# Week 3 Hands On

Eric Vara

The University of Arizona Global Campus

CYB 300

Instructor Bipin Bhatt

28, November 2022

## Part One

### Module 03: Information Security Management Review Questions

1. How do the InfoSec management team’s goals and objectives differ from those of the IT and general management communities?
   * Answer: This includes managing information security requirements. The underlying goal is to address all potential threats and vulnerabilities. Its main purpose is to protect your organization's sensitive data. All risks and opportunities that may lead to loss of confidentiality and integrity are considered. A thorough understanding of how security breaches occur, how to avoid destructive events, and how to protect yourself can help minimize risk. It also deals with the implementation of all systemic regulatory measures.
2. What is included in the InfoSec planning model?
   * Answer: Information security planning includes planning for incident response, business continuity, disaster recovery, policies, staffing, technology adoption, risk management, and security programs.
3. List and briefly describe the general categories of information security policy.
   * Answer: Information security policies fall into three broad categories.
   * (a) general or security program policies (also known as security program policies); (b) Topic-Specific Security Policy. (C) System Specific Security Policy. An organization's overall information security policy is called an overall or security program policy.
4. Briefly describe strategic planning.
   * Answer: Leaders of a company develop their future vision and determine their organization's goals and objectives through the process of strategic planning. Establishing the order in which these objectives should be accomplished can help the organization attain its stated vision.
5. List and briefly describe the levels of planning.
   * Answer: Strategic, tactical, and operational plan types can all be used to help managers achieve organizational goals. Operational plans help realize tactical plans that help realize strategic plans. An administrator should create these three different types of plans plus a backup plan in case the primary plan fails.
6. What is governance in the context of information security management?
   * Answer: Management ensures that controls are in place to mitigate risk, while governance sets the accountability framework and provides oversight to ensure that risk is appropriately mitigated. Your administrator will suggest security measures.
7. Describe the critical characteristics of information. How are they used in the study of computer security?
   * Answer: Information`s value is determined by its essential properties. The value of the information itself can be altered by changing any one of its qualities. There are seven informational traits. Accessibility and accuracy the qualities of authenticity, confidentiality, integrity, usefulness, and possession.
8. What are the differences between a policy, a standard, and a practice? Where would each be used?
   * Answer: Policy: A set of rules outlining acceptable conduct. Standard - Explanation in detail of what must be done to adhere to policy. Practice: Illustrations of conduct that complies with law.
9. What is an EISP, and what purpose does it serve?
   * Answer: An enterprise information security program is NIST SP 800-14. (EISP). The scope, tone, and strategic direction of a corporation, including all security-related matters, are determined by the EISP. The objectives and mission of the organization should be clearly expressed in this policy.
10. Who is ultimately responsible for managing a technology? Who is responsible for enforcing policy that affects the use of a technology?
    * Answer: Employees who oversee the development, review, distribution, and storage of an organization's policies are called policy administrators.
11. What is needed for an information security policy to remain viable?
    * Answer: An information security policy should: Protect all organizational end-to-end security procedures. Be realistic and enforceable. Be frequently updated in response to changing threats and business needs.
12. How can a security framework assist in the design and implementation of a security infrastructure? What is information security governance? Who in the organization should plan for it?
    * Answer: Using a security framework makes your security strategy clearer. Learn more about how to implement security in your enterprise. Appropriate strategies can be extracted and applied using different frameworks. The framework provides a roadmap for necessary improvements. Tasks to be completed and necessary adjustments can be evaluated using the framework. This simplifies your security strategy.

The process of managing multiple security measures is known as information security governance. This includes protecting information and implementing numerous policies and procedures to provide information security. This includes ensuring safety. The corresponding tasks should be monitored and protected.

Information security governance must be planned by the organization's top management, including officers and managers. We need to ensure that the task is executed and effectively completed.

