**Case: Security Audit for XYZ Financial Services**

**Activity Overview**

In this case, you will assume the role of a cybersecurity professional at XYZ Financial Services, a medium-sized financial institution that operates nationally. The organization’s IT manager has entrusted you with the responsibility of conducting an internal audit of the company’s assets, controls, and compliance with regulations and standards. Your primary objective is to assess the current security posture of XYZ Financial Services, identify areas for enhancement, and provide actionable recommendations aligned with the organization’s objectives and risk profile. This audit will be a crucial step for XYZ Financial Services to protect customer data, ensure compliance with financial regulations, and maintain business continuity.

**Scenario**

XYZ Financial Services has been experiencing growth in their customer base and expanding their online services. With this growth, they have recognized the need for a comprehensive security audit. The Chief Information Security Officer (CISO) at XYZ Financial Services believes that an audit is essential to address the following concerns:

* **Data Protection**: Ensuring the security of sensitive customer financial data and personal information.
* **Compliance**: Ensuring compliance with financial regulations such as the Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry Data Security Standard (PCI DSS).
* **Business Continuity**: Identifying potential risks and vulnerabilities that could disrupt financial operations and developing a strategy to maintain business continuity.

**Step-By-Step Instructions**

**Step 1: Access Supporting Materials**

You will have access to the following supporting materials:

* XYZ Financial Services: Risk Assessment (p. 4)
* XYZ Financial Services: Audit Scope and Goals (p. 5-7)

These documents will provide essential information about the organization's assets, risks, and audit objectives. Thoroughly review the provided scenario and supporting documents. Gain a comprehensive understanding of the company’s background, goals, and its current risk exposure.

**Step 2: Analyze the Audit Scope, Goals, and Risk Assessment**

Review the provided audit scope, goals, and risk assessment documents. Consider the following questions:

* What are the most significant risks to XYZ Financial Services considering their line of business?

Currently, in accordance to the scope, goals, and risk assessment XYZ Financial Services contains the following risks.

* Which controls should be prioritized for immediate implementation to address these risks?
* Which compliance regulations and standards must XYZ Financial Services adhere to, and why is compliance crucial for their operations?

**Step 3: Conduct the Audit: Controls Assessment**

Complete the controls assessment for XYZ Financial Services. This involves:

* Reviewing the list of assets managed by XYZ Financial Services, and identifying other assets that should be reviewed in this security audit.
* Reviewing each control name and its type/explanation.
* Marking controls that need to be implemented with levels of priority (high, medium, low, NA).

You will need to consider administrative, technical, and physical controls that are relevant to a financial institution's security.

**Step 4: Conduct the Audit: Compliance Checklist**

Complete the compliance checklist for XYZ Financial Services. This involves:

* Selecting the compliance regulations and standards that XYZ Financial Services needs to adhere to base on their business operations.
* Providing explanations for why each selected regulation or standard is necessary for XYZ Financial Services.

Ensure that your selections align with the organization's goals and risk assessment.

**Step 5: Assess Your Activity**

After completing the controls assessment and compliance checklist, assess your work using the following self-assessment statements:

1. Reviewed the audit scope, considered risks, and ensured controls address these risks.
2. Selected controls based on relevance and rated their priority for implementation.
3. Selected compliance regulations and provided explanations for their necessity.

**Step 6: Create a Professional Stakeholder Memorandum [I am NOT requiring this step be completed]**

1. Compile all your findings, assessments, and recommendations into a professional and structured report.
2. Organize the report logically, employing distinct headings and subheadings for clarity.
3. Employ language and formatting suitable for a professional audience.
4. Guarantee that your report effectively conveys essential information to the IT manager and stakeholders.

This case will provide you with a practical exercise in conducting a security audit, analyzing risks, ensuring compliance in the context of a financial institution, and communicating results, all of which are critical for protecting sensitive financial data and maintaining trust with customers.

