Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
	100%

Report Generated: Saturday, September 14, 2024 at 12:06 PM

Guided Exercises

Part 1: Research the NIST Risk Management Framework

4. **Explain** Figure 1: Organization-wide Risk Management Approach.

Organization-wide risk management theory is used by an organization to develop, implement, and maintain a broad organizationally accepted adoption of a security and privacy risk management framework and life cycle. Adoption and buy-in at levels 1 and 2 are critical to the approach's success. These levels prepare the entire organization for a successful execution of the framework. This framework prepares for an organizational culture change to implement risk management. It focuses on the mission and business processes along with the senior executives' vision, objectives, and goals. Mid-level management outlines, executes, and manages projects. Resources, roles, and responsibilities are structured and allocated at these levels. The organization's risk appetite is established, and business processes are identified. At this stage, assets and threats are identified, risk assessments are completed, requirements are established, boundaries are identified, enterprise architecture is identified, and allocating requirements are completed. Level 3 is the information system perspective and derives guidance from levels 1 and 2. Level 3 is focused on the development, implementation, operation, and maintenance of the actual information systems. All three levels create the concept of a holistic structure to this framework, all working together and flowing, creating a mature risk management model. During the risk management framework outlined, traceability is established. Traceability verifies requirements are implemented according to all levels of the hierarchy.

6. Briefly **explain** two of the items from the preparation list.

One preparation item is identifying the missions, business functions, and mission/business processes the information system is intended to support. The focus is determining the functional support the information system provides the company. How does the IS support the mission? How does the IS support each identified and /or critical business function? How does the IS support business processes, such as accounts payable and receivable or transaction storage for a website? Answering these questions assists in identifying this preparation item.

Another preparation item is determining authorization boundaries for information systems and common controls. Here, the framework identifies the scope of responsibility and the control range. These are the system elements defining the system or a set of controls to adopt. The process includes identifying system components, grouping related systems, and determining how systems interact.

8. **Provide** a reason why you think the risk decisions at Levels 1 and 2 can impact the selection and implementation of controls at the System level.

The decisions developed at levels 1 and 2 are the preparation stages for any execution at level 3. Risk management decisions at levels 1 and 2 guide and inform level 3. Any controls implemented at level 3 were directly impacted by the decisions made at levels 1 and 2. Without levels 1 and 2, level 3 activities can fall out of scope with CBA and personnel and create solutions that do not provide the most effective controls.

10. **Summarize** Figure 2: Risk Management Framework.

The Risk Management Framework has seven steps: six main steps and one preparatory step. All steps are required. The steps are prepare, categorize, select, implement, assess, authorize, and monitor. The RMF is applied at the three levels of the risk management hierarchy: Organization, Mission/Business Process, and Information System.

12. Briefly **explain** why the Monitor step is needed. **Provide** two examples of what the Monitor step should cover.

The monitor step is needed to support risk management decisions. It provides ongoing situational awareness of the information systems' and organizations' security and privacy posture.
One key aspect of the Monitor step is the ongoing assessments, as defined in task M-2. These involve continuously evaluating the effectiveness of controls and reporting the evaluation to senior leaders. The use of automation tools significantly increases the quality and accuracy of these assessments, providing senior leaders with reliable information for decision-making.
Another critical aspect of the Monitor step is authorization package updates, as defined in task M-4. Derived from the continuous monitoring processes, the organization updates security and privacy plans, security and privacy assessment reports, and POAMs to achieve near real-time risk management. Automation tools assist in access to current reports. This step raises awareness of the organization's posture. The integrity of the information contained within this step is ensured. Tracking changes to systems is necessary. Individual accountability is outlined, and an understanding of emerging trends is discussed.

14. **Select** one of the 18 preparation tasks and briefly **explain** that specific task.

The Risk Assessment—System is located at the system level, Task P-14. At this task, a system-level risk assessment is conducted, and the risk assessment results are updated on an ongoing basis. The primary responsibility is assigned to the system owner, system security officer, or system privacy officer. Supporting roles can include the business owner, information owner, or system security officer.

16. **Select** one associated title (for example, Head of Agency, Authorizing Official, Business Owner) and **identify** at least two of their main duties related to the task you selected.

One associated title is the System Security Officer. The System Security Officer protects information and information systems' confidentiality, integrity, and availability from unauthorized activity or behavior. The System Security Officer is also a principal advisor on all matters, technical and otherwise, involving the controls for the system.

18. **Select** one associated title and **identify** at least two of their main duties related to the task you selected.

From the support roles field, the Mission or Business Owner has a security or privacy stake in the organizational systems supporting the business. They are key stakeholders, having a significant role in establishing and maintaining the protection and security of the organization's mission and operations. They provide essential input for the risk management process and may serve as an authorizing official.

Part 2: Create a Risk Management Plan

2. **Select** one task from Table 1 on page 28 and **describe** how the task could help Acme achieve its goal of creating a robust risk management plan.

Organizational risk assessment, as defined in Task P-2, is a risk management strategy that determines organizational risk tolerance. To comply within the scope of a PCI DSS compliance risk assessment, an organizational-wide security and privacy risk assessment will identify the information systems and processes needing compliance. The inputs used for this task will include a strategy, business objectives, current identified threats, system-level assessments, and supply chain assessments. A review of information-sharing agreements or MOUs with any PCI DSS-related vendors or third parties. The use of any previous assessments may help identify threats. Updating the risk assessment results on an ongoing basis will ensure PCI DSS compliance consistency. The totality of risk from the operation and use of information systems, internally or externally owned, and any external providers of services or processes will be considered. These inputs and the aggregated information from system-level assessments and continuous monitoring will result in an organizational-level risk assessment for PCI DSS compliance.

