Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Managers Unit (Module) no and Week No: Unit-2 Week-4 Unit (Module) name: Information security management -2	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other** Streaming Webinar, Text, Self-assessment Exercises, Exercises with answers on discuss forums and be discussed with trainer/mentor
Learning Responsible	• Fatma Gökdemir • Ali Gökdemir
Learning Activity Goals	1. Threat and vulnerability assessment 2. Threat and vulnerability management 3. Types of vulnerability assessment 4. Cyber Continuity of Operations 5. Cyber Asset 6. Evaluation of cyber security policies effectiveness
Skills to be Gained	• IS 1 • IS 3 • MS 5
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Intermediate computer skills

Co-funded by the
Erasmus+ Programme
of the European Union

Brief information about the module

Description
The management of assets has an important place within the scope of ISO 27001 Information Security Management System. In fact, identifying and classifying Information Assets is one of the first steps of information security setup. Identifying and assigning value to assets in an organization is a fundamental step in the risk analysis process. An asset inventory is prepared in order to assign value to assets. An exploratory study covering all employees should be conducted prior to the asset inventory. With this study, the asset inventory of the department is explored and listed with possible risks and confidentiality degree. Asset inventory should be done one by one on the basis of the covered processes. While preparing the asset inventory; the asset group, the environment in which the specified asset is located, the classification code is determined, and the asset value (confidentiality, integrity, accessibility) is calculated. According to the calculation result, the priority status is determined, and action decisions are taken. After the asset inventory work is completed, a detailed inventory list is prepared for the detected software-hardware inventories. Conditions/controls regarding asset management in the ISO27001 standard are gathered under Annex A.8. In this module we will examine the terms for Liability of Assets defined in A.8.1.

Content of the Learning Material

1. Assess Management of Information Security

In the first stage of asset management, it would be useful to first reveal and list what assets we have. What an institution has or does not have should be known first. Then their ownership needs to be defined. No business or transaction should be left unattended. Then, the rules for the use of these assets should be determined.

For the details of the subject, the ISO27002 standard should be examined. The expectations regarding Asset management in ISO27002 are included in the 8th article of the standard:

Asset management and liability for assets

Purpose: To identify the organization's assets and define appropriate protection responsibilities.

1. Asset inventory

Control: Assets related to information and information processing facilities should be identified and an inventory of these assets should be made and maintained.

Application guide: An organization should identify relevant assets in the information lifecycle and document their importance. The information lifecycle should include creation, processing, storage, transmission, deletion, and destruction. Documentation should be maintained in accordance with existing inventories or specifically.

Asset inventory; must be current, consistent, accurate and compatible with other inventories.

Asset ownership should be allocated for each identified asset (see Article 2) and its class should be determined.

Other information: Asset inventory helps to provide effective protection and may also be necessary for other purposes such as health and safety, insurance or financial (asset management) reasons.

The ISO/IEC 27005[11] standard provides examples of assets that may need to be considered by the organization when identifying assets. The process of compiling an asset inventory is an important prerequisite for risk management (see ISO/IEC 27000 and ISO/IEC 27005[11]).

2. Ownership of assets

Control: Owner assignments must be made for all assets held in inventory.

Application guide: Individuals and other entities with approved management responsibility for the asset lifecycle are eligible to be designated as asset owners.

A process is often used to ensure that asset ownership is determined in a timely manner. Ownership must be determined when assets are created or transferred to the organization. The asset owner should be responsible for the proper management of the asset throughout the asset lifecycle.

Asset owner:

a) Ensure that asset inventory is recorded,

b) Ensure that assets are properly classified and protected,

c) Define and periodically review restrictions on access to significant assets and their classification, taking into account the applicable access control policy,

d) Ensure that appropriate action is taken in deleting or destroying assets.

Other information: It can be an individual or entity with approval for management responsibility to control an asset throughout its lifecycle. The identified owner has no ownership interest in the asset.

Routine tasks may be delegated; (for example, a custodian who looks after an asset on a daily basis) but the responsibility rests with the asset owner.

Identifying groups of assets within complex information systems can be useful in providing functions together. In this case, this service owner is responsible for the delivery of the service, including the operation of the assets.

3. Acceptable use of assets

Control: Rules regarding the acceptable use of information and assets related to information and information processing facilities should be determined, documented, and implemented.

Application guide: Employees and external users who use or have access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. These users should be responsible for the use of all information processing resources and for any use that occurs under their own responsibility.

4. Return of assets

Control: All employees and users of external parties must return all corporate assets in their possession upon termination of employment, contract, or agreement.

