​​**Cybersecurity Risk Management Framework Development Plan**

Learner Name: Muhammad Saad Shaikh

Date: 06/06/2024

Business Sector Chosen: Finance and banking

**Step 1: Foundation Setting**

CISSP Domains Overview

* Summarize key points of each CISSP domain relevant to risk management:
  1. **Security and Risk Management**: this domain is responsible for setting security goals,risk mitigation, compliance and business continuity
  2. **Asset Security**: this is responsible for the storage, access, transport and destruction of data
  3. **Security Architecture and Engineering**: focuses on designing, implementing and maintaining secure systems and networks to protect an organisation’s information assets
  4. **Communication and Network Security**: focuses on safeguarding an organisation’s network from potential threats
  5. **Identity and Access Management (IAM)**: it helps security professionals understand how to protect asset access and ensures compliance with CIA requirements
  6. **Security Assessment and Testing**:it is responsible for testing if an organisation’s security function correctly and efficiently
  7. **Security Operations**: it is responsible for launching the correct security measures when an incident occurs
  8. **Software Development Security**: this refers to the security controls that were implemented in to applications during their development stage

Business Context

* **Organization Size**: international
* **Types of Data Handled**: Customer information, payment data, financial data

| **Asset Type**            **1)current asset**          **2)Non-Current Asset (Fixed Asset)**    **3)** Non-Current Asset | **Asset Description**      **1)**Cash on hand and short-term investments that can be quickly converted to cash.      2) Includes real estate, buildings, machinery, and other physical assets owned by HSBC          **3)**Investments in stocks, bonds, and other financial instruments. | **Importance**          **1)**Vital for liquidity, day-to-day operations, and meeting financial obligations.  **2)** Supports the bank’s operations, such as branch offices, data centers, and infrastructure.      **3)** Generates income and diversifies the bank’s portfolio. |
| --- | --- | --- |
|  |  |  |

* **Critical Operations**: retail and corporate banking, technology infrastructure

**Step 2: Risk Assessment Process**

Asset Identification

* List critical assets needing protection: Financial Data, Infrastructure, Payment Processing Systems, Intellectual Property:

Threat Identification

* Identify potential threats for each asset:

| **Asset** | **Potential Threats** |
| --- | --- |
| **1)cash and equivalents**  **2)properties and infrastructure**  **3)investments** | 1)phishing, ransomware, unauthorised access and fraud  2)supply chain attacks,data theft and physical unauthorised access  3)insider threats, data leakage and algorithmic errors |

Vulnerability Assessment

* Determine vulnerabilities for each asset:

| **Asset** | **Vulnerabilities** |
| --- | --- |
| **1)cash and equivilants**  **2) properties and infrastructure**  **3) investments** | 1) phishing, weak authentication, insider threats and 3rd party risks  2) supply chain weaknesses, IoT devices, physical access and outdated software  3) insider trading, algorithmic errors and data leakage |

Risk Analysis

* Analyze and prioritize risks using a risk matrix:

| **Risk** | **Likelihood** | **Impact** | **Priority** |
| --- | --- | --- | --- |
| **1)low to moderate**  **2)moderate to high**  **3)moderate** | 1) **moderate**  **2) low**  **3) moderate** | **1) moderate**  **2) high**  **3) moderate** | 1**)medium**  **2)high**  **3)medium** |

**Step 3: Risk Mitigation Strategies**

* Develop mitigation strategies for high-priority risks:

| **Risk** | **Mitigation Strategy** | **CISSP Domain Alignment** |
| --- | --- | --- |
| **1)cash is susceptible to theft, fraud and loss**  **2)properties are vulnerable to theft, distruption or damage**  **3)investments are subject to market volatility** | **1)strict access controls and regular checks**  **2)conduct risk assessments and vulnerability scans, create an emergency response plan**  **3)stay informed about market trends, consider risk tolerance** | **1)security and risk management**  **2)physical security**  **3)Asset security** |

**Step 4: Implementation Plan**

Action Plan

* Outline steps for implementing mitigation strategies:

| **Strategy** | **Steps** | **Timeline** | **Responsible Party** |
| --- | --- | --- | --- |
| 1)Cash security and Access controls  2)Risk Assessment and Preparedness  3)Investment diversification and review  4)Continuous Risk management | **1) Secure cash in safes or bank accounts. 2. Implement access controls and regular audits.**  **2) 1. Conduct risk assessments. 2. Invest in disaster-resistant infrastructure. 3. Develop emergency response plans.**    **3) 1. Diversify investments across asset classes. 2. Regularly review and adjust portfolios.**    **4)1. Establish risk assessment procedures. 2. Monitor risk indicators. 3. Update strategies as needed.** | **1)Immediate**  **2)On-going**  **3)Quarterly**  **4)Continuous** | **1)Finance department**  **2)Facilities Management**  **3)Investment committee**  **4)Risk management** |

Training and Awareness

* **Training Goals**:

**-Cybersecurity Awareness:** Ensure that all employees understand the critical importance of cybersecurity. The goal is to enhance their knowledge and vigilance in safeguarding HSBC’s digital assets.

**-Risk mitigation:** provide employees with practical skills that will allow them to identify and respond with cyber threats

* **Key Topics**:  
  -**Cybersecurity Best Practices:**
  + Educate employees about safe online practices, including password hygiene, phishing awareness, and secure browsing.
  + Discuss the risks associated with social engineering attacks and how to recognize them.

**-Incident response:**

* + Provide staff with training on incident reporting procedures. Ensure they know how to report suspicious activities promptly.
  + Conduct mock incident response drills to reinforce the process.

-Data Protection:

* Cover data privacy regulations (such as GDPR) and go over the CIA triad.
* Explain the importance of protecting customer data and maintaining confidentiality.

* **Delivery Method**: In - person
* **Schedule**: hold it everyday for 2 weeks (with each day consisting of 1 hour lessons)

**Step 5: Monitoring and Review**

Continuous Monitoring

* **Monitoring Processes**:
* **Tools/Technologies Used**:  
  NIST Risk Management Framework (RMF)  
  Tenable  
  i-CSRF

Periodic Review

* **Review Frequency**: Yearly
* **Review Criteria**:

1)Compliance (ensure it complies with laws and regulations)

2)Risk Assessment and Mitigation: Evaluate the effectiveness of risk assessment processes. Ensure that risks are identified, assessed, and mitigated appropriately. Verify that controls are in place to address identified risks.

3)Control Implementation: Assess the implementation of security controls. Verify that controls are deployed as intended and producing the desired result

**Step 6: Documentation and Communication**

Documentation

* **Location of Documentation**: On the cloud and a some hardcopies that are offsite
* **Access Permissions**: Only the security teams should have access to these documents

Presentation Summary

* **Key Points**:

-it is a collective responsibility to protect the data of the company

-if in doubt then do not press anything and speak to senior staff

-Our number one priority is protecting customer data

* **Expected Outcomes**:

-vulnerabilities have been plugged in and increased security

-Compliance

* **Rationale Behind Strategies**:

-ensuring compliance makes sure that the company is adhering to all regulations and laws which ensures that customer data is protected and prevents the company from being fined for noncompliance

-Ensuring stricter security and access controls helps the company to keep customer data well protected and prevents financial damage as well as identity theft