**XYZ Financial Risk Assessment**

TO: IT Manager, Stakeholders

FROM: Austin Clinefelter

DATE:

SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please find below an overview of the recent internal IT audit conducted at XYZ Financial Services:

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

* The security of sensitive customer financial data and personal information
* The company’s compliance with financial regulations such as the Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry Data Security Standard (PCI DSS)
* Identify potential risks and vulnerabilities that could disable operations
* Develop a strategy to maintain business continuity
* Evaluate current user permissions and access controls
* Evaluate security controls, including firewalls, intrusion detection systems, and encryption
* Review of current cybersecurity policies and procedures
* Review hardware and software used in financial transactions for compliance

**Goals**: The goals for the internal IT audit for XYZ Financial services is to:

* To adhere to the national standards of GLBA and PCI DSS and ensure compliance industry best practices
* Provide the highest possible security controls with firewalls, IDS, and encryption
* Provide a business continuity plan to prevent any delay in service
* Enhanced cybersecurity will limit all risks and vulnerabilities
* Train employees on policies and procedures and provide playbooks
* Establish a policy to provide employees with least permissions on security access

**Risk Assessment**: The following assets will be assessed:

* Customer financial information and data
* Employee devices including computers, tables, and cell phones
* Data infrastructure
* Internet access
* Internal network
* Vendor access
* Transactions processing systems
* Backup systems
* Cybersecurity monitoring
* Physical office locations

**Risk Description**: XYZ Financial Services currently contains several risks that could disrupt their business continuity as well as customers' data and information. Areas of concern include data breaches and unauthorized access from outside sources and keeping the company and employees updated on the latest practices to ensure national compliance.

**Controls Assessment Audit:**

**Administrative Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Customer Financial Data** | | | |
| **Control** | **Type and Explanation** | **Needs to be Implemented** | **Priority (High, Med, or Low)** |
| Access Controls | Implement access controls to limit individuals who can access and modify customer financial records. | [X] | High |
| Employee Training | Employees must be trained on best cybersecurity practices to prevent all incoming risks affecting customer data. | [X] | Medium |
| Least Privilege | Employees should only have access to pertinent data if they need to. | [X] | Medium |
| Disaster Recovery | A disaster recovery plan should be put in place | [X] | Medium |
| Password policies | Employees should be educated on the best password policies to prevent unauthorized access to data. | [X] | Medium |
| Business Continuity | A plan should be put in place to keep the business running in the case of a disaster with little to no downtime. | [X] | Medium |
| **Employee Devices** | | | |
| **Control** | **Type and Explanation** | **Needs to be Implemented** | **Priority (High, Med, or Low)** |
| Laptops | Employees who bring their Own Laptop should be trained to prevent Intrusions and have antivirus software. | [X] | Medium |
| Cell phones | An employee who brings their Own Cell Phone should be trained to prevent Intrusions. | [X] | Medium |
| Tablets | Employees who bring their Own Laptop should be trained to prevent Intrusions and have antivirus software. | [X] | Medium |

**Technical Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Internal Network** | | | |
| **Control** | **Type and Explanation** | **Needs to be Implemented** | **Priority (High, Med, or Low)** |
| Firewall | A firewall must be established before the internet is routed throughout the building to prevent unwanted access to certain cyberattacks. | [X] | High |
| Backups | Information should be backed up daily to prevent any loss of data or financial information. | [X] | High |
| Transaction Processing | All transactions should be monitored and encrypted to prevent the transactions from being seen by an unneeded person | [X] | High |
| **Internet Access** | | | |
| **Control** | **Type and Explanation** | **Needs to be Implemented** | **Priority (High, Med, or Low)** |
| Antivirus Software | All computers that are connected to the network should have antivirus software installed to prevent unwanted virus’s, worms, or trojans. | [X] | High |
| Vendor Access | All vendor access should be monitored with antivirus software installed to verify that virus’s are not sent in to the company. | [X] | High |
| Encryption | Any email or information sent through the internet should be encrypted to prevent any man-in-the-middle attacks to access the contents | [X] | High |

**Data Center Infrastructure**

|  |  |  |  |
| --- | --- | --- | --- |
| **Internal Network** | | | |
| **Control** | **Type and Explanation** | **Needs to be Implemented** | **Priority (High, Med, or Low)** |
| Backup Power | Different forms of backup power should be installed, such as a UPS or generator, so power is always available to the infrastructure. | [X] | High |
| Data Closet | A data closet should be installed to hold all network components. | [X] | Medium |
| Server Rack | A server rack should be installed in the data closet to keep all servers serviced on-site. | [X] | Medium |
| Seamless Cabling | Up-to-date copper through cables should be installed for the fastest data transmission and repair if needed | [X] | Medium |
| Laptop control | A laptop should be used to monitor all data transmission devices to fix and reroute devices quickly. | [X] | Medium |
| HVAC control | Heating, ventilation, and air conditioning should be put in place for all infrastructure to keep a constant temperature of 68 – 75 degrees Fahrenheit. | [X] | Medium |

