**Exam #1**

1. **The NIST Computer Security Handbook approach to computer security has eight major elements. What are they, and briefly describe what each one does**?

**A:**

The eight major elements are:

1. **Computer security should support the mission of the organization.**

Computer security should be designed in such a way that it protects, values, and supports the organization’s mission, including its tangible and intangible assets.

1. **Computer security is an integral element of sound management.**

Information and data are crucial assets that support the organization’s mission, and it's especially important to protect the organization's assets.

1. **Computer security should be cost-effective.**

The cost of security and the advantages it provides should be carefully balanced so that it does not exceed the budget of the organization. Layered security will indeed remove many dangers while increasing productivity.

1. **Computer security responsibilities and accountability should be made explicit.**

Every organizational role's responsibility and accountability must be specified clearly and in detail, leaving no space for uncertainty or ambiguity.

1. **System owners have computer security responsibilities outside their own**

**organizations.**

The owner must provide enough information about their security procedures for users to feel secure with the organization. However, while notifying clients about the nature of their security, the owner may be implicit.

1. **Computer security requires a comprehensive and integrated approach.**

A comprehensive strategy that considers a range of areas both within and outside of the computer security company is essential. Interdependencies among security controls are a powerful addition to computer security.

1. **Computer security should be periodically reassessed.**

Computers and the settings in which they function are both dynamic, hence the security threats are always increasing. Computer security should be periodically audited and updated to the latest technology possible to keep up with new security threats.

1. **Computer security is constrained by societal factors.**

There may be societal difficulties around the privacy of the user's workplace, tracking user behaviours, or regarding the use of different authentication measures. Ideal security measures should be chosen and executed with consideration for others' rights and legitimate interests.

*Ref. SP 800-12 Chapter 02, Pages 9-14.*

1. **An employee is using your organization's servers to host artwork and books that are in the public domain. According to your security program, you are writing for the class, would this be in violation of any policy, if so, please describe. If not, would your security program require a new policy?**

**A:**

ACME Defense Contractors already has an Acceptable Usage Policy (AUP) in place that states that no tangible or intangible assets of the company should be utilized for personal gain, and "use of the organization server to display artwork and books" is a direct violation of the policy. Any employee who violates the rules shall be notified and may face temporary suspension, and the data should be permanently deleted without recovery.

*Ref. Previous Assignment Submissions*

1. **Describe a sequence of steps a determined attacker would use to gain access to an organization's data, and some steps you might take to mitigate the attack. That is, what would you do to try and prevent the attacker from succeeding?**

**A:**

An attacker might obtain access to ACME defense contractors by circumventing physical security by disabling CCTV cameras, acquiring more information with social engineering, stealing any business equipment, logging into the account, and stealing critical information. To counteract the attack, ACME has taken numerous safeguards to prevent these attacks from occurring. First, many CCTV cameras have been put across the facilities as physical security. The primary requirement is that a business-issued device is connected to the ACME Wi-Fi Network and that the user confirms the login in any linked multi-factor authentication. Even if an attacker successfully logs in to an account by connecting to the ACME Wi-Fi Network, the system will continuously collect information about the device's position and behavior. To avoid illegal access to users, the system is associated with layered security, with numerous detection systems on each layer to enhance complexity, and with role-based access control (RBAC) to prevent unauthorized access. In addition, mandatory awareness training and periodic audits should be conducted to improve business security.

*Ref. Previous Assignment Submissions and Module 8*

1. **When writing a security policy, what 5 questions should writers ask themselves to ensure they will end up with well-written policies?**

**A:**

To develop a good policy, the writer must adhere to a consistent framework and describe everything clearly and in detail, leaving no room for uncertainty or doubt. Writers should ask themselves five questions: "Who," "What," "Where," "When," and "Why."

*Ref.* [*https://www.sans.org/white-papers/492/*](https://www.sans.org/white-papers/492/)

1. **There are three foundational principles and two extensions that form the basis for most security plans and controls. Name them and describe each one.**

**A:**

The three foundational principles of security, also known as the "CIAs of security," are confidentiality, integrity, and availability, and the two extensions are authentication and non-repudiation.

* Confidentiality guarantees that only authorized people have access to the information.
* Integrity guarantees that only authorized people have to modify/delete information.
* Availability guarantees that the information is accessible to the authorized user when needed.
* Authentication guarantees that the user is verified by validating their identity through several authentication methods.
* Non-repudiation guarantees that the communication is genuine and that the sender is the one who sent it and cannot subsequently dispute it.

