Student:	Email:
Kaleb Alstott	alstottk1@mymail.nku.edu

Time on Task:	Progress:
	100%

Report Generated: Sunday, October 3, 2021 at 7:51 PM

Guided Exercises

Part 1: Research the NIST Risk Management Framework

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

In figure one we have a board base risk perspective that takes place in three different tier levels. This is an overall diagram that address security and privacy risk. Level one being organization level, level two being the mission/business process level, and the last third tier which is the information system level. Communication and reporting are both bi-directional. The information continuously goes across the three tiers to ensure that risks can be addressed properly.

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

• Assigning roles and responsibilities for organizational risk management processes In this scenery we would be assigning roles and responsibilities for our risk management process. For this we could be assigning roles to specific positions such as a risk team management leader and what they would do. We could also assign more specific roles such as IT management, financial organizer, employee trainer to train employees, etc. • Identifying key stakeholders (internal and external to the organization) that have an interest in the information system In this process we would take a step back and analyze who is buying into our company and who is investing in us. Once we have separated out who invests into our company and who our company is effected by we can separate them into stakeholders of the company and properly inform and manage correctly during the RMP.

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.

I think the reason why the risk decisions at Levels 1 and 2 can impact the selection and implementation of controls at the System level is because, at levels 1 and 2 this is the base of the system levels and anything that is modified or affected at these levels will have a continues effect on the next levels and steps you have to take.

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

Overall the figure is actions taken in the RMP. There is no start or finish to this diagram but yet a continuous cycle. You can start wherever in this cycle but before you do the overall goal you must achieve is the preparation for whatever cycle step you are about to employment. Overall this diagram is demonstrating the risk management plan framework.

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

The monitor step is needed and is a necessity because this is the step that provides feedback from your RMP. The monitoring step is key to finding environmental changes, technical, and flaws in your system. Two examples of what the monitor step should cover is, continuous monitoring on documentation, and "the output of continuous monitoring activities is analyzed and responded to appropriately."

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

TASK P-12 Information Types To identify the types of information to be processed, stored, and transmitted by the system. System design documentation, assets to be protected, mission/business process information, and system design documentation.

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.

System Owner- two of the main duties a system owner may do is developing a system and modification to a system. All systems need to have an owner and an overseer that responsibly monitors, process, integrate, modify, and dispose of a system properly.

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

Information owner or steward - Overall the main goal and two duties that are done here is that all data will have an owner who has to govern its generation, collection, processing, dissemination, and disposal in a safe and proper way.

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.

TASK P-1 RISK MANAGEMENT ROLES By assigning key roles for executing the RMP we have prepared Acme to be able to organize and communicate clear steps to groups or individuals inside his company. This is a huge step in the RMP due to the complexity of breaking assignments down and categorizing them specifically to a department or individual.

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

"For example, the Windows domain controller and user computers were discovered to contain multiple inactive user accounts." All of the information systems and services that contain user accounts is a strong enough clause to receive protection. You have to protect your current users and manage the correct users so your data is protected where need be.

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

Recently the Acme Corporation has undergone an internal PCI DSS audit. During this audit associated with the credit card process, critical vulnerabilities and risks were discovered. An example of one of these vulnerabilities discovered is inactive user accounts. "Ultimately, it was discovered that no individual or team is actively managing user accounts on Acme’s information 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.

To start a mitigation technique we can use in the information system level is to easily delete the inactive users accounts. This will prevent unknown or past users form gaining access to card information or payments that are not required by said users anymore. The second mitigation technique that we can use can be in the mission/business process level in which we would assign an individual or team to manage account activities. This will prevent us from having long term running accounts that are unneeded and that can be used as security threats.

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

I would start off by first by hiring someone to manage the user accounts that are unused. To do so we would look to the IT security manager and discuss the role needed and what skills are needed and start looking for a hire. Once we have found an individual for this assignment we then would implement a prevention system from stopping this from happening again and would also delete the unused accounts as part of the job. There should also be a monitoring on the accounts to be aware of how long ago accounts are created and when they will need new passwords or need to be removed.

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-5: Remediation Actions

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

Some authorization decisions id make would be authorization to operate, authorization to use, common control authorization, denial of authorization to operate, denial of authorization to use, denial of common control authorization. I would make these decisions due to the role of a top-level manager, as we can see it is very important to be able to the a protocol on all documentation or files.

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?

I think both Task M-2: Ongoing Assessments and Task M-6: Ongoing Authorization would be needed for this implementation and authorization. The task of the ongoing assessments would be fulfilled by an information security manager similar to the one I've talked about in the pervious questions. And the ongoing authorization would be handled and fulfilled by someone such as a security administrator, since you are defining and organizing authorization this needs to be a top level of management.

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 I found when reading through the document is lack of audits since the following year of 2015. " Equifax never conducted another audit after the 2015 audit and left several of the issues identified in the 2015 audit report unaddressed in the months leading up to the 2017 data breach.:" Another vulnerability I found that would be tier 3 would have been an Apache Struts which is a web application software "The company’s security staff learned of a critical vulnerability in certain versions of Apache Struts – a widely-used piece of web application software – on March 8, 2017, from the U.S."

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.

For vulnerability number 1 and the issue of lack of audits I would say to implement a monitoring and assessment steps to make sure that audits are being done correctly and yearly, there shouldn't be more than a years gap worth of audits. For vulnerability number 2 dealing with the Apache Struts, I would use a mitigation technique of a transfer and let a third party deal with the web application.