Application guide: The termination process should be formulated to include the return of ownership of all previously granted physical and electronic assets or escrows of the organization.

When an employee or outside user purchases or uses the organization's equipment, procedures are followed to ensure that all relevant information is transferred to the organization and securely deleted from the equipment.

Where an employee or external user has information that is important to ongoing operations, this information needs to be documented and transferred to the organization.

During the termination notice period, the organization; control the unauthorized copying of related information, such as intellectual property, by terminated employees and contractors.

2. Threat and vulnerability assessment and management

Almost every organization has sensitive and valuable assets that need to be protected. However, not every organization has a comprehensive and fully thought-out strategy for protecting these assets. In cybersecurity, vulnerability management strategies are the foundation of strong defense. Typically, vulnerability management strategies are designed to help an organization's systems, networks, applications, etc. It adopts a holistic and continuous approach to managing security vulnerabilities in These vulnerabilities are then identified, evaluated, and fixed as soon as possible.

Security threats and trends are constantly evolving, requiring effective, preventive efforts to manage threats and vulnerabilities that could compromise your data. To identify all potential targets for a breach or attack, its risk must first be mitigated by conducting an asset inventory. The targets must then be classified and continuously monitored for new potential vulnerabilities. A threat model that identifies the organization's most valuable assets at high risk should then be developed and tested. The primary purpose of the Threat and Vulnerability testing process (assessment) is to best understand the criticality of assets, the vulnerabilities to these assets, and reduce the necessary measures to effectively protect these assets.

2.1. What is vulnerability assessment?

Vulnerability assessment is the process of identifying, identifying, classifying, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures.

Vulnerability assessments also provide an organization with the knowledge, awareness and risk background necessary to understand and respond to threats to its environment. A vulnerability assessment process aims to identify threats and the risks they pose. Often they involve the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report.

Organizations of any size, even individuals at increased risk of cyberattacks, can benefit from some form of vulnerability assessment, but large organizations and other types of organizations exposed to ongoing attacks will benefit most from vulnerability analysis.

Because vulnerabilities can allow hackers to gain access to IT systems and applications, it is critical for organizations to identify and fix vulnerabilities before they are exploited. A comprehensive vulnerability assessment combined with a management program can help companies improve the security of their systems.

2.2. The importance of vulnerability assessments

To better illuminate the importance of vulnerability assessment, let's consider it through the eyes of a physical property owner. If you own a valuable building, you probably take a number of measures to protect it: You maintain it, insure it, and make sure the doors, windows, are locked, and alarms are activated. All of these steps can be termed as managing the risk to the property and its contents.

Now what if you could hire someone to test and report on your alarms and external defenses? Cybersecurity vulnerabilities are approached in a similar way. Vulnerability management is an overarching and ongoing strategy, while vulnerability assessments are a specific tool used in this broader management strategy.

A vulnerability assessment provides an organization with detailed information about any security weaknesses in its environment. It also provides direction on how to assess the risks associated with these weaknesses. This process provides the organization with a better understanding of its assets, security flaws and overall risk, reducing the likelihood of a cybercriminal breaching its systems and catching the business off guard.

2.3. Types of vulnerability assessment

Vulnerability assessments discover different system or network vulnerabilities. This means that the assessment process includes using a variety of tools, scanners and methodologies to identify vulnerabilities, threats and risks.

Some of the different types of vulnerability assessment scans include (Figure 1):

