Nerdnest Project 8 – Full Submission

Final Project – Nerdnest Governance, Risk & Compliance (GRC), ITIL, and Cybersecurity Audit

Submitted by: Judy Raj

Task 1: Identify the critical elements of a GRC framework

1. Key Components:

Nerdnest's GRC framework should include governance structure, risk assessment, risk management, compliance management, policy and procedure development, control implementation, regular audits, clear responsibility assignments, communication protocols, and continuous improvement processes. These ensure alignment with regulations and standards while mitigating risks.

2. Risk Assessment:

A comprehensive risk assessment helps Nerdnest proactively identify threats and vulnerabilities, evaluate impact and likelihood, and prioritize mitigation aligned with industry best practices. This minimizes potential damages and strengthens cybersecurity posture.

3. Continuous Monitoring:

Continuous monitoring is vital for maintaining compliance and detecting non-conformance in real time. It enables proactive remediation, prevents costly violations, and sustains regulatory alignment through ongoing oversight and alerting.

Task 2: Identify and apply ITIL processes

1. ITIL Processes:

Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement (CSI). Each ensures services align with business goals, efficiency, and resilience.

2. Adoption Benefits:

ITIL standardizes IT service management, improving efficiency, visibility, customer focus, and cost optimization. It enhances collaboration, quality of service delivery, and data-driven improvement.

3. Importance of Change Management:

Change Management provides control, stakeholder engagement, risk evaluation, and minimizes disruptions during IT transitions, ensuring seamless updates and user satisfaction.

4. Incorporation into ITIL Framework:

Nerdnest integrates Change Management via standardized processes, CMS tracking, clear role definitions, communication, evaluation, and performance measurement—ensuring effective transitions.

Task 3: Identify and apply cybersecurity laws

1. Sarbanes–Oxley Act (SOX):

Ensures Nerdnest’s financial integrity through strong internal controls, management accountability, and auditor independence. It requires documentation, segregation of duties, and compliance reviews.

2. HIPAA:

Requires Nerdnest to secure healthcare data using access controls, encryption, employee training, and breach notification. It emphasizes PHI confidentiality and vendor compliance.

3. CCPA / CPRA:

These regulations enforce consumer rights over data (access, deletion, opt-out), mandate transparency, limit data collection, and require secure handling of sensitive information.

Task 4: Cybersecurity audits

1. Benefits:

Regular audits identify vulnerabilities, ensure compliance, improve risk management, and enhance data protection and reputation. They enable early threat detection, better efficiency, and informed decision-making.

2. Preparation:

Nerdnest should conduct pre-audit risk reviews, update policies, test controls, document evidence, train staff, and perform internal audits to demonstrate compliance and readiness.

Conclusion:

The project emphasizes the importance of a unified GRC and ITIL strategy, continuous monitoring, legal compliance, and audit readiness. Together, they strengthen Nerdnest’s operational resilience and regulatory confidence.