Final Project – Nerdnest Cybersecurity Strategy

Task 1: Governance, Risk, and Compliance (GRC)

1. Key Components of a GRC Framework for Nerdnest:

- Governance: Establish clear roles, responsibilities, and decision-making structures. Implement oversight from senior leadership and formalize cybersecurity policies and procedures.
- Risk Management: Develop a risk management plan including risk identification, analysis, response strategies, and risk monitoring.
- Compliance: Ensure alignment with relevant regulations (e.g., SOX, HIPAA, CCPA). Conduct regular audits and gap assessments.
- Policy Management: Create and maintain policies for acceptable use, data protection, and incident response.
- Training and Awareness: Implement ongoing staff training to reinforce the importance of cybersecurity practices and compliance obligations.
- Monitoring and Reporting: Continuously monitor risk indicators and compliance metrics, and report findings to stakeholders.

2. Importance of Comprehensive Risk Assessment:

- Helps Nerdnest identify internal and external threats (e.g., phishing, insider threats, misconfigurations).
- Pinpoints vulnerabilities across systems, networks, and procedures.
- Aligns cybersecurity investments and controls with industry best practices and business risk tolerance.
- Enables prioritization of mitigation efforts and improves incident response readiness.

3. Importance of Continuous Monitoring:

- Detects anomalies, intrusions, or compliance violations in real-time.
- Ensures up-to-date reporting for regulatory audits and internal review.
- Maintains alignment with evolving industry standards and threat landscapes.
- Strengthens Nerdnest's ability to proactively address security gaps before they become

critical.

Task 2: ITIL Processes

1. Key ITIL Processes for Nerdnest:

- Incident Management
- Problem Management
- Change Management
- Service Request Management
- Configuration Management
- Service Level Management
- Capacity Management
- Availability Management

2. Benefits of ITIL Adoption:

- Provides structured processes to deliver consistent IT services.
- Aligns IT efforts with business goals, improving operational efficiency.
- Reduces downtime and improves customer satisfaction.
- Enhances accountability and tracking of service issues.
- Supports measurable improvements through continual service improvement (CSI).

3. Importance of Change Management:

- Prevents service disruption by managing changes systematically.
- Ensures all changes are evaluated, approved, and documented.
- Reduces the risk of implementing faulty or untested updates.
- Enhances transparency and communication across IT teams and stakeholders.

4. Incorporating Change Management into ITIL:

- Define a Change Advisory Board (CAB) to review and approve changes.
- Use a formal change request process with risk impact assessments.
- Implement change scheduling and testing protocols.
- Conduct post-implementation reviews to assess the success and learn from issues.
- Integrate change records into the Configuration Management Database (CMDB).

Task 3: Cybersecurity Laws and Regulations

1. Role of SOX:

- Requires Nerdnest to maintain accurate financial reporting and internal controls.
- Ensures transparency and accountability through auditable processes and internal audits.
- IT systems supporting financial data must have strong access control, change management, and audit logging.

2. HIPAA Compliance:

- Applies if Nerdnest processes or stores protected health information (PHI).
- Requires implementation of physical, administrative, and technical safeguards, such as:
  - Encryption of health data
  - Access control to limit data access to authorized personnel
  - Employee training and incident response procedures
- Helps prevent unauthorized access and ensures data confidentiality and integrity.

3. Impact of CCPA & CPRA:

- Grants California residents the right to:
  - Know what personal data is collected
  - Request deletion of personal data
  - Opt out of data sale
- Nerdnest must update privacy policies, implement data classification, and maintain consumer consent logs.
- CPRA enhances enforcement and introduces data minimization and purpose limitation principles.

Task 4: Cybersecurity Audits

1. Benefits of Regular Cybersecurity Audits:

- Identifies vulnerabilities and misconfigurations before they are exploited.
- Validates the effectiveness of security controls and policies.
- Supports regulatory compliance and reduces risk of penalties.
- Increases trust and transparency with customers, investors, and partners.
- Encourages continuous improvement of security measures.

2. How Nerdnest Can Prepare for a Cybersecurity Audit:

- Define the audit scope: systems, locations, processes to be reviewed.
- Update and document security policies and procedures.
- Conduct internal self-assessments to detect weaknesses early.
- Ensure asset inventories, access controls, and data protection measures are current.
- Train employees on audit protocols and compliance responsibilities.
- Perform a mock audit or pre-assessment review.
- Assign audit liaisons to facilitate efficient communication during the audit.