testing is a vulnerability testing method focused on identifying security weaknesses in network infrastructure, including devices, protocols, and configurations. It aims to discover vulnerabilities that could allow unauthorized access, eavesdropping, or Denial of Service (DoS) attacks on the network. Network testing typically involves both active and passive testing techniques to evaluate the network's security posture comprehensively. Examples of network testing include:

- Scanning for open ports and services on network devices.
- Analyzing network protocols and configurations for security flaws.

d) **Distributed Testing:** Distributed testing is a vulnerability testing method that involves using multiple testing tools or systems, often deployed across different locations, to scan and analyze the target system, network, or application for vulnerabilities. This approach can help provide a more comprehensive view of the target's security posture, as it helps identify vulnerabilities that may be visible only from specific locations or under specific conditions. Distributed testing can also help distribute the load of vulnerability testing, reducing the impact on the target system and increasing the efficiency of the testing process. Examples of distributed testing include:

- Using multiple vulnerability scanners from different locations to scan a web application for potential security flaws.
- Coordinating a team of testers in different geographical locations to perform simultaneous network vulnerability testing.

Possible Causes of Vulnerabilities

1. Human error: When end users fall victim to phishing and other social engineering tactics, they become one of the biggest causes of vulnerabilities in security.

2. Software bugs: These are flaws in a code that cyber criminals can use to gain unauthorized access to hardware, software, data, or other assets in an organization's network/ They can access sensitive data and perform unauthorized actions, which are considered unethical or illegal.

3. System complexity: When a system is too complex, it causes vulnerability because there is an increased likelihood of improper configurations, flaws, or unwanted network access.

4. Increased connectivity: Having so many remote devices connected to a network creates new access points for attacks.

5. Poor access control: improperly managing user roles, like providing some users more access than they need to data and systems or not closing accounts for old employees, makes networks vulnerable from both inside and outside breaches.

Threats

A threat is any action or event that has the potential to adversely impact individuals or organizational operations or assets that could result in destruction, disclosure or unauthorized modification of information, etc.

Threat Sources

It is important to recognize that threat sources are not static and that they can evolve over time, as technology advances and new vulnerabilities emerge, threat actors may adapt their tactics to exploit these weaknesses. By conducting regular threat assessments and staying informed about emerging trends in system security, you can stay one step ahead of potential attackers and strengthen your organization's security posture. Threat sources can be broadly categorized into adversarial and non-adversarial sources.

- Adversarial threats are intentional and malicious in nature, originating from individuals or groups with ill-intent. Adversarial threat sources tend to exhibit distinct traits that differentiate them from non-adversarial threats. They are deliberate, opportunistic, and highly skilled. Adversarial threats can exploit vulnerabilities in systems and networks, causing harm to an organization and its stakeholders. The craftiness of adversarial threat actors lies in their ability to adapt and evolve their tactics, often staying one step ahead of conventional security measures.

- Non-adversarial threats are unintentional, typically arising from human errors, faulty systems, or natural disasters. Non-adversarial threats, while not intentional, can still result in significant damages due to their unpredictable nature. These threats can include system failures, natural disasters, or even unintentional actions by individuals.

Different Kinds of Threats

- Malware: These are malicious software created to infect and cause damage to computer system without the user's knowledge or permission, such as viruses and worms.
- Natural Disasters: Fire, flood, earthquake, lightning, rain, hurricane, tornadoes, etc.
- Human error: This involve things like accidents, employee mistakes, failure to follow policies, etc.
- Information Theft: This involves the use of another person's identity, like name, identification number, or credit card number, etc without their knowledge to commit fraud or other crimes.
- Sabotage or vandalism: Physical damage or destruction of systems or information system assets.
- Technical failure: Hardware and software issues such as errors or bugs, code problems, loopholes, backdoor, using outdated software/technologies.
- Software Piracy: This is the use of software without proper license. That might include copying, modifying, distributing or selling the software in ways that contravene copyright laws or license terms.

- Espionage: This is the act spying or using spies to obtain secret or confidential information of organization or government. It can be carried out by insiders with access to this kind of information.

INFORMATION GATHERING

Information gathering extends beyond mere data collection. It is a systematic process that involves acquiring, arranging, and evaluating data, facts, and knowledge from diverse sources using sophisticated information gathering tools. By gathering information, organizations and individuals can better understand the environment in which they operate, identify potential risks, develop strategies, and make informed decisions.

Information Gathering Techniques

There are various methods of data collection; choice of the method depends on the type of system involved; the most common methods include:

- Interview
- Observation
- Questionnaire
- Online Survey

1. Interview

Interview is a planned meeting during which information can be obtained from another person. It is a structured conversation where one participant asks questions, and the other provides answers. The analyst should have the basic skills needed to plan, conduct and document interviews successfully. It is the most common method for data collections /facts gathering. Interviewing the prospective users can provide the valuable accurate information about a system. The system analyst can interview any personnel in an organization and should create the environment for interview setting time for whom, when, and about what.