For examples, check out Google’s Botium Toys case scenario -

1. Botium Toys: Audit scope and goals - <https://docs.google.com/document/d/1bA-J96jzDVFi9XjNOKd4w2bCR7X7ZTs3_szPElOkyFM/template/preview>
2. Botium Toys: Risk Assessment - <https://docs.google.com/document/d/1rdjLtrTQD7c8K3cUeKnrhyq3DzXpKNL9vdHI1T9Vu80/template/preview?resourcekey=0--N8L-3p4Hel22vaxVLjIOA>
3. Compliance checklist template – (the on-campus class indicated one of these templates is not reachable but that the exemplar is available, so that will still give you the template, just filled in for the Botium Toys example.) <https://docs.google.com/document/d/1h69F8hWxm8SY0zrv80zJImJBb41gwJ4wcWtB_Px2sk4/edit?resourcekey=0-V_JsZIEF-xm0nFYVdHMxLA#heading=h.goe9xzxx0fid>
   1. Compliance Checklist Exemplar - <https://docs.google.com/document/d/15e7OA0qWg4g9KUqaqwXZBEGMdcxPJLuD72xk1LK813k/template/preview>
4. Controls Assessment template - <https://docs.google.com/document/d/1nZMG55Hw-vjhpV_5ZtqNMk3Tiqw7d2P6IPeE2excOvI/template/preview?resourcekey=0-AtDwkpM9ssckGMJULHMrjA>
   1. Controls Assessment Exemplar - <https://docs.google.com/document/d/1A4Zutk-dw71Vq-aR-vKu7BaKeZSjSp_FC5OYRFAz5Zk/template/preview?resourcekey=0-xS6eMAb-h0QilpkYFzP-GQ>
5. ~~Stakeholder memorandum template -~~ [~~https://docs.google.com/document/d/1qMI-xUxzueqiODCVuRlZDWSHJgWVXlXPvbWMRppCvBc/edit?resourcekey=0-S8aWUEPm7QpWE5yRgZ23ow#heading=h.wj2j189xt6fj~~](https://docs.google.com/document/d/1qMI-xUxzueqiODCVuRlZDWSHJgWVXlXPvbWMRppCvBc/edit?resourcekey=0-S8aWUEPm7QpWE5yRgZ23ow#heading=h.wj2j189xt6fj)
   1. ~~Stakeholder memorandum exemplar -~~ [~~https://docs.google.com/document/d/1z2euYO5Na\_HkoYu55Cj3Y-n-ZsaiNeFc3CctkY5Fkmk/edit?resourcekey=0-qNGf8KD-RSJekN0bbrOgaw#heading=h.wj2j189xt6fj~~](https://docs.google.com/document/d/1z2euYO5Na_HkoYu55Cj3Y-n-ZsaiNeFc3CctkY5Fkmk/edit?resourcekey=0-qNGf8KD-RSJekN0bbrOgaw#heading=h.wj2j189xt6fj)

**XYZ Financial Services: Risk Assessment**

**Current Assets:**

* Customer financial data and records
* Employee devices (computers, mobile phones, etc.)
* Data center infrastructure
* Internet access
* Internal network
* Vendor access management
* Transaction processing systems
* Backup systems
* Security monitoring tools
* Physical office locations

**Risk Description:** Currently, there are several risks associated with XYZ Financial Services' operations. These include the potential for data breaches, unauthorized access to financial records, disruption of financial services, and non-compliance with financial regulations.

**Control Best Practices:** The organization should implement controls such as data encryption, access controls, intrusion detection systems, regular data backups, and employee training on cybersecurity best practices.

**Risk Score:** On a scale of 1 to 10, the overall risk score is 7, indicating a moderate level of risk. This score is due to the sensitivity of financial data and the need for compliance with financial regulations.

**Additional Comments:** The impact of a data breach or non-compliance with regulations could result in financial losses, reputational damage, and legal consequences. It is essential to prioritize security measures to mitigate these risks.

**XYZ Financial Services: Audit Scope and Goals**

**Scope:** XYZ Financial Services internal IT audit will assess the following:

● Current user permissions set in the following systems: customer financial data and records, employee devices, data center infrastructure, internet access, internal network, vendor access management, transaction processing systems, backup systems, security monitoring tools, physical office locations.

● Current implemented controls in the following systems: customer financial data and records, employee devices, data center infrastructure, internet access, internal network, vendor access management, transaction processing systems, backup systems, security monitoring tools, and physical office locations.

● Current procedures and protocols set for the following systems: customer financial data and records, employee devices, data center infrastructure, internet access, internal network, vendor access management, transaction processing systems, backup systems, security monitoring tools, and physical office locations.

● Ensure current user permissions, controls, procedures, and protocols align with necessary compliance requirements.