*Ref. Module 2.ppt*

1. **If the cost of controls to deal with a risk associated with a specific asset is greater than the value of the asset, what is the appropriate risk management decision? Explain why.**

**A:**

If the cost of the controls exceeds the asset's worth, it is preferable to avoid the risk using any of the risk mitigation methodologies such as "Risk Avoidance." The right risk management decision is to mitigate the risk, and in this situation, avoiding the risk by removing the risk source and/or consequence is still mitigation since the risk is avoided.

*Ref. Module 3.ppt Slide 14, SP 800-30 Chapter 4 Page 27.*

1. **In regards to information classification, why is it important to establish a classification scheme to classify an organization’s information?**

**A:**

It is critical to build a categorization scheme because it allows us to determine which types of nature are extremely sensitive and can be stored on the right system where they can be secured with high security. Classification allows us to prioritize the information by classified, unclassified, sensitive, not sensitive, protected, not protected, restricted, not restricted, confidential, not confidential, and many more criteria. This also helps us determine which roles in the business have access to various sorts of information.

*Ref. Module 2.ppt*

1. **Why is it considered inappropriate to include how to do something within a policy?**

**A:**

It is not proper to put instructions on how to do something in a policy since a policy is just a collection of rules or guidelines for the business to follow to achieve its goal. The primary purpose of the business is for users to follow the policy without violating it. Policies may contain rules or standards that aid in maintaining discipline, guaranteeing compliance, making decisions, and so on but do not contain procedures. Procedures are instructions on how to do something in an organization that is inappropriate to include within a policy.

*Ref. Google Search*

1. **What is the first process in the risk management methodology and describe its function?**

**A:**

The first process in risk management is to identify risks. which is further subdivided into asset identification, threat assessment, impact definition and quantification, control design and evaluation, and residual risk management.

* Asset identification is the process of identifying, categorizing, and prioritizing assets based on the risk associated with the asset.
* Threat assessment is the calculation of events such as catastrophes, fraud, theft, and attacks that have the potential to destroy an asset.
* Impact definition and quantification is the process of converting risk into the impact that it can have when an event occurs. The impact may be both tangible and intangible.
* Control design and evaluation is the process through which controls are established to reduce vulnerabilities to an acceptable level to control risk.
* Residual risk management is the process of evaluating all residual risks after controls have been implemented.

*Ref. Module 3.ppt Slides 19-32.*

1. **In any organization that heavily relies on information technology, who is responsible for the security of information, assets, etc.?**

**A:**

The organization heavily relies on its Chief Information Security Officer (CISO) for data security. The CISO is responsible for creating, modifying, updating, and managing the policies and strategies to secure data from threats and vulnerabilities. Everyone is accountable for the security of information, assets, and obligations.

*Ref.* [*https://www.spirion.com/blog/who-responsible-data-security-management-compliance/*](https://www.spirion.com/blog/who-responsible-data-security-management-compliance/)

1. **Why are Human Resource security policies dealing with terminations important? There are quite a few attributes to this questions so be thorough as you can with the information provided during the class and reading.**

**A:**

Dealing with HR policies is critical because, if not managed effectively, they might put the company's sensitive or secret information in danger and cause many other consequences. HR policies for terminations are divided into friendly and unfriendly terminations; friendly terminations are for people who retire by choice or leave for a better position, where access to sensitive business information is decided by the individual and is flexible. Unfriendly terminations are often classified as unhappy employees who may have an impact on the firm. To avoid this, each scenario should be assessed on its own merits. Control access to sensitive business information, remove access rights, collect access cards and badges, immediately change passwords and combinations, and accompany employees to their cabins to retrieve personal things and to the building's exterior.

*Ref. Module 2.ppt Slide 58-66.*

1. **When deciding on a risk assessment design, there are two standard methods for an organization to determine what is at risk and by how much and decide which is the highest priority. Describe what you would design and why you would choose the method(s) including reasons why one is preferred over the other.**

**A:**

The two standard methods are qualitative assessment and quantitative assessment.

When assessing risk qualitatively, the effect of the threat must be compared against its probability of occurring. When a threat has a high impact and a high probability of occurring, the risk exposure will be high, and when a threat has a low impact and a low probability of occurring, the risk exposure will be low.

When assessing risk quantitatively, they may depend on models that aid in decision-making in the form of quantitative measurements. It also predicts future performance using previous data and trends.