Tips for a Successful Interview

i. Be punctual. This often means 10-15 minutes early. Interviewers are often ready before the scheduled time.
ii. Have the questions prepared in advance.
iii. Have a reliable instrument for recording.
iv. Be formal and stay focused.

2. Observation

With this method, the analyst visits the organization to personally observe and understand the flow of documents, working of the existing system, the users of the system etc. Sometimes a system can be better understood by just observing its operation. Seeing the system in action could provide additional perspective and a better understanding of the system and its procedures. Personal observation also allows an analyst to verify responds obtain using questionnaires and interviews and determine whether the procedures really correspond to what was obtained; so, it could serve as an additional measure to obtain more insight. Through observation, the accuracy of information obtained from questionnaires and interview could be validated.

Personal observation also can provide important advantages in later SDLC phases. For example, recommendations often are better accepted when they are based on personal observation of actual operations. Observations also can provide the knowledge needed to test or install future changes and can help build relationships with the prospective users of the system. Observing the employees working in the organization with the present situation of the system and its environment is very useful in data collection. It should be planned in advance by preparing a checklist of specific tasks to be observed and likely questions that could be asked. The following issues should be considered when preparing a list:

i. Ask sufficient questions to ensure a complete understanding of the present system operation is established. A primary goal is to identify the methods of handling situations that are not covered by standard operating procedures.
ii. Observe all the steps in a processing cycle and note the output from each step.
iii. Examine each pertinent form, record, and report. Determine the purpose each item of information serves.
iv. Consider each person who works with the system and ask the following questions: what information is received from other people? What information is generated by this person's work? What tools are used in the process?
v. Talk to the people who receive current reports to ensure that the reports are complete, timely, accurate, and in a useful form.

3. Questionnaires

Questionnaire is a document containing a number of standard questions that could be administered to many individuals. It can be a valuable tool in a system development project; it is usually employed to obtain information from a large number of people. A typical questionnaire starts with a heading, which includes a title, a brief statement of purpose, the name and the telephone number of the contact person, the deadline date for completion, and how and where to return the form, and then the questions and possible options to select from.

General instructions are provided to guide the respondents on how to answer the questions. When designing a questionnaire, the most important rule is to make sure that the questions return the right data in a form that it can be use to advance fact-finding. Listed are some additional ideas to keep in mind when designing questionnaires:

a) Keep the questionnaire brief and user-friendly.
b) Provide clear instructions that will help answer all anticipated questions.
c) Arrange the questions in a logical order, going from easy to more complex topics.
d) Phrase questions to avoid misunderstandings; use simple terms and words.
e) Try not to lead the response or use questions that give clues to expected answers.
f) Limit the use of open-ended questions that will be difficult to tabulate.
g) Limit the use of questions that can raise concerns about job security or other negative issues.
h) Include a section at the end of the questionnaire for general comments.
i) Test the questionnaire whenever possible on a small group before finalizing it.

4. Online survey

Online survey is one of the most popular data-collection sources, where a set of survey questions are sent out to a target sample, and the members of this sample can respond to the right questions through digital platforms. It is sometimes also referred to as online poll. Respondents can receive surveys via various mediums such as email, embedded in websites, social media, application etc. It enables gathering information from a wider audience or respondents. It also allows data analysis to be performed easily and quickly.

Respondents have more anonymity with online surveys so they provide more valid and candid answers. They are also more likely to give honest and open answers which provide more accurate data. The same approaches used in the aforementioned methods can still be applied in online survey; the only difference is that online survey is carried out on the internet platform using digital devices and network.

OVERVIEW OF INFORMATION SECURITY AS A RISK MANAGEMENT FUNCTION

Risk can be defined as the chance of loss or an unfavorable outcome associated with an action. Risk management is the process of identifying, assessing and controlling threats that could stem from wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents, malicious attacks, or natural disasters.

Information security risk management (ISRM) is the process of managing risks associated with the use of information technology. It is a fundamental part of any successful security strategy that involves identifying, assessing, and addressing risks to the confidentiality, integrity, and availability of an organization's information systems. Its main goal is to treat risks in accordance with an organization’s overall risk tolerance. It is not possible to eliminate all risks in business; rather, organizations seek to identify and achieve an acceptable risk level.