1. Where can a security administrator find information on established security frameworks?
   * Answer: Security administrators can use many well-known security frameworks, including the Information Technology Code of Practice for Information Security Management, ISO 17799/BS 7799 and ISO 17799/BS 7799, the NIST security model including SP 800-12. can refer to 14, 18, 26, 30 and VISA international security models.
2. What is the ISO 27000 series of standards? Which individual standards make up the series?
   * Answer: There are 46 distinct standards in the ISO/IEC 27000-series, including ISO 27000. Its foundation is ISO 27001, which describes the conditions for putting an ISMS into place. The sole ISO 27000 series standard that businesses can be audited and certified against is ISO IEC 27001:2013.
3. What documents are available from the NIST Computer Security Resource Center (CSRC), and how can they support the development of a security framework?
   * Answer: A number of resources available from the National Institute for Standards and Technology's Computer Security Resource Center describe additional strategies. (http://csrc.nist.gov) These documents were among the documents emphasized by the federal government in making its decision not to use the ISO.IEC 17799 standard. The sections below consider these documents in the context of information security planning. SP 800-12, 800-14, 800-18, 800-26, 800-30
4. What Web resources can aid an organization in developing best practices as part of a security framework?
   * Answer: The US government website fasp.nist.gov provides security guidelines and best practices.
   * Technology Manager Forum website (www.techforum.com);
   * Information Systems Audit and Control Association and Information Security Forum website (www.isfsecuritystandard.com) (www.isaca.com)
   * Website for Professional Security Consultants (www.iapsc.org)
   * Global Grid Forum website
   * Visit the Internet Security Task Force website (www.ca.com/ISTF) to see parties concerned with Internet security.
   * Modules with connection and security instructions are available on the Computer Emergency Response Team website (www.cert.org).
5. Briefly describe management, operational, and technical controls, and explain when each would be applied as part of a security framework.
   * Answer: Operations management addresses operational security within an organization, such as incident response and disaster recovery. It also includes personal protection, physical protection, and protection of manufacturing inputs and outputs.
   * Technical controls address tactical and technical issues related to developing and implementing security within an organization and evaluating and selecting appropriate technology for information protection. Logical access controls such as identity, authorization, accountability, and authentication fall into this category.
6. What is defense in depth?
   * Answer: Defense in depth is essentially a network security protection method that thwarts attackers by layering or deploying a series of security measures in sequence. This hierarchy provides multiple redundancies should a system or data be compromised. Defense in depth means that when one layer of security is compromised, numerous other layers of security will ambush, greatly increasing the difficulty of a full-scale breach.
7. Define and briefly explain the SETA program and what it is used for.
   * Answer: SETA is a program designed to help organizations reduce the frequency of security breaches caused by human error. To avoid security breaches, people should be aware of information security rules and be able to apply them in their daily lives.
8. What is the purpose of the SETA program?
   * Answer: For over 40 years, SETA has transformed lives through effective programs to help people achieve their work and life goals. Our strategy is holistic.
   * We support independence by responding to all needs, such as childcare, education, and training.
9. What is security training?
   * Answer: IT and security professionals use security awareness training as a strategy to reduce and prevent user risk. These initiatives are designed to help users and employees understand their role in preventing information security breaches.
10. What is a security awareness program?
    * Answer: The CISA Cybersecurity Awareness Program is a nationwide campaign to raise public awareness of cybersecurity issues and provide Americans with the knowledge and tools they need to stay safer online. Security in the digital space is a collaborative effort. We all need to do our part to keep the internet safe.

### Module 04: Risk Management Review Questions

1. What is risk management?
   * Answer: Risk management involves identifying, evaluating, and prioritizing risks in order to reduce the likelihood or impact of adverse events, monitor and control them, or maximize the realization of opportunities. This is followed by coordinated and efficient use of resources.
2. According to Sun Tzu, what two things must be achieved to secure information assets successfully?
   * Answer: Organizations need to understand themselves (including their resources and the processes used to protect them) and their adversaries in order to mitigate risks (the types of threats they face).
3. Which community of interest usually takes the lead in information asset risk management? Which community of interest usually provides the resources used when undertaking information asset risk management?
   * Answer: Information asset risk management is typically managed by management. The process of identifying potential risks and threats to the organization should be initiated by the administrator.
4. In risk management strategies, why must periodic reviews be a part of the process?
   * Answer: All hardware components are already identified by model, brand, and location, so an automated asset inventory system can help with the risk identification process.
5. What value would an automated asset inventory system have for the risk identification process?
   * Answer: Since all hardware components are already identifiable by model, brand, and location, automated inventory systems aid in the risk detection process. This allows administrators to assess the system's most important components.
6. Which is 5 2 the information asset classification scheme: that it be comprehensive or that it be mutually exclusive?
   * Answer: This indicates that all assets are covered even if they appear in multiple places, so it is desirable to thoroughly classify the information.
7. What is the difference between an asset’s ability to generate revenue and its ability to generate profit?
   * Answer: Even if some assets are able to operate and generate income, they cannot be profitable after expenses are paid.
8. Describe the TVA worksheet. What is it used for?
   * Answer: The TVA worksheet is a combination of your organization's top threats list and top assets and vulnerabilities list. The resulting grid provides a convenient way to view the 'exposure' of your assets, allowing for quick vulnerability analysis.
9. Examine the simplest risk formula presented in this module. What are its primary elements?
   * Answer: Probability of loss, value at risk, percentage of potential loss already managed, and tolerance for uncertainty are key elements of risk estimation.
10. What is competitive advantage? How has it changed in the years since the IT industry began? What is competitive disadvantage? Why has it emerged as a factor?
    * Answer: Competitive advantage is achieved when an organization develops business strategies, methods, or techniques that enable it to offer goods and services superior to those of its competitors. Competitive advantage was more prevalent in the early days of IT system development. Companies are still using the same degree of automation today.
11. Describe the strategy of risk transfer.
    * Answer: Pure risk is contractually transferred from one party to another as part of the risk management and control process.
12. Describe the strategy of risk mitigation.
    * Answer: Organizations can use risk mitigation as a technique to prepare for potential hazards and reduce their impact. Risk mitigation, like risk mitigation, requires actions to reduce the negative impact of risks and disasters on business continuity (BC).
13. Describe residual risk.
    * Answer: Risk that exists after efforts have been made to identify and mitigate some or all types of risk. The remaining risks are significant for several reasons. Remaining risks after applying security controls and process improvements should be the first consideration.
14. What are the three common approaches to implement the mitigation risk treatment strategy?
    * Answer: The three most prevalent strategies are technology implementation, policy enforcement, and education and training enforcement.
15. Describe how outsourcing can be used for risk transfer.
    * Answer: If a company chooses to hire an ISP or consulting firm for goods and services such as server acquisition and configuration, web development, maintenance, administration, or even InfoSec capabilities, outsourcing can be used to transfer risk. increase. This allows companies to offload the risks associated with managing these complex systems to companies with the relevant expertise.
16. What conditions must be met to ensure that risk acceptance has been used properly?
    * Answer: An asset's risk level is determined, the probability of an attack and the probability of successful exploitation of a vulnerability is assessed, the annual frequency of such attacks is roughly calculated, the outcome of an attack is estimated, and a thorough cost estimate is made. increase. Risk acceptance is properly deployed when a benefit analysis is performed, and the controls are evaluated using their respective appropriate feasibility types.
17. What is risk appetite? Explain why risk appetite varies from organization to organization.
    * Answer: Risk appetite is the level of risk an organization wants to consider when weighing the benefits of perfect security versus perfect accessibility. Different companies have different risk tolerances due to differences in size, spending, culture, and the importance of certain assets.
18. What is a cost-benefit analysis?
    * Answer: A cost-benefit analysis compares the potential benefits (avoided losses) and potential costs (costs required to implement controls) of control efforts.
19. What is the difference between intrinsic value and acquired value?
    * Answer: Intrinsic value is the asset`s fundamental worth, whereas acquired value is the added value that some information assets accrue over time.
20. What is single loss expectancy? What is annualized loss expectancy?
    * Answer: The estimate that corresponds to the single instance of loss that is most likely due to an attack is called the Single Loss Expectancy (SLE). The calculated number corresponding to the annual loss from the most probable attack is called the Annual Expected Loss (ALE). Multiplying the SLE by the estimated annual number of occurrences yields the ALE.
21. What is a qualitative risk assessment?
    * Answer: Analyzing potential risks and their impact on a project is the process of qualitative risk assessment. In addition to identifying key risk areas and increasing awareness of project hazards, it helps project managers prioritize risks by likelihood and impact.