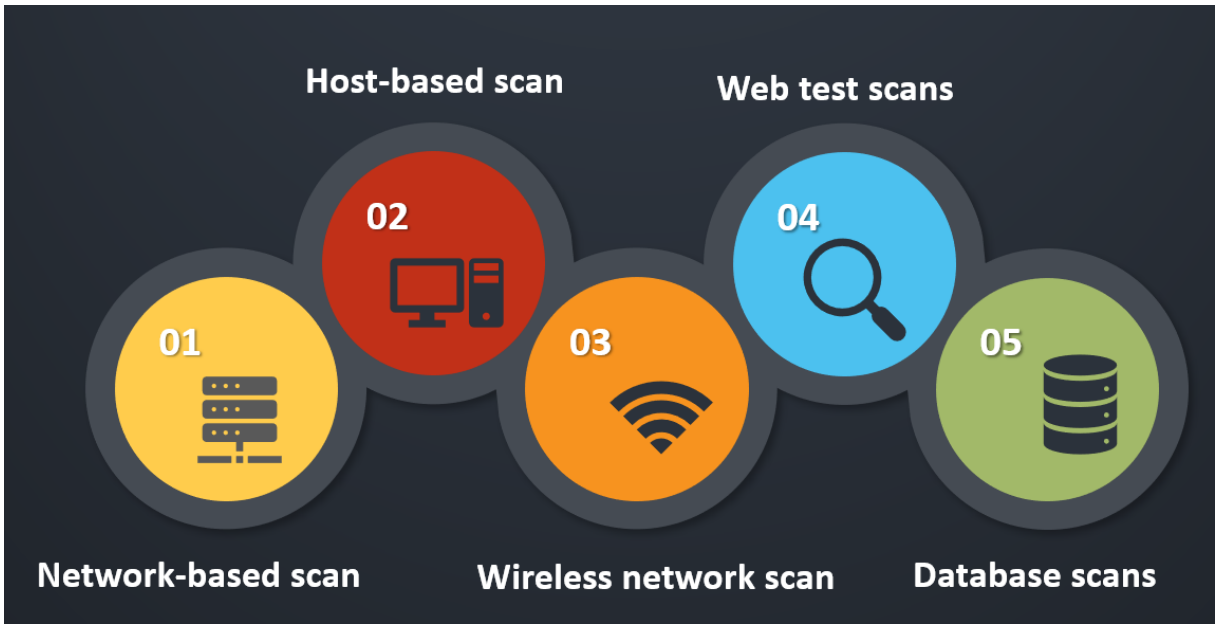

Figure 1. Types of vulnerability assessment

- **Network-based scans** are used to identify potential network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks.
- **Host-based scans** are used to find and identify vulnerabilities in servers, workstations, or other network hosts. This type of scan usually examines ports and services, which can also be seen in network-based scans. However, it offers greater visibility into the configuration settings and patch history of scanned systems, including legacy systems.
- **Wireless network scans** of an organization's Wi-Fi networks often focus on attack points in the wireless network infrastructure. In addition to identifying rogue access points, wireless network scanning can also verify that a company's network is securely configured.
- **Web scan test** sites to detect known software vulnerabilities and misconfigurations in application, network or web applications.
- **Database scans** can identify weak spots in a database to prevent malicious attacks.SQL injection attacks.

2.4. Vulnerability assessments and penetration tests

A vulnerability assessment often includes a penetration testing component to identify vulnerabilities in an organization's personnel, procedures, or processes. Vulnerability assessments share many of the same characteristics as penetration tests because both allow organizations to rigorously examine their defenses. These vulnerabilities may not normally be detected by network or system scans. The process is sometimes referred to as vulnerability assessment/penetration testing or **VAPT**.

However, penetration testing is not sufficient as a complete vulnerability assessment and is actually a separate process. A vulnerability assessment aims to uncover vulnerabilities in a network and suggest appropriate mitigation or remediation to mitigate or eliminate risks.

A vulnerability assessment uses automated network security scanning tools. The results are listed in the vulnerability assessment report, which focuses on providing organizations with a list of vulnerabilities that need fixing. However, it does this without evaluating specific attack targets or scenarios.

Organizations should regularly perform vulnerability testing to ensure the security of their networks, especially when changes are made. For example, testing should be done when services are added, new equipment is installed, or ports are opened.

In contrast, penetration testing involves identifying vulnerabilities in a network and attempts to use them to attack the system. Although sometimes performed in conjunction with vulnerability assessments, the primary purpose of penetration testing is to check whether a vulnerability actually exists. Additionally, penetration testing attempts to prove that exploiting a vulnerability can harm the application or the network.

While a vulnerability assessment is usually automated to cover a wide variety of unpatched vulnerabilities, penetration testing often combines automated and manual techniques, helping testers further investigate vulnerabilities and leverage them to gain network access in a controlled environment.

2.5. Vulnerability Management and Risk Management

While vulnerability management is an ongoing process of managing vulnerabilities, risk management takes a broader view of anything that can pose a threat to an organization. A sound risk management strategy allows risks to be identified, analyzed and effectively mitigated. This approach helps organizations understand not only the vulnerabilities that exist, but the scale of damage that can occur if abused. A risk and vulnerability assessment conducted under the

umbrella of risk management can provide a particularly broad perspective on the strength of an organizational security posture.

3. Cyber Continuity of Operations

Increasing resilience against threats of destructive malware requires insight into the current security posture, planning and coordinating key defensive actions, and aligning key defensive resources correctly.

Cyber incidents have likewise challenged basic continuity planning efforts. While many jurisdictions have equipment and strategies to identify, detect, and protect against cyberattacks, far fewer have worked through the hard realities of continuity of their operations through an actual attack. When cyberattacks do strike, many affected jurisdictions find that that their basic COOP plans don't hold up. While the plans are adequate for transitioning to an alternate work site, they have much less to offer when it comes to working without access to the systems and data staff need to perform their mission essential functions. Existing plans also lack the specificity needed to guide the response, and major stakeholders such as members of the IT staff are often not integrated into response structures. And plans are untested against an exercise or real-world incident.

