Final Project Scenarios

Task 1: Identify the critical elements of a GRC framework that Nerdnest needs to implement

This task consists of three questions and carries 9 points. Thoroughly review the scenario and answer the questions.

Scenario

Nerdnest has been expanding rapidly over the last two years, increasing its customer base and introducing new services. However, with this growth has come an uptick in cybersecurity threats. Recently, Nerdnest experienced a data breach that exposed sensitive customer information. The incident resulted in financial loss and damaged the company's reputation. Consequently, the leadership team at Nerdnest recognizes the urgent need to fortify their cybersecurity measures to protect against future attacks.

Previously, Nerdnest managed its cybersecurity through a patchwork of basic security controls and ad-hoc responses. However, the recent breach highlighted significant gaps, such as the lack of a comprehensive governance structure, insufficient risk assessment practices, and non-standardized compliance procedures. The company's stakeholders are now committed to developing a robust and cohesive cybersecurity framework that protects their digital assets and complies with relevant regulations.

To address these challenges, Nerdnest has decided to implement a Governance, Risk, and Compliance (GRC) framework as the foundation of its cybersecurity strategy. The leadership team believes that a well-defined GRC framework will provide the necessary oversight and structured approach to managing cybersecurity risks and ensuring compliance with legal and industry standards.

Task 1 questions:

1. Identify the key components Nerdnest should include in its Governance, Risk, and Compliance (GRC) framework to effectively align its processes with industry standards and regulations.
2. Explain how conducting a comprehensive risk assessment can help Nerdnest identify potential threats and vulnerabilities and align its risk management strategies with industry best practices.
3. Explain the importance of continuous monitoring in maintaining compliance with industry standards and regulatory requirements.

Task 2: Identify and apply the ITIL processes to Nerdnest

This task consists of four questions and carries 8 points. Thoroughly review the scenario and answer the questions.

Scenario

With the implementation of a GRC framework, Nerdnest's leadership team recognizes the need for an IT Service Management (ITSM) strategy to improve efficiency and align IT services with business objectives. To achieve this, they have adopted the Information Technology Infrastructure Library (ITIL) framework.

Task 2 questions:

1. Identify the key ITIL processes Nerdnest should incorporate into its ITSM strategy to align its services with business objectives. *Note: List all for full credit*
2. Explain how the adoption of ITIL can help Nerdnest streamline its IT service delivery and improve the overall quality of its services.
3. Explain the importance of Change Management in ensuring implementation of changes to IT services is done in a controlled and efficient manner.
4. Explain how Nerdnest can incorporate Change Management into its ITIL framework.

Task 3: Identify and apply laws related to Nerdnest's operations

This task consists of three questions and carries 6 points. Thoroughly review the scenario and answer the questions.

Scenario

As Nerdnest expands its business operations, compliance with relevant cybersecurity laws and regulations is crucial. Failure to comply can result in hefty fines, legal consequences, and company reputation damage.

Nerdnest has its headquarters in San Francisco, California, which places the company under the jurisdiction of both federal and state cybersecurity laws and regulations. Being based in the United States, Nerdnest must comply with various federal regulations depending on the nature of its business operations, such as:

- The Sarbanes-Oxley Act (SOX)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Federal Information Security Management Act (FISMA)

In addition, California's stringent data privacy and protection laws, such as the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), also

apply to Nerdnest.

Understanding and adhering to these laws is crucial for maintaining compliance, avoiding legal repercussions, and protecting the company's reputation in the marketplace.

Task 3 questions:

1. Explain the role of the Sarbanes-Oxley Act (SOX) in regulating Nerdnest's financial reporting and internal controls.
2. Describe how the Health Insurance Portability and Accountability Act (HIPAA) requirements impact Nerdnest's handling of sensitive healthcare information and the measures that must be implemented to comply with these regulations.
3. Explain how the CCPA and CPRA requirements impact Nerdnest's collection, use, and sharing of personal information.

Task 4: Identify the benefits of conducting regular cybersecurity audits and explain how Nerdnest can prepare for an audit

This task consists of two questions and carries 7 points. Thoroughly review the scenario and answer the questions.

Scenario

Regular cybersecurity audits are essential for ensuring the effectiveness of security controls, identifying vulnerabilities, and maintaining compliance with laws and regulations. For a company like Nerdnest that handles sensitive data, audits are crucial for instilling confidence in clients, investors, and other stakeholders.

Task 4 questions:

1. Explain the benefits of conducting regular cybersecurity audits for Nerdnest.
2. Describe the preparations Nerdnest can make to ensure a successful cybersecurity audit.