Types of Risks

Information security risks come in many shapes and forms. In one way or another, they compromise the confidentiality, integrity, and availability of organization's information assets. Listed are some common examples:

- Strategic Risks: These are risks that arise from an organization’s business strategy and objectives. For example, entering a new market or launching a new product may have strategic risks associated with them.
- Operational Risks: These are risks that arise from an organization’s day-to-day activities and processes. Examples include technology failures, employee errors or supply chain disruptions.
- Financial Risks: These are risks that arise from an organization’s financial operations and management. Examples include credit risk, market risk and liquidity risk.
- Legal/Compliance Risks: These are risks that arise from an organization’s failure to comply with laws, regulations or industry standards. Examples include contract disputes, intellectual property disputes, employment law violations, data privacy violations or non-compliance with environmental regulations.

- Reputational Risks: These are risks that arise from damage to an organization’s reputation, image or brand. Examples include product recalls, lawsuits or negative media coverage.

Stages of Information Security Risk Management

The stages of Information Security Risk Management (ISRM) require a systematic approach to addressing security risks within your organization. These stages typically include:

- Risk identification
- Risk assessments
- Risk management strategy
- Risk communication strategy
- Continuous improvement cycles

1. **Risk identification:** Risk Identification is the first phase in Information Security Risk Management (ISRM), where potential threats and vulnerabilities to organization's information systems are identified and documented. It requires conducting comprehensive assessments to identify areas of concern. It should focus on core areas such as:

- Assets: These include physical equipment like servers, laptops, and mobile devices and digital assets like data, software, and intellectual property.
- Threats: Threats are actors or events that could exploit vulnerabilities and destroy assets.
- Vulnerabilities: Vulnerabilities are weaknesses present in assets that threats could exploit. Vulnerabilities can be technical (software bugs, security configuration flaws) or procedural (no strong password policy, lack of training).
- Controls: These are the measures that organizations implement to mitigate risks. They can be preventive, like firewalls, or detective, like security monitoring and log reviews.

2. **Risk assessment:** Risk Assessments are essential components of the ISRM process that involves the evaluation of potential risks, vulnerabilities, and impacts on organization's information assets. These assessments play a key role in prioritizing security measures and controls for organization's protection. It involves identifying the likelihood and impact of each risk. Likelihood is the probability of the risk occurring, while impact is the severity of the consequences if it does occur. Based on the likelihood and impact, the risks are prioritized. All risks are not equal, some are more likely to happen and have a greater impact. Prioritize risks helps to focus resources on mitigating the most critical.

3. **Risk management strategy:** Developing a risk management strategy entails creating plans and implementing actions to mitigate identified security risks efficiently. It is designed to establish protocols for risk treatment and response. Some risk treatment strategies are:

- Remediation: Remediation involves eliminating the underlying vulnerability that is creating the risk; for examples, patching a software vulnerability or implementing a new security control.

- Mitigation: Mitigation is the most common risk response approach that involves assessing all possible solutions, devising a plan, taking action, and monitoring the results. It reduces the likelihood or impact of a risk.

- Acceptance: Acceptance involves making a conscious decision to accept the risk. This strategy may be appropriate for risks that are low in likelihood or impact or for risks that are too costly or difficult to mitigate.
- Avoidance: Eliminating the risk by changing processes, technologies, or practices. For instance, discontinuing the use of a vulnerable software application.
- Transference: Transference involves transferring the risk to another party. Some risks may be challenging that an organization may not be able to avoid, accept, or mitigate them. Such situation may require outsourcing or transferring the risk to another party; for example, an insurance company. which may reimburse organizations for certain realized risks.

4. **Risk Communication Strategy:** Risk communication strategy encompasses the distribution of risk-related information to stakeholders and decision-makers within an organization. This strategy is essential for maintaining transparent and effective communication regarding security risks and the corresponding mitigation efforts.

Continuous Improvement Cycle: Risk management is not a one-off task, it is an ongoing process that needs to adapt and evolve over time. Continuous improvement cycle emphasizes the iterative nature of the risk management process. It requires continuous monitoring, evaluation, and enhancement of security measures to adapt to the evolving landscape of threats and vulnerabilities effectively.

THE ROLE OF ICT IN FRAUD

Fraud is an intentional act of deceit designed to reward the perpetrator or to deny the rights of a victim, it is usually target at individuals, businesses or government. It results to substantial monetary losses and can have damaging effects on an organization's reputation, placing at risk the ability to operate effectively, establish partnerships and receive contributions. Effective fraud prevention, detection and response mechanisms, therefore, play a key role in safeguarding organizations' interests against these negative impacts. Anti-fraud measures play an equally important role in enhancing the accountability and effectiveness of the information system and in promoting appropriate oversight and the responsible use of resources. Fraud is a menace that deserves serious attention and immediate action by both the individuals, organizations and government.

Adoption of Information and communications technology (ICT) seems to have increase the chances of fraud due to the fact that most activities that were carried out ordinary currently rely upon online and real time. The levels of staff wages are also a motivation for fraud from the employee side.