5. In the context of the recent PCI DSS audit findings at Acme Corporation, **identify** a clause that describes the assets requiring protection.

“The assets that require protection are identified based on stakeholder concerns and the contexts in which the assets are used.”
Assets requiring protection can be tangible and intangible, each providing unique value to achieving mission and business objectives. Tangible assets, such as user accounts (software), are crucial for operations. However, the lack of management of these accounts (human and processes/functions) poses a significant risk. Similarly, technical vulnerabilities with physical servers (machine elements/software) need to be addressed to ensure the continuity of operations.

8. **Describe** the system at Acme Corporation that was audited recently.

Acme’s account management system processes credit cards using a PCI DSS standard. The system consists of servers and user computers in a Windows architecture environment running a Windows domain controller and Windows desktop operating systems.

11. **Describe** two controls that could help mitigate the findings in the PCI DSS audit. One control should be in the information system tier and one control should be in the Organization or Mission/Business Process level.

The Windows domain controller and user computers should actively maintain user accounts. One information system control assigns a team to discover inactive user accounts and deactivate or delete them. Another control in the business process category implements a policy that applies responsibility for continuous vulnerability scanning and mitigation for critical servers.

14. **Describe** how the two controls you selected should be implemented.

Implementation of a team to discover inactive user accounts and deactivate or delete them starts with identifying personnel with an assurance requirement in responsibility, skill, and training to accomplish the mitigation strategy while maintaining consistency with the enterprise architecture. An initial control assessment will be conducted during the implementation of this team to identify appropriate skills, identify any deficiencies, and provide cost-effective corrective actions if any deficiencies are identified.

Implementing a policy to assign responsibility for continuous vulnerability scanning and mitigation for critical servers starts with an assurance requirement in the policy's design, development, and implementation. The policy should adhere to best practices and industry standards. An assurance requirement will also be for training and adherence to the policy. An initial control assessment will be conducted during the implementation of this policy to ensure clarity and that the policy's objectives are being met, identify any deficiencies, and provide cost-effective corrective actions if any deficiencies are identified.

17. Which Assess task should you follow after completing Task A-3? **Specify** the code and name of the task from Table 6 on page 61.

TASK A-4
ASSESSMENT REPORTS

20. **Assume** the role of a top-level manager. What authorization decision would you make and why?

After reviewing the information in the audit findings, control implementation information, control selections, and the assessment report, the authorization decision is authorized to operate. Ongoing authorization is granted with a continuous monitoring strategy as long as it remains acceptable. The reasoning for this is based on the mitigation solutions aligning with the organization's risk tolerance and lowering the residual risk to an acceptable level.

22. **Think** about the vulnerability of a lack of account management procedure. Which monitor tasks would you suggest to monitor the implementation of this control and the authorization of the implementation? Who would be the responsible parties for these tasks?

Implementing Task M-2 Ongoing Assessments will provide a continuous monitoring strategy to give feedback on the effectiveness of the account management procedures. This will also provide input for ongoing authorization of operation and implementation. The control assessor would hold primary responsibility with supporting roles coming from the Authorizing Official or Authorizing Official Designated Representative; System Owner or Common Control Provider; Information Owner or Steward; System Security Officer; System Privacy Officer; Senior Agency Information Security Officer; Senior Agency Official for Privacy.

Challenge Exercise

Carefully review this report and **identify** two vulnerabilities from different organizational levels, such as one vulnerability from Level 3 and one vulnerability from Level 1 or 2.

One vulnerability identified from level 2 is a lack of an asset inventory policy. In 2015, Equifax had not completed a comprehensive IT asset inventory and failed to document its network accurately. An organization can only defend the assets it's aware it operates and maintains. Equifax was unaware of this vulnerable Struts server because of a lack of inventory reports. When the breach occurred in July 2017, no inventory had been completed. It wasn't until August 2017 that the Struts server was patched, which was due to a lack of comprehensive, timely, and ongoing inventory reports. At the time of the breach, in late July 2017, there was no complete inventory in place.

Another vulnerability identified from level 3 that allowed for deeper penetration into Equifax's systems was due to a lack of network segmentation. A failure to segment its network resources permitted the hackers to access credentials for other databases and applications due to Equifax employees having saved credentials on a file share that was discovered and exploited so the attackers could move across the network laterally. Network segmentation would have restricted this access to these other systems and databases and detained the attackers within the dispute portal. Equifax allowed this failure of network segmentation based on business operations and functionality needs over industry-standard security protocols.

Now think about the seven steps of the RMF. **Summarize** how these steps could have helped Equifax prevent or mitigate the vulnerabilities you identified. **Identify** at least one step for each vulnerability.

The Select step could have mitigated the vulnerability of Equifax's failure to have an asset inventory policy. Equifax could have selected an initial asset inventory policy and tailored the policy as needed to reduce risk to an acceptable level by allowing for the complete identification of all systems, specifically the exploited Struts server. This most likely would have allowed for the notification to the software developer who was aware that Equifax ran vulnerable versions of Apache Struts who never received the GTVM alert because the distribution list used to disseminate it did not include all application owners.

The Implement step could have mitigated the failure of Equifax to properly segment its network based on industry-standard security protocols. Completing the Implement step would have implemented the appropriate security segmentation protocols and documented how the segmentation is employed and the environment it operates within. Successful adoption of the Implement step for network segmentation protocols would have reduced the potential for the attackers to laterally access other databases within Equifax's network to an acceptable level of risk.