Traditional COOP plans fall short for continuity during cyber incidents in several ways (Figure 2):

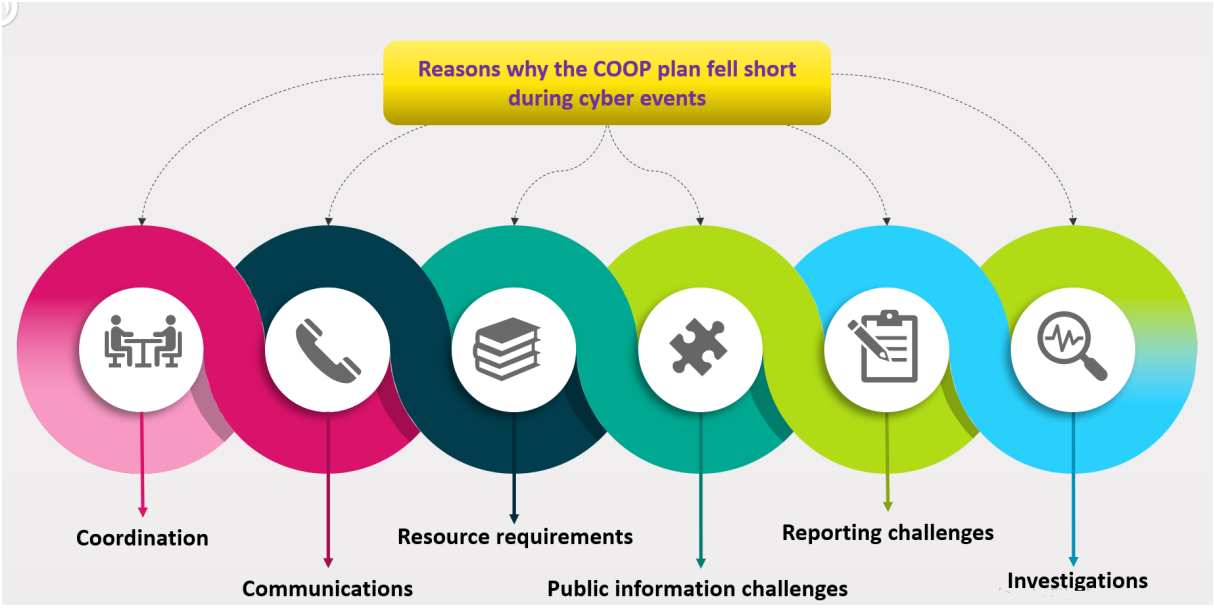

Figure 2. Reasons why COOP plans are insufficient for continuity during cyber events

Coordination: including who is involved in decision-making when it comes to ransomware, decisions to take systems offline, and decisions to activate the jurisdictional Emergency Operation

Center. Additionally, most local governments do not have clear escalation levels for an attack, nor the associated action items for each level. Response leadership and staffing may also be unclear; the types of subject matter expertise needed to guide a community through a cyber incident are different from those needed for extreme weather.

Communications: including how local managers will rapidly provide information to staff when a cyberattack has severely compromised communications. This includes both immediate communications explaining what to do when the attack begins and ongoing communications, such as how salaries will be provided by payday. Both are critical to response, and yet both may have to be relayed without the benefit of typical emergency communications systems.

Resource requirements: Which may be very different from those for a more traditional response. For example, staff might require clean computers, clean servers, local printers, and even fax machines and paper. Importantly, staffing requirements may surge even more during recovery than in response, as departments and agencies struggle to replicate missing or suspect data.

Public information challenges: Including public information officers with little to no training or experience in cybersecurity, a lack of pre-scripted messages, and disagreement on when information about the attack should be made public. Providing information to the public is critical because citizens worry about their data and the trustworthiness of key democratic systems such as voting and justice.

Reporting challenges: That can delay response, as outages aren't reported in a consistent manner, leaving IT departments without the necessary common operational picture to quickly identify an attack. In addition, the lines of reporting are often unclear, and few people outside of IT understand which systems are connected both within and external to the jurisdiction.

Investigations: Which is a black box for many localities. The involvement of one or more federal organizations and the limits investigations place on remediation efforts are not well understood or planned for. This makes continuity planning extremely difficult, because there is uncertainty about how and when remediation can even begin.