Some ICT Related Frauds

- Forgery: This is a white-collar crime that generally consists of the false making or material alteration of a legal instrument with the specific intent to defraud. Tampering with a certain legal instrument may be forbidden by law in some jurisdictions but such an offense is not related to forgery unless the tampered legal instrument was actually used in the course of the crime to defraud another person or entity. Copies, studio replicas, and reproductions are not considered forgeries, though they may later become forgeries through knowing and willful misrepresentations.

- Identity Theft: Identity theft is the use of an individual's personal or financial information to carry out fraud in that person's name. Identity theft has ballooned in recent years because there are so many ways to steal information beyond straightforward pick-pocketing. Most are digital methods like installing skimmers at ATMs, pirating users of public Wi-Fi, or phishing for information from unwary consumers.
- Sextortion: This is a crime that involves coercing victims into sending explicit images online, which is used to exploit the victim. It employs non-physical forms of coercion to extort sexual favors from the victim. It refers to the broad category of sexual exploitation in which the means of coercion exploitation is threat to release sexual images or information.
- Ransomware: This fraud utilizes malware that encrypts the victim's personal data or system and denies the owner access until a ransom is paid. They commonly use difficult-to-trace digital currencies such as Bitcoin, making tracing and prosecuting the perpetrators difficult. Ransomware attacks have become prominent and visible, recent attacks have impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations.
- Racketeering: This refers to a type of organized crime in which the perpetrators set up a coercive, fraudulent, or otherwise illegal coordinated scheme or operation (known as a "racket") to repeatedly or consistently collect a profit. Usually, the perpetrators offer a service that will not be put into effect, offer a service to solve a non-existent problem, or offer a service that solves a problem that would not exist without the racket.

Fraud Control Methods

Fraud investigations become increasingly complex, stretched teams are seeking the help from advancements in technology, with automation and machine learning being incorporated into everyday processes and tasks. Fraudsters develop more sophisticated tactics, with increased volume of fraudulent activity. Automation is easily scaled to handle this growing workload, ensuring that investigators are not overwhelmed. ICT plays a major role in minimizing the risk of human error and inconsistencies in fraud management. Automated tools follow predefined rules and algorithms consistently, this consistency can be crucial in maintaining the integrity of the investigation. Some fraud control measures include:

1. Prevention Controls: Prevention fraud controls are the most common and cost effective way to stop fraud. They prevent or limit the size of the fraud risk by reducing the occurrence or impact of fraud. They include:

i. Disciplinary Measures and Sanctions: Determination and will on the part of management are necessary to follow up on investigation reports and take action to punish fraud perpetrators, internally and externally. Without the effective enforcement of a sanctions, there cannot be an effective anti-fraud programme. This should include disciplinary measures for internal staff and debarment for external parties. While policies to pursue disciplinary measures appear to be in place, most organizations weigh the legal risks heavily when deciding if and what disciplinary measures should be imposed.

ii. Performance Reporting and Feedback: Management and legislative bodies are deprived of accurate and readily available information on the status of fraud in organizations, and this hinders accountability and informed decision-making. This emphasizes the importance of collecting, verifying and collating information relating to fraud in a thorough and systematic manner from the corporate levels, regional and other field presences. It also recommended that the task of fraud disclosure and reporting should not be left only to reports by the internal oversight bodies or be unceremoniously hidden in the pages of financial statements that are presented to external auditors. Rather, the executive heads of organizations should provide annually comprehensive management reports to their legislative and governing bodies on the overall state of affairs in regard to fraud. Proper documentation of agendas or standing item relating to fraud is imperative as well as implementation of the anti-fraud activities and providing guidance and oversight on fraud related matters.

2. Detective Controls: Detection fraud controls can help identify when fraud has occurred, disrupt additional fraud and reduce the consequences. Detection fraud controls are not as cost effective as prevention fraud controls. However, if detected early, the impact of fraud can be significantly reduced. It could be achieved using some of these methods:

i. Predictive Analytics: Predictive analytics is a powerful and dynamic concept which uses historical data to forecast future fraudulent activities. This stronghold in the digital defence arena relies on the insightful power of machine learning algorithms to identify and thwart common types of fraud.

ii. Behavioral Analytics: This emphasizes the critical significance of understanding user behaviour patterns. It involves establishing a baseline for 'normal' user activity to keenly identify irregularities that may signal potential fraud. This method, powered by machine learning algorithms, plays a pivotal role not only in preventing identity theft but also in detecting and responding to suspicious activities in real-time.