● Ensure current technology is accounted for. Both hardware and system access

**Goals:** The goals for XYZ Financial Services' internal cybersecurity audit are as follows:

● To adhere to the General Data Protection Regulation (GDPR)

● To adhere to the Payment Card Industry Data Security Standard (PCI DSS)

● To adhere to the Health Insurance Portability and Accountability Act (HIPAA)

● To adhere to the Federal Energy Regulatory Commission -North American Electric Reliability Corporation (FERC-NERC)

● Establish a better process for their systems to ensure they are compliant

● Ensure systems control throughout all their assets

● Implement the concept of least permissions when it comes to user credential management

● Establish their policies and procedures, in compliance to the institutions manual

● Maintain organizations integrity and accountability

This audit aims to provide XYZ Financial Services with a comprehensive assessment of their cybersecurity program, ensuring they can protect customer data, maintain regulatory compliance, and continue to provide essential financial services securely.

**Findings:** Should be addressed; with immediate need levels

● Finding 1: BYOD controls

- This is an immediate threat. This finding is on the basis that there are currently no controls on the BYOD policies in effect at XYZ Financial Services. Controls will need to be set immediately and implement access controls and regularly monitor user permissions.

● Finding 2: Compliance with GDPR

- This is an immediate threat. This finding is on the basis that XYZ Financial Services is not fully in compliance with GDPR. General Data Protection Regulation (GDPR), GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens’ data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and an E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident. Immediate actions will need to be taken to ensure full compliance. This is done y maintaining consent practices and implementing proper protection measures. Full compliance will also avoid fines and legal consequences.

**Findings:** Should be addressed; with no immediate need levels

● Finding 1: Security controls at physical locations

- While this is not an immediate threat. This finding is on the basis that more security barriers are needed at physical locations. It should be acted upon as soon as possible, after urgent findings are addressed. Physical security will keep the facility as well as employees safe from outside threats. Threats can arise from not only external but internal intruders. Physical barriers such as turnstiles and locks shall be implemented throughout the site.

● Finding 2: Employee training on controls

- While this is a not an immediate threat. This finding is on the basis that proper employee training is needed after controls have been properly set. This should be done after the controls have been set. Effective training is important in creating proper compliance and reducing the risks of BYOD policies. Employees will be able to them protect not only themselves but also regulatory and litigation risks.

**Administrative Controls:**

**Asset Category:** Customer Financial Data

| **Control Name** | **Control Type and Explanation** | **Needs to be Implemented (X)** | **Priority (High, Medium, Low, NA)** |
| --- | --- | --- | --- |
| Access Controls | Implement strong access controls to limit who can access and modify customer financial records. | [X] | High |
| Employee Training | Conduct cybersecurity training for employees to reduce the risk of human errors in data handling. | [X] | Medium |

**Asset Category:** Employee Devices

| **Control Name** | **Control Type and Explanation** | **Needs to be Implemented (X)** | **Priority (High, Medium, Low, NA)** |
| --- | --- | --- | --- |
| Access Controls | Implement access controls to restrict unauthorized access to employee devices (computers, phones). | [X] | High |
| Employee Training | Train employees on cybersecurity best practices to minimize security risks associated with devices. | [X] | Medium |

**Technical Controls:**

**Asset Category:** Customer Financial Data

| **Control Name** | **Control Type and Explanation** | **Needs to be Implemented (X)** | **Priority (High, Medium, Low, NA)** |
| --- | --- | --- | --- |
| Data Encryption | Implement data encryption to protect customer financial data in transit and at rest. | [X] | High |
| Intrusion Detection Systems | Implement IDS to quickly identify and respond to potential security incidents related to customer data. | [X] | High |
| Regular Data Backups | Regularly backup customer financial data to ensure business continuity and data recovery capabilities. | [X] | Medium |

**Asset Category:** Employee Devices

| **Control Name** | **Control Type and Explanation** | **Needs to be Implemented (X)** | **Priority (High, Medium, Low, NA)** |
| --- | --- | --- | --- |
| Access Controls | Implement access controls to identification and authentication mechanisms. | [X ] | High |
| MDM software controls | Implements MDM’s to manage employees devices (computers, phones). | [X ] | Medium |
| Employee Training | Train employees on safe practices to maximize security associated with their devices. | [X ] | Medium |