3.1. Priorities for Immediate Action with Coordinated Defense

- Develop a cyber 'Go Bag' with essential procedures and information.
    - o Assemble mobile cyber security toolkits that include procedures for establishing, implementing, maintaining, and enabling the continuance of cyber resilient TTPs within a COOP-designated facility

- Develop, test and validate playbooks, roles, responsibilities, and tools.

    o Designate specific cyber roles, associated responsibilities, and the cyber tools that may be deployed to ensure implementation of cyber COOP.

    o Define standard cyber COOP plays for individual or cyber team execution using cyber 'Go Bag' tools and elastic TTPs.

    o Conduct different types of cyber exercises (e.g. mini-table top type exercises) using the cyber 'Go Bag' and playbook.

- Define collaboration processes and acquire tools for cyber defenders and incident responders.

    o Ensure both mobile and stationary cyber COOP processes incorporate communication and coordination dovetailing to promote adequate management of cyber defenses, synergy among all response activities, and reduction of security coverage gaps during recovery activities.

While basic COOP plans have furthered local preparedness for many of the threats that jurisdictions face, they fall short during situations that create an environment very different than the norm. As IT departments around the country continue to make systems and data as secure as possible, it is up to emergency managers to stretch their imaginations and plan for cyberattacks that seriously impact critical systems and data.

3.2. Priorities for Immediate Action with Realignment

- Identify mission and business function dependencies on cyber resources.

    o Determine the mission purposes of resources so that uses that increase risk without any corresponding mission benefit can be identified and eliminated.

        ✓ Identify and remove or replace data feeds and connections for which risks outweigh benefits.

    o Consider the interdependencies between and among mission and non-mission business functions and organizations that share critical roles in the delivery of NEF capabilities.

        ✓ Reallocate resources or reassign administrative and management responsibility based on risk to mission and business function.

- Identify non-mission and business function dependencies on or uses of cyber resources.

o Make use of mission flow analysis, mission dependency analysis, tabletop exercises, and Red Teaming to uncover undocumented mission dependencies.

o Review and correlate mission and business functions with dependency model mapping and impact analysis activities and results.

o Identify systems, applications and processes of non-mission critical functions and the resources that support them.

- ✓ Assess those functions against a fluid Cyber COOP implementation strategy to accommodate priority operations and better dependency utilization or elimination.

4. Cyber Asset, Change and Configuration Management

- ✓ **Asset:** Let's start with the definition of an asset. The dictionary definition of an asset is a useful or valuable thing or person. Similarly, assets of an IT service provider are its tools, applications, configuration items, and any other valuable items that help to deliver services to the customers or business. Assets are one part of service asset and configuration Management.

- ✓ **Configuration Item:** Configuration Item is abbreviated as CI and a configuration item is any component that needs to be managed in order to deliver an IT Service. Examples of configuration items are IT services, hardware, software, buildings, people and formal documentation. So briefly, any component or item that helps to deliver an IT service to the customer is classified as a Configuration Item. Information about each configuration item is recorded in a Configuration Record within the Configuration Management System and this information is maintained through its lifecycle by Configuration Management.

- ✓ **Configuration Management Database:** Configuration Management database is abbreviated as CMDB. CMDB is a database used to store configuration records throughout their lifecycle. CMDB stores information about your CIs, each distinguished by a unique identifier, including identifying information like its serial number, MAC address or IP address; its current version; its location; and its vendor and supplier information.

- ✓ **Configuration Management System:** Configuration Management system is abbreviated as CMS and is a set of tools and databases that are used to manage an IT Service Provider's Configuration Data. Data about configuration items are stored in configuration records, and configuration records are included in the Configuration Management System Databases. The CMDBs of an IT Service provider to manage the configuration data is included in the service asset and configuration management process. The Configuration Management System also includes information about incidents, problems, known errors, changes and releases, employees, suppliers, locations, business units, customers, and users. In summary, all necessary information about configuration items and IT assets are included in the Configuration Management System. When needed, this information is acquired from the CMS and used respectively.

Configuration management, which is basically defined as the process of identifying, controlling, monitoring and auditing changes made, is a critical part of a strong security program. Change and

configuration management within an organization has strong links to audit requirements in nearly all security frameworks and regulations.

Configuration management is based on the control and release of various product versions. Default configurations for operating systems and applications are generally geared towards ease of deployment and use, not cybersecurity best practices. Today, configuration management is an in-demand discipline with significant cybersecurity implications, especially as organizations move from out-of-the-box default configurations to more secure application and hardware configurations.