iii. Complaint Mechanisms: Comprehensive whistle-blower policies are key to an effective anti-fraud programme. Whistle-blowing is an act of a person, often an insider, revealing information about activity within a private or public organization that is deemed illegal, immoral, illicit, unsafe or fraudulent. Research has discovered that whistle-blowers alone account for the uncovering of more fraud and corruption than all other measures of fraud detection combined. There is a need to consolidate, clarify, and make readily available basic information on whistle-blower policies to staff and third parties. Organizations that already have a whistle-blower policy should adopt good practice benchmarks that relate among others to the duty to report fraud and misconduct, and require fraud reporting by third parties including vendors, suppliers and implementing parties.

iv. Investigation: This involves the study of facts that are used to inform criminal trials. A complete criminal investigation can involves searching, interviews, interrogations, evidence collection and preservation, etc. Modern-day criminal investigations commonly employ many modern scientific techniques known collectively as forensic science. Because of the protracted process and the challenges that most organizations are facing in pursuing perpetrators effectively, there is a perceived sense of impunity among fraud perpetrators within the organizations. This may result in perpetrators not being deterred from committing fraud and staff being unwilling to report fraud.

v. Verification and Authentication: Comprehensive identity verification and authentication are the fortress against the looming threat of identity theft in today's digital landscape. In an era where identity theft poses significant fraud risks, robust ID verification with advanced features become indispensable layer of defense.

vi. Real-time transaction monitoring: Real-time transaction monitoring is a dynamic method that scrutinizes transactions as they unfold, playing a pivotal role in promptly detecting fraudulent activities. This proactive approach is the digital guardian that prevents potential financial loss by swiftly identifying and flagging contentious transactions for review.

vii. Advanced fraud detection using ML and AI: This is the frontier of fraud detection, in the ongoing battle against fraud, ML and AI stand as game-changers, armed with adaptive capabilities and the capacity to learn from ever-evolving fraud patterns. These technological marvels are not just effective; they redefine the landscape of fraud prevention and detection.

3. Corrective Controls: Corrective fraud controls respond to fraud after it has occurred to help reduce or disrupt additional consequences. They are not as cost effective as prevention or detection fraud controls. However, the impacts of fraud can be significantly reduced (if implemented effectively).

Challenges of Fraud Prevention and Detection Systems

Like any organizational process, there are implementation challenges and considerations. These can include the following:

- Fraudster techniques are ever-evolving as they get more creative to work around heightened security measures. There is no one-size-fits-all approach to fraud detection, this means that efforts to prevent and detect suspicious behaviour also need to change.
- While data collection is essential to mitigate fraud, too much can become cumbersome to handle. For example, aggressive ID verification every time someone logs in may backfire on you.
- False positives can lead to frustrations and lower customer experience and satisfaction. False positives include declining a genuine purchase, locking out a user from their account, or flagging suspicion where there is none.
- A stringent fraud detection protocol can slow down access to services and drive customers towards competitors.

ETHICS OF INFORMATION COMMUNICATION TECHNOLOGY

Ethics are moral standards that help guide behaviour, actions, and choices. Ethics are grounded in the notion of responsibility (as free moral agents, individuals, organizations, and societies are responsible for the actions that they take) and accountability (individuals, organizations, and society should be held accountable to others for the consequences of their actions). In most societies, a system of laws codifies the most significant ethical standards and provides a mechanism for holding people, organizations, and even governments accountable.

In a world where information and communication technology has come to define how people live and work, and has critically affected culture and values. Issues bothering around how well trained and ethical ICT professionals are in dispensing their duties should not be ignored. Faulty and useless systems that cause disasters and hardships to users might be built by incompetent ICT professionals if unchecked. In dispensing their duties ICT professionals must demonstrate best practices and standards as set by professional bodies for quality assurance.

ICT Ethical Frameworks

Analyzing and evaluating the impact of ICT can be very difficult. ICT does not only involve technological aspects, but also epistemology since the main component of ICT is information which represents data, information, and knowledge. Some of the impact and changes of ICT are obvious, but many are subtle. Benefits and costs need to be studied closely for a nation to progress and improve the quality of life for its citizens.

Ethics in ICT encompasses a wide array of principles that guide the responsible development, use, and impact of technology on individuals and society. It involves a commitment to fairness, accountability, transparency, and respect for the privacy and rights of users. The rapid pace of technological advancements demands a proactive approach in establishing ethical frameworks that can adapt to emerging challenges. These include:

i. Digital Inclusion and Accessibility: Ethical considerations extend to ensuring digital inclusion and accessibility for all individuals, regardless of their socio-economic status or physical abilities. ICT should not create or exacerbate societal divides but should strive to provide equal opportunities for participation and access to information and services.

ii. Cybersecurity and Digital Trust: As digital interactions become increasingly integral to daily life, maintaining cybersecurity and fostering digital trust are essential ethical imperatives. Cyber threats, ranging from hacking to identity theft, require constant vigilance and the implementation of ethical practices to protect users and their digital assets.