**Physical Controls:**

**Asset Category:** Physical Office Location

| **Control Name** | **Control Type and Explanation** | **Needs to be Implemented (X)** | **Priority (High, Medium, Low, NA)** |
| --- | --- | --- | --- |
| Security Monitoring Tools | Implements security systems such as turnstiles and physical barriers to identify personal credential access. | [ X] | High |
| Employee authorized controls | Implement access controls to identify and authenticate where access is allowed for each employee. | [ X] | High |
| Physical records stored in secured area | Implement security areas for the sole purpose to store physical records that is stored in secured areas; proper personnel status will be needed to gain access. | [X ] | High |

**Compliance Checklist Exemplar for XYZ Financial Services**

Here is a compliance checklist exemplar for the XYZ Financial Services scenario, considering the relevant compliance regulations and standards:

**Compliance Checklist:**

**Asset Category:** Customer Financial Data

| **Compliance Regulation/Standard** | **Needs to be Implemented (X)** | **Explanation** |
| --- | --- | --- |
| General Data Protection Regulation (GDPR) | [X] | XYZ Financial Services operates internationally and may handle data of European Union (EU) citizens. GDPR compliance is essential to protect EU citizens' data and privacy. |
| Payment Card Industry Data Security Standard (PCI DSS) | [X] | As a financial services provider, XYZ Financial Services processes credit card payments, making PCI DSS compliance mandatory to secure cardholder data. |
| The Health Insurance Portability and Accountability Act (HIPAA) | [ ] | HIPAA typically applies to healthcare providers and insurers. Since XYZ Financial Services is not in the healthcare sector, HIPAA compliance may not be necessary. |
| System and Organizations Controls (SOC type 1, SOC type 2) | [X] | SOC reports assess the controls relevant to financial and data security. Adherence to SOC standards ensures transparency and trust with clients and partners. |
| Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC) | [ ] | FERC-NERC regulations pertain to the electricity sector and critical infrastructure, which may not be directly relevant to XYZ Financial Services' operations. |

**Asset Category:** Employee Devices

| **Compliance Regulation/Standard** | **Needs to be Implemented (X)** | **Explanation** |
| --- | --- | --- |
| General Data Protection Regulation (GDPR) | [X] | GDPR compliance is necessary to protect EU citizens' data privacy, even when handled on employee devices. |
| Payment Card Industry Data Security Standard (PCI DSS) | [ ] | While PCI DSS compliance is crucial for customer payment data, it may not directly apply to employee devices unless used for payment processing. |
| The Health Insurance Portability and Accountability Act (HIPAA) | [ ] | HIPAA compliance may not be relevant to employee devices in a financial services organization unless they handle healthcare data. |
| System and Organizations Controls (SOC type 1, SOC type 2) | [X] | SOC compliance ensures secure user access policies, data integrity, and overall data safety, which apply to employee devices. |
| Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC) | [ ] | FERC-NERC regulations are primarily applicable to the electricity sector and critical infrastructure, not employee devices. |

**Asset Category:** Server Infrastructure

| **Compliance Regulation/Standard** | **Needs to be Implemented (X)** | **Explanation** |
| --- | --- | --- |
| General Data Protection Regulation (GDPR) | [X] | GDPR compliance is vital to protect sensitive data stored on servers, especially if it includes EU citizens' information. |
| Payment Card Industry Data Security Standard (PCI DSS) | [X] | PCI DSS compliance is essential as servers process credit card transactions and store cardholder data. |
| The Health Insurance Portability and Accountability Act (HIPAA) | [ ] | HIPAA typically applies to healthcare data, so server compliance may not be necessary unless healthcare data is involved. |
| System and Organizations Controls (SOC type 1, SOC type 2) | [X] | SOC compliance ensures secure data handling, which is crucial for server infrastructure hosting sensitive financial data. |
| Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC) | [ ] | FERC-NERC regulations are primarily for the electricity sector and may not directly apply to server infrastructure. |