## Part Two

### Hands-On Project: Windows Password Management

Complete the Hands-On Project: Windows Password Management

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

Please share your experiences in using the Widows Password Management system.

|  |
| --- |
| I leanred a lot using the windows password management system. I found that the different privileged accounts on the network need to be identified and consolidated in order for the Windows infrastructure to implement an efficient password management mechanism. The local admin and domain admin accounts are quickly and easily found by Password Manager Pro's discovery features, and they are then added to the inventory. By identifying the various Windows server components that are executed using domain accounts and associating the services and scheduled activities with the appropriate accounts, it also aids in the discovery of service accounts. |

Please share your experiences in exploring the Windows Password Policies:

|  |
| --- |
| I discovered some interesting information regarding password policy implementation and best practices considerations, policy location, default values for the server type or GPO, relevant differences in operating system versions, security considerations (including the potential vulnerabilities of each setting), countermeasures that you can take, and the potential impact for each setting. |

### Hands-On Project: Malware Defense

Complete the Hands-On Project: Malware Defense

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

Please share your experiences in installing the antivirus software program.

|  |
| --- |
| It was excellent. It was rather boring at first because it takes longer to install, but it was quite wonderful after installation. It displays a warning notice if a drive with corrupted files is inserted, stating that it may contain hazardous files. |

Did your scan reveal any malware operating on your computer? If yes, please describe.

|  |
| --- |
| No, there was nothing in my PC after installing antivirus software. My machine contains no malware. |

Did your scan reveal any malware operating on your computer? If yes, please describe.

|  |
| --- |
| Yes, there was malware or virus on my computer before I installed antivirus software. As a result, the computer lags frequently. Tasks take much longer than usual to resume or complete. It may say that this file cannot be opened because some of the files are corrupted. Therefore, I installed antivirus software to protect my files from corruption and virus infection. |

Were you able to install and run SpyBot Search and Destroy? If yes, describe the results of your scan.

|  |
| --- |
| Installing antivirus software adds an important second layer of protection to your machine or network. I have verified that I have obtained my antivirus software package from a trusted source. I made sure no other programs were running during the antivirus installation. Went online to get more files and updates. After the installation is complete, restart your computer and update the program. The file you downloaded is most likely not the latest version, so you need to log into your antivirus server and download the latest updates. |

Please share your experiences in using the Windows AntiVirus solution. Did it find malware undiscovered by the earlier programs?

|  |
| --- |
| Experience with Windows antivirus software and other antivirus software has been mostly positive. However, Windows Antivirus is more adaptive and efficient than its predecessor. |