NIST 800-53 Framework

Security Audit

CyberTech Innovations

By Tanasha Bryant

**Risk Management Framework Implementation Plan**

**Company Overview**

CyberTech Innovation is a forward-thinking technology company specializing in innovative solutions across various industries. The company has rapidly grown into a leading technology firm by pioneering solutions in AI, loT, blockchain across various sectors such as healthcare, finance, and manufacturing. With its headquarters in Silicon Valley and multiple offices worldwide, CyberTech is at the forefront of technological innovation, aiming to revolutionize how industries operate while ensuring the highest cybersecurity standards.

Implementing the NIST Risk Management (RMF) is crucial for CyberTech Innovations enhance cybersecurity, ensure regulatory compliance, and mitigate risks across its critical systems. RMF provides a structed approach to identifying, assessing, and managing cybersecurity threats, protecting sensitive customer data, R&D assets, and supply chain operations. It helps the company meet industry standards like PCI DSS, HIPAA, and GDPR, reducing legal and financial risks.

Additionally, RMF strengthens business resilience by preventing cyberattacks, securing third-party vendors, and ensuring continuous operations. By adopting RMF, CyberTech Innovations can achieve Authorization to Operate (ATO), improve decision-making, and safeguard its reputation in an involving landscape.

**Categorization of Information Systems**

* **Customer Data Management Systems (CDMS) – High Impact**: Contains sensitive customer data, making it a prime target for identity theft, fraud, and regulatory violations under laws such as PCI DSS.
* **Research & Development (R&D) Network – Moderate Impact:** Holds proprietary research data that, if compromised, could lead to loss of competitive advantage, but does not directly affect customer data or financial transactions.
* **Supply Chain Management System (SCMS) – High Impact:** Any disruption to the supply chain due to cyberattacks can lead to operational downtime, financial losses, and reputational damage, justifying its high-impact rating.
* **Payment Processing System (PPS) – High Impact:** Processes financial transactions, making it vulnerable to fraud, payment breaches, and regulatory penalties requiring stringent security measures.

**Side Note**: Each system is categorized to ensure that security controls are applied appropriately, aligning with NIST guidelines and ensuring compliance with industry-specific regulations.

**Selection of Security Controls**

The following controls are selected from NIST SP 800-53 based on system categorization:

* **Access Control (AC-2) –** Role-based access control ensures that only authorized personnel have access to sensitive systems, reducing the risk of insider threats and unauthorized data exposure.
* **Audit and Accountability (AU-6)** – Logging and monitoring help detect anomalies, ensuring accountability and facilitating forensic analysis in case of security incidents.
* **Incident Response (IR-4)** – Rapid incident detection and response are crucial in minimizing damage from cyberattacks, ensuring business continuity and data protection.
* **Encryption (SC-12, SC-13**) – Encrypting data at rest and in transit safeguards against data breaches, ensuring compliance with industry standards like PCI DSS.

**Assessment Strategy**

To ensure comprehensive evaluation and validation of security controls, the following methods and tools will be utilized:

* **Penetration Testing:** ethical hacking techniques such as Metaspoilt, Burp, and Suite will simulate real-world cyberattacks to test the effectiveness of security controls.
* **Automated Vulnerability Scans**: tools such as Nessus, Qualys, and OpenVAS will be used to identify security vulnerabilities and misconfigurations across CyberTech Innovations’ systems.
* **Manual Security Control Reviews:** manual assessments will be conducted by reviewing system configurations, security policies, and access control mechanisms to ensure compliance with NIST SP 800-53 guidelines.
* **Security Awareness Training for Employees:** employees will undergo periodic cybersecurity training using platforms like KnowBe4 to reduce human-related security risks.
* **Compliance Audits:** regular security audits will be performed to validate compliance with industry regulations such as PCI DSS, GDPR, and HIPAA.
* **Security Information and Event Management (SIEM):** tools like Splunk and IBM QRadar will be deployed to monitor logs and detect suspicious activities in real time.

**Implementation Milestone**

The implementation milestones are structures to ensure a logical, phased approach to securing CyberTech Innovations’ systems. Each phase builds upon the previous one to achieve an optimal cybersecurity posture:

1. **Phase 1 – Initial assessment and risk identification:** This phase establishes the baseline security posture, identifies potential threats, and assess vulnerabilities.
2. **Phase 2 – Control selection and security enhancements:** based on identified risks, appropriate security controls are selected and implemented to mitigate threats efficiently.
3. **Phase 3 – testing and validation of implemented controls**: security measures are tested using vulnerabilities scanning, penetration testing, and manual reviews to confirm their effectiveness before full deployment.
4. **Phase 4 – Final risk assessment and compliance verification**: this ensures that all implemented controls meet regulatory requirements and that residual risks are documented.
5. **Phase 5 – Authorization to Operate (ATO) submission**: the final phase involves submitting documentation for ATO approval, ensuring that CyberTech Innovations’ systems comply with industry standards and are approved for secured operations.