The architecture of risk assessment differs from business to business. We can create qualitative risk assessments, but pure quantitative risk assessments are impossible. To select the appropriate risk assessments, the company must examine the project's criticality, available resources, and management style.

Depending on the business, if the business does not have time, it is preferable to create a qualitative risk analysis that is rapid yet subjective. If the business has the time and resources, it is preferable to create quantitative risk analysis, which takes more time, is more complex, is difficult to collect, and may be costly.

*Ref. Module 3.ppt, slides 35 to 51, and* [*https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/qualitative-vs-quantitative-risk-assessment*](https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/qualitative-vs-quantitative-risk-assessment)

1. **When designing a training program, why is it not enough to create one single training program for the entire organization?**

**A:**

We can’t create one single training program for the organization because we don’t have a fixed template for it. We need to specially tailor each training program to different users in an organization. Every user should be trained on how to safeguard physical spaces, equipment, and passwords, email, report security violations, understand the organization's roles and duties and learn about safety, sexual harassment, environmental management, and regulatory compliance. Users with specific tasks should get specialized training, such as incident response users receiving forensic training, system users receiving security access control training, and management receiving management training. The most significant and consistent feature of all training programs is that they must be updated on a regular basis in order to improve knowledge and stay up with the current technology.

*Ref. Module 4.ppt, slides 14-18.*

1. **Describe the requirement and steps for implementing an effective computer security awareness training program.**

**A:**

The requirements for implementing an effective computer security awareness training program (CSAT) are proper planning, implementation, maintenance, and periodic evaluation.

* Proper Planning - identify the program scope, goals, objectives, training staff, and target audiences.
* Implementation - Motivate management and employees. Administer the program.
* Maintenance - Maintain the program.
* Periodic Evaluation - Evaluate the program.

This is a lifecycle that continues to occur in order to enhance the CSAT by obtaining feedback for the next CSAT.

*Ref. SP 800-12 Chapter 13, page 150.*

1. **What is the confidentiality model and property that ensures that a classified object can only be read/written by a subject with the same classification label?**

**A:**

Bell-LaPadula (BLP) is a security model that was developed to address data confidentiality. And the property that ensures that a classified object can only be read/written by a subject with greater than or the same classification is the Bell-LaPadula Strong Star Property, also known as the Strong \*-property.

*Ref. Module 6.ppt, pages 5-11.*

1. **What are the three primary integrity goals of the Clark-Wilson Security Model?**

**A:**

Three integrity goals of the Clark-Wilson Security Model are:

1. Prevent unauthorized users from making modifications.
2. Prevent authorized users from making unauthorized or improper modifications.
3. Maintain internal and external consistency.

*Ref. Module 6.ppt, page 21.*

1. **Describe Least Privilege and its importance.**

**A:**

The least privilege is limiting and managing access to only what is absolutely necessary, allowing the user to complete activities without any additional permissions. The least important privilege is significant because it benefits the business. When a corporation limits access, it also limits the amount of harm that can be done to the business. For instance, a user with the least privilege will not have access to any private or sensitive data, avoiding a lot of danger to the company.

*Ref. Module 5.ppt, Page 4.*

1. **Explain why a constrained data object cannot be modified by a subject with the Clark-Wilson security model.**

**A:**

Clark-Wilson's security model is an integrity model that prevents unauthorized users from making modifications. A “constrained data item (CDI)” is one of the levels of integrity in the Clark-Wilson model that assures no user can modify data directly as it could violate integrity. It can only be modified by trusted transformation (TP) processes that have access to it.

*Ref. Module 6.ppt, pages 21-26.*

1. **Which of the Access Control Methods (Access Controls.pdf) would be best suited for a business that has thousands of employees, hundreds of thousands of files/applications/devices that need appropriate access controls, and there is a high turnover rate of employees? Explain your answer.**

**A:**

Role-Based Access Control (RBAC) is best suited for any business with thousands of employees, and hundreds of thousands of files/applications/devices because we control access based on the employee role rather than giving access to every individual separately and differently. The same goes for files, applications, and devices. RBAC is also chosen for the high turnover rate of employees.

*Ref. Access Controls.pdf*

1. **List the possible forms that can be used in multifactor authentication.**

**A:**

There are many forms in which we can use multi-factor authentication (MFA). We can use any of these following methods to approve the login request.

* Email or SMS codes
* Text and call one-time passwords (OTPs)
* Biometric verification
* Security key
* Authenticator app

*Ref.* [*https://www.itsasap.com/blog/types-of-mfa*](https://www.itsasap.com/blog/types-of-mfa)