Graded assignment.

1

**Key components that neardnest should implement:**

Govern: establish cyber security policies and strategies

Identify: recognize assets assesses risk

Detect: identifies potential cyber threats

Respond :prepare and manage responses to incident

Recover: restores operations after a cyber-security breach

**Explain how to conduct a comprehensive risk assessment.**

Access Control system

Password security for staffs, with at least eight characters.

Physical security, Eg. Cctv and passkeys

Data encryption, secure socket layer and transport layer security.

**Explain the importance of continuous monitoring.**

Improved Incident Management and Post-Incident Analysis: aids staffs to be alert and never taken unaware by a cyber-threat.

**Data Integrity and Confidentiality: protects the reputation of the company my keeping customer data true to itself.**

**Early Detection of Threats: helps in identifying security threats right on time.**

Real-time Incident Response: facilitates I-R activities as staffs can easily eliminate threat ones spotted.

2

**Identify key ITIL processes to incorporate into ITSM strategy.**

Service strategy:

Service design:

Capacity management:

Availability management:

**Explain how adopting ITIL streamlines IT service delivery and quality:**

ITIL streamlines IT service delivery and enhances quality by standardizing processes, aligning IT services with business objectives, improving service management practices, ultimately delivering greater value to the business and end-users.

**Explain the importance of change management**.

Helps organizations adopt to new technologies and regulation as well as it keeps the organizations firmware running with latest compliance tools.

Guiding transitions in goal processes and technology.

**Explain how to incorporate Change Management into the ITIL framework.**

Integrating Change Management with the ITIL framework requires focus on defining the change process and establishing the roles and responsibilities from classification, prioritization and integration of changes into other ITIL processes.

3

Explain the role of the Sarbanes-Oxley Act (SOX):

The **Sarbanes-Oxley Act (SOX)** indirectly affects cyber security practices by requiring organizations to implement robust internal controls and safeguards for financial data and reporting systems. While it doesn't explicitly focus on cyber security, its requirements for data integrity, access control, audit trails, and system availability heavily rely on cyber security measures to be effective.

**Describe how HIPAA requirements impact Nerdnest:**

Privacy rule: ensures that customer data stays confidential.

Security rule: provides a firm security framework that governs all activities and prevents threat

Administrative: prioritizes and make best results through administration, regularly updating security measures, and encrypting ePHI.

Physical safeguard and technical safeguards

**Explain how CCPA and CPRA requirements impact Nerdnest.**

The CCPA and CPRA carry immense weight in Nerdnest's cybersecurity, mainly because they pertain to the safeguarding of consumers' data, respecting privacy rights, and internal controls.

**Explain the benefits of conducting regular cybersecurity audits.**

Conducting regular cybersecurity audits offers numerous benefits, including identifying vulnerabilities, ensuring compliance, improving incident response, and mitigating risks. They help enhance data protection, strengthen policies, and ensure business continuity, while also boosting stakeholder confidence and tracking security improvements over time. Ultimately, regular audits are an essential component of a proactive and effective cybersecurity strategy, safeguarding an organization’s data, systems, and reputation from evolving cyber threats.

**Describe the preparation required for a successful cybersecurity audit**.

* **Define the Scope of the Audit Purpose**: Clearly define what the audit will cover. This includes the systems, applications, processes, and security controls that will be examined. **Understand the Audit Framework and Standards**
* **Frameworks and Guidelines**: Identify the standards, frameworks, or best practices the audit will follow, such as **NIST**, **ISO 27001**, **CIS Controls**, or regulatory frameworks like **PCI-DSS**, **SOX**, or **GDPR**.
* **Engage Stakeholders and Key Personnel Internal Team Involvement**: Identify the key internal stakeholders (e.g., IT staff, security officers, risk managers, compliance officers) who will play a role in the audit.
* **Establish a Timeline and Communication Plan Audit Timeline**: Set a clear timeline for the audit, including deadlines for document submission, audit meetings, and follow-up actions.