iii. Environmental Sustainability: The environmental impact of ICT infrastructure is another area demanding ethical scrutiny. The energy consumption of data centers, electronic waste management, and the carbon footprint of ICT activities must be minimized to align with ethical standards that prioritize environmental sustainability.

iv. Social Responsibility in ICT: Ethical considerations in ICT extend beyond technical aspects to encompass social responsibility. Companies and developers bear a responsibility to contribute positively to society, respecting human rights, and avoiding technologies that could be used for harmful purposes. This includes being mindful of the potential social, economic, and political implications of their innovations.

v. Educating Users: Ethics in ICT also involves educating and empowering users to make informed decisions about their digital presence. This includes promoting digital literacy, educating users about the risks and benefits of technology, and enabling them to navigate the digital landscape responsibly.

INFORMATION LEAKAGE

Information leakage refers to the unintentional release of sensitive or confidential information to the general public or unintended recipients. It can be as a result of criminal exploitation, improperly configured server or application, eavesdropping or social engineering attack that targets an employee and tricks them into sharing secret information or disclosing access credentials for a secured system. Stolen information may used to commit fraud or identity theft, steal financial resources, or gain access to other restricted systems.

The main attribute of information leakage attacks is that the goal is usually to compromise sensitive data that is owned by a target organization. Information leakage attacks can take many forms and leverage a variety of digital attack vectors. Information leakage could also happens by accident; employees may accidentally share confidential information with a friend or family member, or they may mistakenly send sensitive information to the wrong recipient.

Preventing Information Leakage

i. Implement Cryptography. This provides encryption algorithms for all information that is transmitted over networks or stored on a server. Even if a message is intercepted, it will not be useful to the recipient. Portable encryption, for example, automatically encrypts data that leaves organization, making it harder for attackers to read and exploit.

ii. Use Strong Passwords: It is a good practice to use a combination of lowercase and uppercase letters, numbers, and symbols in password to make it more difficult to guess or obtain from brute force attacks.

iii. Check before sending: It is a good habit to always double-check the recipient when sending messages, especially if the information is confidential. This includes checking the main recipient Cc and Bcc. With one simple and careless mistake and a messages may end up the wrong recipient.

iv. Using Software: Some security model such as Tenant isolation can be deployed. Tenant isolation creates a logical or physical boundary between each user's data, making it impossible for one user to access or manipulate another user's sensitive information.

v. Educate employees: Training employee and getting them acquainted with the threats and vulnerabilities that can be exploited and company-wide policies for keeping information secure within an organization.

INFORMATION SECURITY GOVERNANCE

Information Security Governance describes the entire function of controlling, or governing, the processes used by a group to accomplish some objective. It represents the strategic controlling function of an organization’s senior management, which is designed to ensure informed, prudent strategic decisions made in the best interest of the organization.

According to the Information Technology Governance Institute (ITGI), information security governance includes all of the accountability and methods undertaken by the board of directors and executive management to provide:

- Strategic direction
- Establishment of objectives
- Measurement of progress toward those objectives
- Verification that risk management practices are appropriate
- Validation that the organization’s assets are used properly

Information Security Governance Outcomes

Effective communication among stakeholders is critical to the structures and processes used in governance at every level, especially in information security governance. This requires the development of constructive relationships, a common language, and a commitment to the objectives of the organization. The five goals of information security governance are:

i. Strategic alignment of information security with business strategy to support organizational objectives
ii. Risk management by executing appropriate measures to manage and mitigate threats to information resources
iii. Resource management by using information security knowledge and infrastructure efficiently and effectively
iv. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved
v. Value delivery by optimizing information security investments in support of organizational objectives.

INFORMATION SECURITY POLICY

Policies are Written instructions provided by management of organizations that inform employees and others in the workplace about proper behavior regarding the use of information and information assets. Policies are the basis for all information security planning, design, and deployment, so good security programs begin and end with policy.

Policies direct how issues should be addressed and how technologies should be used. Policies do not specify the proper operation of equipment or software—this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation.

According to Special Publication (SP) 800-14 of the National Institute of Standards and Technology (NIST), management must define three types of security policy:

1. Enterprise information security policies (EISP): This is also known as a general security policy, organizational security policy, IT security policy, or information security policy. EISP is an executive-level document that guides the development, implementation, and management of the security program. It sets out the requirements that must be met by the information security framework. It defines the purpose, scope, constraints, and applicability of the security program and also addresses legal compliance.
2. Issue-specific security policies (ISSP): An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as one of its processes or technologies.
3. Systems-specific security policies (SSSP: This functions as standards or procedures to be used when configuring or maintaining systems; example, describing the configuration and operation of a network firewall.