Today, configuration management means different things to different people. In some implementations, it refers to the way network devices are configured. In others, it's about the version of an app a team is running. Sometimes people in the industry confuse IT asset management with change and configuration management. While they are similar and equally important to the business, they are not the same. IT management solutions monitor, optimize and manage assets across the entire asset lifestyle. Meanwhile, CM collects, stores, manages, updates and analyzes all configuration items.

While many organizations have immature CM programs, they are critical to the modern cybersecurity landscape and will only increase in importance as the threat landscape continues to evolve.

4.1. Configuration Management and Disaster Recovery

When it comes to modern disaster recovery, configuration management is essential. In the event of a cybersecurity disaster, (76% of organizations have experienced an IoT cybersecurity incident, after all) it can be impossible to recover to the most recent configuration if there is no documentation of said configuration.

The same goes for cybersecurity: it’s impossible for teams to know if something is amiss if there’s not a standardized way of configuring, changing, and documenting the digital environment.

4.2. Change Management

Change management runs parallel with configuration management, although the two things are *not* the same. People confuse them all the time.
While configuration management is the process of identifying and documenting hardware components and software and the associated settings, change management is an underlying function of the larger configuration management process. Change management relates to the associated processes and seeks to create stability within a system and prevent uncontrolled or random changes or to document change processes when you have turnover within the

organization. In other words, it allows companies to plan for change, rather than just reacting to it.

4.2.1. The Change Management Process

Today, a well-structured change management process will include the following:

- Change request submittals
- Risk and impact assessments
- Approve/reject change functions
- Testing
- Scheduling/user notification/training functions
- Implementation
- Validation
- Documentation

One of the places change management thrives is in the event of emergency decisions, when changes must be made. Once the change has been implemented, it should be fed back into the change management process, where it will then benefit from the validation and documentation protocols that were already established.

4.3. Cybersecurity asset management

Cybersecurity asset management is the process of gathering asset data (devices, cloud instances, and users) to strengthen core security functions, including:

- **Detection and response:** Ensuring detection and response capabilities provide coverage across the enterprise
- **Vulnerability management:** Understanding which assets may be vulnerable to exploits, and ensuring all assets are being evaluated for vulnerabilities
- **Cloud security:** Ensuring that cloud instances are secure and configured to prevent overly permissive access rights, even when they're commissioned and decommissioned rapidly
- **Incident response:** Using enriched, correlated data on assets to expedite incident response investigations and remediation
- **Continuous control monitoring:** Identifying when security controls are missing and need to be applied

5. Evaluation of cyber security policies effectiveness

The development of an information system progresses through several distinct phases from analysing the problem through to the implementation of the system. Throughout this process each step is documented through a series of deliverables that range from a feasibility study, through to training manuals and system documentation. In the development of a security policy this self- documentation process generally does not occur.

Many policies developed currently attempt to fit everything into the security policy: the justification of importance and specific system instructions and descriptions. Certainly, the security policy itself is already long-winded enough, without having details on how the document was created, who was consulted in its production or how the policy formulation was achieved. Nor will there be any documentation of political problems that may have occurred during the implementation of the policy, or of how to train people about the policy. With the use of documentation techniques during the development of the policy, however, a security policy could become a principles document again. Other issues not dealing with the principles of security policy would be documented elsewhere along with the justification for the policy.

The most important information that is often missing or just inadequate when we attempt to evaluate a security policy in an organization is the requirements documentation. Without a clear understanding of the requirements, evaluation of the quality of a security policy is almost impossible. An analysis of the risks/threats faced by the organization is only part of the requirements needed for the development of a security policy. The organization's objectives and other political issues that influence the development, implementation and acceptance of the security policy are just as important. The availability of extensive documentation including the outcomes of an extensive requirements analysis will allow the evaluation of the security policy to reach a greater depth, instead of just superficially evaluating the end product. For instance, rather than concentrating only on whether the policy has been implemented in a particular area, the evaluation can now also consider how that area was developed within the policy. Documentary evidence could be evaluated to determine if the policy adequately covers all issues identified within development without watering any of them down. However, security policies vary greatly depending on the context of the organization and one would expect that their development would also vary. Some commonalities between policies would exist, even as target areas digress. Unlike product evaluation however, many criteria in security policy evaluation will be of a subjective nature. This is because of the subjective nature of developing a policy and of the environment in which the policy is implemented.

5.1. Maintaining Effectiveness of IT Security Policies

Information technology, or IT, is arguably the technology of the century. It sure has transformed the world. With all the benefits of IT, however, a lot of security risks have also penetrated our lives. Organizations must design effective information security policies to ensure that their

business operations remain safe from the malicious intruders and data to thieve. Ironically, an excellent way to maintain the effectiveness of security policies against the changing IT risk landscape is to use more IT.

