**Cybersecurity Risk Management Framework Development Template**

Learner Name: Kabir Chand

Date: 20/03/2025

Business Sector Chosen: Healthcare

**Step 1: Foundation Setting**

**CISSP Domains Overview**

* **Security and Risk Management**: Ensures risk governance, legal and regulatory compliance (e.g., HIPAA for healthcare). Defines risk tolerance and management policies.
* **Asset Security**: Focuses on data classification, ownership, and secure data handling practices to protect patient records.
* **Security Architecture and Engineering**: Applies secure design principles for healthcare IT infrastructure, such as encryption and secure network segmentation.
* **Communication and Network Security**: Ensures secure data transmission, VPN use, and protection against network-based attacks.
* **Identity and Access Management (IAM)**: Controls access through authentication, authorization, and auditing for healthcare professionals and staff.
* **Security Assessment and Testing**: Regular vulnerability assessments and penetration testing to identify security gaps.
* **Security Operations**: Incident response planning, logging, and monitoring healthcare data access.
* **Software Development Security**: Secure coding practices for healthcare applications to prevent vulnerabilities like SQL injection and XSS.

**Business Context**

* **Organization Size**:

Medium-sized hospital with multiple departments and 500+ employees.

* **Types of Data Handled**:
* Electronic Health Records (EHRs), insurance details, billing information, patient prescriptions.
* **Critical Operations**:

- Patient data management

- Electronic medical records (EMR) access

- Online appointment scheduling

- Telemedicine services

**Step 2: Risk Assessment Process**

* **Asset Identification**

| **Asset Type** | **Asset Description** | **Importance** |
| --- | --- | --- |
| EHR System | Stores patient health records | High |
| Network Infrastructure | Routers, firewalls, IDS/IPS systems | High |
| Employee Workstations | Computers used by healthcare professionals | Medium |
| Medical IoT Devices | Connected devices for patient monitoring | High |
|  |  |  |
| Cloud Storage | Offsite storage for patient data | High |

* **Threat Identification**

| **Asset** | **Potential Threats** |
| --- | --- |
| EHR System | Ransomware, unauthorized access |
| Network Infrastructure | DDoS attacks, MITM attacks |
| Employee Workstations | Phishing, malware infections |
| Medical IoT Devices | Unauthorized access, firmware exploits |
| Cloud Storage | Data leakage, insider threats |
|  |  |

* **Vulnerability Assessment**

| **Asset** | **Vulnerabilities** |
| --- | --- |
| EHR System | Misconfigured firewall rules |
| Network Infrastructure | Unpatched software vulnerabilities |
| Employee Workstations | Default passwords, outdated firmware |
| Medical IoT Devices | Improper access controls |
| Cloud Storage | Weak authentication mechanisms |
|  |  |

* **Risk Analysis**

| **Risk** | **Likelihood** | **Impact** | **Priority** |
| --- | --- | --- | --- |
|  |  |  |  |
| Ransomware Attack | High | High | Critical |
| Phishing Attacks | High | Medium | High |
| IoT Device Exploit | Medium | High | High |
| Insider Threats | Medium | Medium | Medium |
| Data Breach | High | High | Critical |

**Step 3: Risk Mitigation Strategies**

| **Risk** | **Mitigation Strategy** | **CISSP Domain Alignment** |
| --- | --- | --- |
|  |  |  |
| Ransomware | Backup policies, endpoint detection & response | (Security Operations) |
| Phishing | Security awareness training, email filtering | (Security & Risk Management) |
| IoT Device Exploit | Network segmentation, firmware updates | (Security Architecture) |
| Data Breach | Encryption, data loss prevention | (DLP) tools (Asset Security) |

**Step 4: Implementation Plan**

**Action Plan**

| **Strategy** | **Timeline** | **Responsible Party** |
| --- | --- | --- |
| Implement daily backups and test recovery process | 3 months | IT Team |
| Conduct security training and phishing simulations | Ongoing | HR & Security Team |
| Secure IoT devices with password changes and patches | 2 months | Network Team |
| Enforce least privilege access policies | month | Admin |

**Training and Awareness**

* **Training Goals**: Reduce human error-related security breaches.
* **Key Topics**: Phishing prevention, secure password management.
* **Delivery Method**: Online modules, interactive sessions.
* **Schedule**: Quarterly training sessions.

**Step 5: Monitoring and Review**

**Continuous Monitoring**

* Monitoring Processes:

SIEM-based log analysis, network traffic monitoring.

* Tools/Technologies Used:

Splunk, ELK Stack, IDS/IPS.

**Periodic Review**

* + Review Frequency:

Bi-annual security audits

* + Review Criteria:

Compliance adherence, incident response effectiveness.

**Step 6: Documentation and Communication**

**Documentation**

* Location of Documentation:

Secure repository with role-based access control.

* Access Permissions:

Restricted to security personnel.

**Presentation Summary**

* Key Points:

Risk identification, mitigation strategies, implementation roadmap.

* Expected Outcomes:

Improved cybersecurity resilience, compliance with HIPAA.

* Rationale Behind Strategies:

Aligning security measures with business objectives

**Reflection and Next Steps**

* Challenges Encountered:

Integrating security controls with legacy healthcare systems.

Educating non-technical staff about cybersecurity risks.

* Learnings:

Importance of proactive threat detection and response.

Need for continuous training to mitigate human error.

* Next Steps for Further Improvement:

Explore \*\*AI-driven threat detection\*\* for real-time security analytics.

Conduct \*\*red team exercises\*\* to test the resilience of defences.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*