In general, the issue-specific security policy (ISSP) addresses specific areas of technology as listed below, requires frequent updates, and contains a statement about the organization's position on a specific issue. An ISSP may cover the following topics, among others:

- E-mail
- Use of the Internet and World Wide Web
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibitions against hacking or testing organization security controls
- Home use of company-owned computer equipment
- Use of personal equipment on company networks (BYOD: bring your own device)

- Use of telecommunications technologies, such as fax and phone
- Use of photocopy equipment
- Use of portable storage devices such as USB memory sticks, backpack drives, game
- players, music players, and any other device capable of storing digital files
- Use of cloud-based storage services that are not self-hosted by the organization or
- engaged under contract; such services include Google Drive, Dropbox, and Microsoft Live

Security Policy and Law

Security affairs are increasingly intertwined with legal complexities. Experts, practitioners and stakeholders thus experience a growing need for guidance at the intersection of security policy and international laws. It is the responsibility of policymakers to close the gap between policy and law.

Policies should never contradict law; policy must be able to stand up in court, if challenged; and policy must be properly administered through dissemination and documented acceptance. Policy that conflicts with law is by definition illegal; therefore, following such a policy is a criminal act. Policies function like laws in an organization because they dictate acceptable and unacceptable behavior there, as well as the penalties for failure to comply. Like laws, policies define what is right and wrong, the penalties for violating policy, and the appeal process.

INFORMATION SECURITY COMPLIANCE

Information security compliance refers to the process of adhering to regulatory requirements, industry-specific laws, and internal security policies. While regulatory compliance entails abiding by external laws and regulations relevant to an organization's business processes, security compliance encompasses meeting specific security frameworks, standards, and internal policies to uphold data protection and privacy.

To achieve security compliance, organizations must establish risk management processes and security measures to safeguard their data, assets, systems, and operations from potential threats and lessen the likelihood and impact of security incidents such as data breaches. An organization's security compliance must also be validated through an external audit.

Information Security Compliance Frameworks

To facilitate their compliance with the laws and regulations above, there are various security frameworks that organizations can utilize to guide the development of their security compliance management program. A few of these frameworks include:

1. Security Standards

Standards provide requirements, specifications or characteristics that must be observed by individuals and organizations to ensure that the products, processes, and materials have acceptable levels of quality. The qualities that various standards provide may be those of safety, reliability, or other product characteristics. Examples safety staandards include:

- ISO/IEC 27000 a set of international security standards originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005. It is global standard for Information Security Management Systems (ISMS) that details requirements for establishing, implementing, maintaining and continually improving information security management system with the aim of helping organizations make information assets more secured. They include ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27035, etc.

- NIST CSF – The National Institute of Standards and Technology's Cybersecurity Framework equips organizations with best practices and actionable steps in managing cybersecurity risks. It establishes 6 functions for risk management that can be tailored to fit the specific context of an organization: Govern, Identify, Protect, Detect, Respond, and Recover, with each function extending to categories and sub-categories that contain security controls. Compliance with NIST CSF can be measured by conducting an internal assessment. Unlike ISO 27001, it does not require an external audit or certification.

2. Plan, Do, Check, Act (PDCA)

Plan, Do, Check, Act (PDCA) is an iterative design and management method used in business for the control and continual improvement of processes and products. It is a four-step model for carrying out change; just as a circle has no end, the PDCA cycle is repeated for continuous improvement until the goal is reached. It is considered as a project planning tool.

The model is associated with W. Edwards Deming, who is considered the father of modern quality control; however, he used PDSA (Plan-Do-Study-Act). A fundamental principle of the plan–do–check–act is iteration. Once a hypothesis is confirmed (or negated), executing the cycle again will extend the knowledge further. Repeating the PDCA cycle can bring its users closer to the goal, usually a perfect operation and output.

Stages of PDCA:

The PDCA cycle has four stages:

i. Plan: Determine the goals for a process and needed changes to achieve them.
ii. Do: Carry out a small-scale study to implement the change.
iii. Check: Review the test, analyze the results, and identify the performance.
iv. Act: Depending on the results; incorporate the change, otherwise, go through the cycle again with a different plan.

Application of PDCA Cycle

The Plan, Do, Check, Act can be applied to different scenarios, including:

i. Starting a new improvement project.
ii. Developing a new or improved design of a process, product, or service.
iii. Defining a repetitive work process.
iv. Planning data collection and analysis in order to verify and prioritize problems or root causes.

3. Certification

Certification provides an official document attesting to a status or level of achievement. A common type of certification is professional certification, where a person is certified as being able to complete an activity in a certain discipline at a stated level of competency. Professional certification also can also verify the holder's ability to meet professional standards and to apply professional judgment in solving or addressing problems. Professional certification can also involve the verification of prescribed knowledge, the mastering of best practice and proven methodologies, and the amount of professional experience.