Here are some of the ways in which IT can maintain the effectiveness of security policies:

- **Better risk assessment:** Security risk assessment is an essential first step in designing any information security policy. To address the threats arising from the rapidly evolving IT sector, IT is the only antidote. Since risks change constantly, IT is a must to keep the new threats in check. It allows you to easily discover new risks based on your previous compliance records, rank and classify the risk factors and assess the damages it can cause. Thus, it is important to learn from the new developments–good or bad–in IT. This will improve your risk assessment as well as your preparedness in case a threat is imminent.
- **Better compliance**: IT helps you monitor how well the employees and the heads of your organization remain compliant with the regulatory authorities as well as your organization-specific security policies. Through a single software, you can keep an eye on access authorizations, insecure data sharing, unsafe web surfing, insufficient data encryption, and countless other factors that can gravely affect your security.
- **Constant up-gradation is a must**: Since the world of IT is changing with every breath we take, you must constantly be on the look-out for new changes that can break your system. Monitor the developments in the world of cyber-risks, cyber-crime, and cyber-security. Upgrade your information security policies and your security software frequently and regularly, because they can get out-of-date very quickly. This way, you can maintain the effectiveness of your security policies.
- **Quick mitigation**: If your organization does face an impending security threat that can lead to potential data loss or theft, you must have a mitigation or remediation plan at hand. IT helps you plan mitigation in a simple and efficient manner. With IT, you can assign and link risk mitigation steps to different potential risks when you design your security policies. This will make mitigation timely and more effective, thus maintaining the effectiveness of your security policies.
- **Improved accountability**: No information policy can remain effective if people are not held responsible and accountable for risks, compliance, and mitigation. IT makes it easier to ensure the accountability of remedial action. It can greatly improve the Visibility of Risks and Maturity assessment, compliance, and the remediation measures that your organization undertakes. This means that your employees will be more prompt and more accountable towards the steps listed in your information security policies.

5.2. Evaluation Security Risks

Risk Assessment, after determining which information assets will be protected, the risk assessment method is selected, and the risks are defined. According to the chosen risk assessment method, information assets are positioned on the risk map shown in the figure. After the assessment is made, the risk assessment map covers the processes of improving and controlling risks for threats with high impact and probability. Since the location of information assets in the risk map may change, the risk assessment map should be updated regularly, and necessary precautions should be taken.

Risk is defined as the combination of the probabilities of an event and its outcome. Risk assessment, which is a step of risk management, is a process in which risks are defined and the effects and priorities of these identified risks are determined. Risk management is to determine an acceptable level of risk, to evaluate the current risk, to take the necessary steps to reduce this risk to an acceptable level, and to maintain this risk level. Information and other assets, threats to these assets, vulnerabilities in the existing system, and security system controls are the components that determine the current risk. Identifying information or assets that need to be protected; determining how valuable these assets are to the establishments; revealing which of the known and possible threats to these assets will be tried to be prevented; investigating how possible losses might occur; identifying the extent of possible threats to each asset; Examination of what can be done in the first place to reduce the extent and probability of losses that may occur in these assets and planning the steps to be taken to keep the forward-looking threats at a minimum level are certain phases of risk assessment. The cost of the security system to be established and implemented as a result of risk management is another important issue to be considered. The cost of the security system should be limited by the value of the information protected and the risk determined by examining possible threats. Along with the principle that there will be no 100% security, the ideal configuration of information security is realized through three processes. These processes are prevention, detection and response (response or reaction).

Prevention; It is the process that security systems focus on and work the most. Various measures are being developed to insulate the system against threats and attacks against computer systems, such as security measures used in daily life such as fencing a house's garden and using a steel door. Regarding personal computer security, having virus scanning programs installed, performing these programs and operating system service packs and error correction and updates at regular intervals, using a password-protected screen saver on the computer, leaving the system after being away from the computer for a long time, estimating the passwords used is difficult. determining, keeping these passwords confidential and changing them at regular intervals, being careful about disk sharing, paying attention to files downloaded from the Internet or sent by e-mail, protecting important documents with a password or keeping them encrypted, e-mail confidential or important information, sites without security certificates. Some of the measures

that may seem simple, but save lives, such as not being sent via unsafe means, turning off internet access when not in use, taking regular backups of important information and documents. Prevention steps to be implemented in computer security in corporate environments are broader and more complex. Some of the things that are done about prevention in such systems where security experts work:

- Periodically reviewing the service packs and updates of the operating system and software,
- Keeping user rights to a minimum, not running unused protocols, services, components and processes,
- Encryption techniques in data transmission, vulnerability scanners,
- Using Virtual Private Network,
- The use of Public Key Infrastructure and e-signature can be listed as the use of Biometric-based systems.