**Asset Category:** Network Infrastructure

| **Compliance Regulation/Standard** | **Needs to be Implemented (X)** | **Explanation** |
| --- | --- | --- |
| General Data Protection Regulation (GDPR) | [X] | GDPR compliance is necessary to protect data transmitted over the network, especially if it includes EU citizens' information. |
| Payment Card Industry Data Security Standard (PCI DSS) | [X] | PCI DSS compliance is vital for network security when processing credit card transactions and transmitting cardholder data. |
| The Health Insurance Portability and Accountability Act (HIPAA) | [ ] | HIPAA typically applies to healthcare data, so network compliance may not be necessary unless healthcare data is transmitted. |
| System and Organizations Controls (SOC type 1, SOC type 2) | [X] | SOC compliance ensures secure data transmission, a crucial aspect of network infrastructure, especially in a financial organization. |
| Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC) | [ ] | FERC-NERC regulations are primarily for the electricity sector and may not directly apply to network infrastructure. |

**XYZ Financial Services: Risk Assessment**

*Current Assets*

Assets managed by XYZ Financial Services encompass a wide range of resources, each carrying its own set of risks and vulnerabilities:

1. **Physical Assets**
   * Office Buildings and Facilities
   * Data Centers
   * Hardware (Servers, Workstations, Printers)
   * Networking Equipment (Routers, Switches)
   * Mobile Devices (Laptops, Tablets, Smartphones)
2. **Data and Information Assets**
   * Customer Data (Personal and Financial Information)
   * Transaction Records
   * Intellectual Property
   * Employee Records
   * Business Contracts and Agreements
3. **Digital Assets**
   * Software Applications (Banking Systems, Accounting Software)
   * Databases (Customer Databases, Financial Databases)
   * Websites and Online Services
   * Email Communication Systems
4. **Financial Assets**
   * Bank Accounts and Funds
   * Investment Portfolios
   * Assets Under Management (AUM)
   * Securities and Holdings
5. **Human Resources Assets**
   * Employee Skills and Expertise
   * Key Personnel (Management, IT Administrators)
6. **Infrastructure Assets**
   * Network Infrastructure (Wired and Wireless)
   * Cloud Services (Data Storage, Backup Services)
   * Server Rooms and Data Centers

*Risk Description*

1. **Physical Assets**
   * Risk: Theft, Damage, Unauthorized Access
   * Description: Physical assets are vulnerable to theft, damage from natural disasters, and unauthorized access. This includes the risk of unauthorized personnel entering server rooms or offices.
2. **Data and Information Assets**
   * Risk: Data Breaches, Unauthorized Access, Data Loss
   * Description: Customer data, transaction records, and intellectual property are high-value targets for cybercriminals. Unauthorized access or data breaches can lead to significant financial and reputational damage.
3. **Digital Assets**
   * Risk: Cyberattacks, Data Loss, Service Disruption
   * Description: Software applications, databases, and online services are susceptible to cyberattacks, which could result in data loss or service disruption.
4. **Financial Assets**
   * Risk: Fraud, Unauthorized Transactions
   * Description: Financial assets such as bank accounts, investment portfolios, and securities are at risk of fraud and unauthorized transactions, which can have severe financial implications.
5. **Human Resources Assets**
   * Risk: Talent Attrition, Insider Threats
   * Description: The loss of key personnel or insider threats can impact the organization's operations and security.
6. **Infrastructure Assets**
   * Risk: Service Disruption, Data Loss
   * Description: Network infrastructure and cloud services are critical for daily operations. Any disruption or data loss can affect business continuity.

*Control Best Practices*

Implementing control measures is essential to mitigate the risks associated with these assets:

1. **Physical Security**
   * Implement access control systems.
   * Install surveillance cameras and alarms.
   * Conduct regular security audits of facilities.
2. **Data Encryption**
   * Encrypt sensitive data both in transit and at rest.
   * Implement data access controls and role-based permissions.
3. **Firewall and Intrusion Detection**
   * Employ robust firewall solutions.
   * Utilize intrusion detection systems to monitor network traffic.
4. **Employee Training**
   * Provide cybersecurity training to employees.
   * Foster a culture of security awareness.
5. **Redundancy and Disaster Recovery**
   * Establish data backup and recovery plans.
   * Implement failover systems for critical infrastructure.

*Risk Score*

Assessing the overall risk score for XYZ Financial Services, considering the expanded list of assets, indicates a moderate to high level of risk. The organization must continue to implement and update controls to mitigate these risks effectively.

*Additional Comments*

The dynamic nature of the financial industry necessitates ongoing risk assessments and adaptations to control measures. XYZ Financial Services should remain vigilant and proactive in addressing emerging threats and vulnerabilities to ensure the security of its assets.