Professional certification are usually obtained by taking various courses and engaging in training in conjunction with writing and passing certification exam in some cases. certifications validate the knowledge of professionals in IT industry standard processes and techniques. Common certifications include:

- Systems Security Certified Practitioner (SSCP). This certification validates skills to design, implement, and monitor a secure IT infrastructure. It focuses on access controls, risk identification and analysis, security administration, incident response, cryptography, and network, communications, systems, and application security. It is designed for IT professionals working hands-on with an organization's security systems or assets.
- GIAC Certified Incident Handler (GCIH): This certification validates holders understanding of offensive operations and certifies the ability to detect, respond to, and resolve computer security incidents using a range of essential security skills. It covers incident handling, computer crime investigation, hacker exploits, and hacker tools.
- Certified Information Systems Security Professional (CISSP): Earning CISSP certification demonstrates experience in IT security and capability of designing, implementing, and monitoring a cybersecurity program.
- Certified Ethical Hacker: The ethical hacking certification demonstrates the skills of holders to in penetration testing, attack detection and prevention.
- Certified Information Security Manager (CISM): This certification validate the holders expertise in the management of information security in different areas like governance, program development, and program, incident, and risk management.

FORENSIC INVESTIGATION

Forensic investigation is the application of scientific methods and techniques to the investigation of crime. It involves scientific inquiry into all crime-related physical evidence in order to come to a conclusion about a suspect. It is considered a part of the litigation process because it is often necessary when gathering the evidence required to present a successful case to a court. It utilize DNA analysis, fingerprint, bloodstain pattern, toxicology analysis, etc.

It spans across a wide range of disciplines including accounting/auditing, computer or cyber forensics, crime scene forensics, forensic archaeology, forensic graphology, forensic graphology, forensic pathology, forensic toxicology. It aids in resolving civil disputes, enforcing criminal laws, and safeguarding public health. Forensic scientists and crime scene investigators work together to uncover scientific evidence that can be used in legal proceedings.

Forensics and Investigations in Classified Sensitive Data

Forensic investigations often involve collecting and analyzing sensitive information such as financial records, medical data, trade secrets, and personal communications. Protecting this kind of information is essential for both legal and ethical reasons. The volumes and variety of data have grown beyond expectation and relevant data from various sources are collected, documented and processed in an effective and defensible way for potential investigation. This has influenced the rapid evolution of digital forensics since it provides support crucial for law enforcement investigations. With criminal evidence increasingly residing on electronic devices, digital forensics has become a critical tool in combating crimes. To simplify the process of securing sensitive data, corporate IT structures are put in place using reputable, robust and defensible digital forensics tools and developing a response plan. This helps to detect data-related crime more quickly and prevent it over the long term. Simple step could also involve:

i. Investigators should obtain informed consent from individuals before collecting or analyzing personal information.
ii. Data should be collected and stored using secure methods, such as encryption and password protection.
iii. Only authorized personnel should have access to sensitive information.
iv. When data is no longer needed, it should be disposed of securely to prevent unauthorized access.

Digital Forensics

Digital forensics is a branch of forensic science, deals with the acquisition and analysis of digital evidence. This evidence is crucial in investigating cyber-security incidents or other criminal activities, contributing to legal procedures and incident response efforts. Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations. Electronic evidence can be collected from a wide array of sources, such as computers, smartphones, remote storage, local storage devices, unmanned aerial systems, etc. The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution. Digital evidence can generally be classified into two main types:

1. Volatile data: Temporary data that is lost once the system is powered off. This data provides real-time information about the system and is usually collected first during digital forensics. Examples include Random Access Memory (RAM) contents, Central Processing Unit (CPU) cache data, and running processes.

2. Non-volatile data: Data stored in permanent mediums such as Hard Disk Drives (HDDs), Solid-State Drives (SSDs), and Non-Volatile Memory (NVM).

- Computer Forensics: Involves the recovery and analysis of data stored on computers, laptops, servers, and other storage media.
- Network Forensics: Monitors and analyses network events or traffic to identify the source of cybersecurity incidents.
- Mobile Device Forensics: Analyses electronic evidence extracted from mobile devices such as phones, digital cameras, tablets, or smartwatches.
- Cloud Forensics: Involves recovery and investigation of data from cloud storage platforms and services.
- Memory Forensics: Studies the volatile data found in primary storage devices.
- Database Forensics: Examines databases and their metadata to identify fraudulent transactions or the validity of transactions through timestamps.
- Forensic Data Analysis: Involves analyzing structured and unstructured data, often used for financial crime investigations.