In fact, if the progress determined in the prevention process could be perfect, further processes would not be needed at all. All attacks would have been prevented at the worst. But no security product is perfect or complete. In addition, almost every day, various vulnerabilities are detected in transmission systems, Internet services, web technologies and security applications. From this point of view, using detection and matching processes increases.

Determination; Security is not just a matter of prevention. For example, the fact that a museum is well protected, that the museum is surrounded by fences, that the doors are closed and locked, does not necessitate the use of guards at night in that museum. In the same way, the use of methods to detect attack attempts on computer systems is also increased. Prevention is building a barrier that either makes attacks stronger (but not impossible) or discourages (but does not destroy) attackers. Prevention without detection and response may have only limited benefit. If only prevention were sufficient, most attacks would not even have been known. With detection, previously known or newly emerged attacks can be reported and given appropriate responses. The first and most basic step in detection is to monitor the entire state and movement of the system and to keep records of this information. In this way, data and evidence are also collected for post-attack analysis. Firewalls, intrusion detection systems, network traffic monitors, port scanners, honeypot usage, real-time protection virus and spyware tools, file checksum control programs and network Sniffer sensors are some of the most common methods used in the detection process.

AnswerBack; Just as a place equipped with guards, dogs, security cameras, sensors can attract the attention of thieves, computer systems with real-time detection systems are also attractive to hackers and attackers. Rapid response emerges as an essential element that complements the security system to repel these attacks. Response can be defined as the execution of actions that

will respond immediately or as soon as possible to attack attempts that cannot be dealt with by the prevention process and determined by detection processes. Intrusion detection systems can make sense if there is someone or a system to respond to this detection. Otherwise, this situation does not go beyond the benefit of a car alarm that no one hears and cares about. In this respect, reciprocation is an important link that completes the security process. Even if the attack is not completely prevented; It allows the system to return to its normal state, to identify the causes of the attack, to catch the attacker, when necessary, to identify security system vulnerabilities, and to reorganize the prevention, detection and response processes. Planning the actions to be taken when an attack is detected, in advance, will ensure that this process works effectively and will not waste time and money. Disaster recovery is at the forefront of the major worst-case plans undertaken for this phase.

Questions:

1. Which of the following is not one of the stages of asset management.

A) Making an inventory of assets

B) Determination of ownership of assets

C) Determination of the cost account

D) Determination of asset usage rules

2. What is the primary purpose of the Threat and Vulnerability testing process?

A) To best understand the security vulnerabilities of the assets and to take the necessary measures to protect these assets effectively.

B) Managing security vulnerabilities

C) Obtaining preliminary information about the asset inventory

D) Closing security vulnerabilities

3. Which of the following is not a type of vulnerability assessment?

A) Network-based scans

B) Host-based scans

C) Database scans

D) Server-based scans

4. Which of the following is not one of the Cybersecurity asset management process?

A) Vulnerability management

B) Cost management

C) Continuous control monitoring

D) Detection and intervention

5. Which of the following is not a way for IT to maintain the effectiveness of its security policies?

A) Risk assessment

B) Constant up-gradation

C) Quick mitigation

D) Security policies

6. Which of the following is not one of the three processes that constitute the ideal configuration of information security?

A) Preparation

B) Prevention

C) Determination

D) Answerback

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- **What is vulnerability of IT systems**
- **Explain and give sample for Vulnerability Management and Risk Management**

Attachments (PowerPoint presentation, handouts, prints, links, video…):

References:

1. Evaluating IS Security Policy Development S.B. Maynard1 & A.B. Ruighaver2 Department of Information Systems University of Melbourne Australia
2. https://www.bizzsecure.com/how-it-can-maintain-the-effectiveness-of-security-policies/
3. https://blog.masterofproject.com/service-asset-and-configuration-management/
4. https://www.apptega.com/blog/change-configuration-management-cybersecurity
5. https://cam.scmagazine.com/it-service-management-vs-cybersecurity-asset-management/
6. http://www2.mitre.org/public/industry-perspective/documents/06-ar-cyber-coop-planning.pdf
7. https://icma.org/articles/pm-magazine/cyber-continuity-planning-go-big-or-go-home
8. https://www.kroll.com/en/services/security-risk-management/security-consulting/threat-vulnerability-assessments
9. https://www.xmcyber.com/blog/what-is-the-difference-between-vulnerability-assessment-and-vulnerability-management/
10. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis