Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

Time on Task:	Progress:
Unknown	100%

Report Generated: Monday, July 7, 2025 at 9:38 PM

Guided Exercises

Part 1: Research the NIST Risk Management Framework

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

Figure 1 demonstrates a tiered strategy for managing risk that tackles security and privacy risks at the organizational level, the mission/business process level, and the level of information system. Communication and reporting involve two-way exchanges of information throughout the three tiers to guarantee that risk is managed across the organization.

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

1. •Assigning roles and responsibilities for organizational risk management processes. This means that when preparing the organization for RMF execution, everyone should be delegated a role and task to do to ensure maximum level of efficiency and to make sure there aren't too many people being allocated to do the same thing.2. Identifying key stakeholders (internal and external to the organization) that have an interestin the information system. This is important because the higher ups in the company should be informed that there is a situation at hand. Once they are informed they can make decisions such as how much money will be delegated to the issue at hand.

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.

Without adequate risk management preparation at the organization level, security and privacy activities can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions. So if the risk decision at level 1 and 2 is not good, it sets up level 3 for failure as level 3 addresses risk from an information system perspective and is guided and informed by the risk decisions at the organization and mission/business process. levels.by the risk decisions at the organization and mission/business process levels

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

Figure 2 is all the steps in the RMF. First should be to prepare, then the 6 main steps follow after. The steps following the prepare can be done in any order, hence why the arrows points in all directions. Once the preparation is done, the six main steps is to prepare, categorize, select, implement, assess, authorize, and monitor, which can be done in any order, although organizations executing the RMF for the first time for a system or set of common controls typically carry out the remaining steps in this sequential order

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

The monitor step is needed so you can maintain an ongoing situational awareness about thesecurity and privacy posture of the information system and the organization in support of riskmanagement decisions, essentially meaning to watch what is happening. One example of what the monitor steps should cover is system and environment changes, meaning that the system and environment changes are monitored in accordance with the continuous monitoring strategy. Another example is ongoing assessments of control effectiveness, which are also conducted in accordance with the continuous monitoring strategy.

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

Task P-1:
Risk Management Roles: "Identify and assign individuals to specific roles associated with security and privacy risk management." Everyone should be delegated a role to ensure maximum level of efficiency, and so it's organized and not everyone working on the same problem. Everyone should be working on something different based on their skillset and experience to speed it up.

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.

Chief Information Officer:
Relating to risk management roles, they oversee personnel with significant responsibilities for security and ensuring that the personnel are adequately trained. They ensure that an organization-wide security program is effectively implemented resulting in adequatesecurity for all organizational systems and environments of operation

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

Senior Accountable Official for Risk Management:
The senior accountable official for risk management determines the organizational structure and responsibilities of the risk executive (function), and in coordination with the head of the agency, may retain the risk executive (function) or delegate the function to another organizational official or group. They are also the individual that leads and manages the risk executive (function) in an organization and is responsible for aligning information security and privacy risk management processes with strategic, operational, and budgetary planning processes

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.

P-1 Risk management roles:
They can achieve their goal of creating a robust risk management plan by finding the best individuals for a certain task and assign key roles to execute the risk management framework. This would ensure that the best are in each role and everyone has a role to get the situation under control as soon as possible.

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

Information assets can be tangible or intangible assets, and can include theinformation needed to carry out missions or business functions, to deliver services, and for system management/operation; controlled unclassified information and classified information; and all forms of documentation associated with the information system

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

The audited system at Acme Corporation is in the Operations/Maintenance phase, supporting key business processes and integrating into the enterprise architecture. It includes detailed documentation of its components, users, network connections, and security measures, which is updated regularly to address risks and changes.

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.

A baseline control selection approach, or an organization-generated control selection approach can be used. The baseline control selection approach uses control baselines, which are pre-defined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. These baselines serve as a starting point for the protection of individuals' privacy, information, and information system. Another control would be a privacy risk assessment. This assessment along with privacy requirements derived from stakeholder protection needs, laws, executive orders, regulations, policies, directives, instructions, and standards (see Task P-15) helps inform the selection of privacy control baselines.

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

Baseline Control Selection:
Organizations use best practices when implementing controls, including systems security and privacy engineering methodologies, concepts, and principles. The tests, evaluations, and validations consider products in specific configurations and in isolation; control implementation addresses how the product is integrated into the system while preserving security functionality and assurancePrivacy Risk Assessment:Risk assessments guide and inform decisions regarding the cost, benefit, and risk trade-offs in using different technologies or policies for control implementation. Risk assessments may determine how gaps in security or privacy requirements between systems and common controls affect the risk associated with the system, and how to prioritize the need for compensating or supplementary controls to mitigate specific risks

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 from Table 6 on page 61 of NIST SP 800-37 Revision 2

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

The authorization decision is conveyed by the authorizing official to the system owner or common control provider, and other organizational officials, as appropriate.The decision conveys the terms and conditions for the authorization to operate; the authorization termination date or time-driven authorization frequency; input from the senior accountable official for risk management or risk executive (function), if provided; and for common control authorizations, the system impact level supported by the common controls. As a top-level manager I would authorize the system to operate under strict surveillance and ongoing monitoring so there would be a balanced risk management and to mitigate threats effectively

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?

Task M-1 and M-2 should be suggested to monitor the implementation of this control and the authorization of the implementation. M-1 would monitor what changes in the system and environment, specifically what would impact account management. M-2 should be used to assess the effectiveness of account management controls as part of a continuous monitoring strategy.

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.

A level two vulnerability:
Equifax lacked a comprehensive IT asset inventory. "The audit report also noted that Equifax lacked a comprehensive IT asset inventory, meaning it lacked a complete understanding of the assets it owned. This made it difficult, if not impossible, for Equifax to know if vulnerabilities existed on its networks." This is level 2 because it was an operational flaw in asset managment that led to vulnerabilities
Level 3:
The usernames and passwords the hackers found were saved on a file shared by Equifax employees. Equifax told the Subcommittee that it decided to structure its networks this way due to its effort to support efficient business operations rather than security protocols. This is level 3 because security was overlooked in favor of operational efficiency.

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.

Level 2 risk: Lack of Comprehensive IT Asset Inventory
Categorize - If Equifax had categorized all IT assets, it would have been easier to track and prioritize the assets for vulnerability management based off importance. Categorizing them would help show the sensitive systems that need immediate attention to ensure they're securedAssess - Regular vulnerability assessment would allow Equifax to see the systems weakness. It would shows which systems are exposed to threats, allowing them to get to it before its gets exploited
Level 3 risk: Storing usernames and passwords on a shared file
Select - During this phase Equifax could have implemented a stronger security control for sensitive information such as usernames and passwords. This could have been MFA, encryption or access control policies. This would keep the usernames and passwords safe even if they were compromisedMonitor - Continuous monitoring could be put on sensitive information, so if the information got compromised they would be alerted. This would let them get to the threat as early as possible.