**Physicals Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Security and Safety** | | | |
| **Control** | **Type and Explanation** | **Needs to be Implemented** | **Priority (High, Med, or Low)** |
| Office Locations | Appropriate offices should be located near the needed space for service and support. | [X] | Medium |
| Lighting | Lighting should be installed outside and inside during the night to keep all areas lit up and prevent unwanted intruders. | [X] | Medium |
| Video surveillance | Video surveillance should be put in place to monitor all security areas and discourage unwanted intruders. | [X] | Medium |
| Signage | Signs should be posted to inform all persons about the areas they cannot enter. | [X] | Medium |
| Outer Locks | An increased number of locks should be implemented as security increases to only allow authorized persons to enter. | [X] | Medium |
| Fire detection and suppression | A system should be put in place to detect a fire and put it out as quickly as possible to prevent data loss or damage. | [X] | High |

**Compliance Checklist**:

|  |  |  |
| --- | --- | --- |
| **Compliance Regulation/Standard** | **Needs to be Implemented [X]** | **Explanation** |
| **Customer Financial Data** |  |  |
| General Data Protection Regulation (GDPR) | [X] | GDPR compliance is needed to protect all customer financial data that deals internationally in the European Union. |
| Payment Card Industry Data Security Standard (PCI DSS) | [X] | All credit card processes should be monitored and in compliance with the PCI DSS to keep all payments and cardholders' data secure. |
| Health Insurance Portability and Accountability Act (HIPPA) | [] | HIPPA keeps all healthcare data secure and verifies that only individuals with access to it need to see it. |
| System and Organizations Controls (SOC type 1) | [X] | SOC is used to access financial and data security and verify that it is compliant. |
| Federal Energy Regulatory Commission – North American Electric Reliability (FERC-NERC) | [] | FERC-NERC regulates all energy that is provided to all infrastructures which includes the building and the internal data infrastructure locations. |
| Federal Deposit Insurance Corporation (FDIC) | [] | Federal program that backs up any financial losses. |
| Gramm-Leach-Bliley Act (GLBA) | [X] | GLBA requires financial agencies to explain information sharing practices |
| **Employee Devices** |  |  |
| General Data Protection Regulation (GDPR) | [X] | GDPR compliance is needed to protect all customer financial data that deals internationally in the European Union. Employees devices should be safeguarded against losing data. |
| Payment Card Industry Data Security Standard (PCI DSS) | [X] | All credit card processes should be monitored and in compliance with the PCI DSS to keep all payments and cardholders' data secure. Employees devices should not be used in processing card orders |
| Health Insurance Portability and Accountability Act (HIPPA) | [] | HIPPA keeps all healthcare data secure and verifies that only individuals with access to it need to see it. |
| System and Organizations Controls (SOC type 1) | [X] | SOC is used to access financial and data security and verify compliance. |
| National Institute of Standards and Technology (NIST) | [X] | NIST provides recommendations on best practices used with technology. |
| Fair Labor Standards Act (FLSA) | [X] | FLSA verifies that employees are supervised when using sensitive information. |
| Telework Enhancement Act (TEA) | [] | TEA oversees employees who work from home and use their own devices. This will not be accepted at XYZ. |
| **Server Infrastructure** |  |  |
| General Data Protection Regulation (GDPR) | [X] | GDPR compliance is needed to protect all customer financial data that deals internationally in the European Union. |
| Payment Card Industry Data Security Standard (PCI DSS) | [X] | All credit card processes should be monitored and in compliance with the PCI DSS to keep all payments and cardholders' data secure. |
| Health Insurance Portability and Accountability Act (HIPPA) | [] | HIPPA keeps all healthcare data secure and verifies that only individuals with access to it need to see it. |
| System and Organizations Controls (SOC type 1) | [X] | SOC is used to access financial and data security and verify that it is compliant. |
| Federal Energy Regulatory Commission – North American Electric Reliability (FERC-NERC) | [] | FERC-NERC regulates all energy that is provided to all infrastructures which includes the building and the internal data infrastructure locations. |
| National Infrastructure Protection Plan (NIPP) | [X] | NIPP regulates how infrastructures in the community work together to manage risks |
| **Network Infrastructure** |  |  |
| General Data Protection Regulation (GDPR) | [X] | GDPR compliance is needed to protect all customer financial data that deals internationally in the European Union. |
| Payment Card Industry Data Security Standard (PCI DSS) | [X] | All credit card processes should be monitored and in compliance with the PCI DSS to keep all payments and cardholders' data secure. |
| Health Insurance Portability and Accountability Act (HIPPA) | [] | HIPPA keeps all healthcare data secure and verifies that only individuals with access to it need to see it. |
| System and Organizations Controls (SOC type 1) | [X] | SOC is used to access financial and data security and verify that it is compliant. |
| Federal Energy Regulatory Commission – North American Electric Reliability (FERC-NERC) | [] | FERC-NERC regulates all energy provided to all infrastructures, including the building and the internal data infrastructure locations. |
| Cybersecurity and Infrastructure Security Agency (CISA) | [X] | CISA works to help keep companies updated to defend against threats and keep them more secure. |

**Activity Assessment**

The following has been reviewed from XYZ Financial Services:

* Audit Scope
* Considered Risks
* Controls and their relevance and risk priority
* Compliance and their regulations

**Critical Findings** (Must Be Addressed Immediately):

1. A firewall should be set up after the internet enters the facility but before the router.
2. Set up an Intrusion Detection System to detect and prevent worms, spyware, and viruses.
3. Perform a deep packet inspection on all BYOD devices annually.
4. Set up access controls on all employees and financial departments to have least privilege.
5. Set up a backup system that performs a backup of all financial and technical data.
6. All emails and internal and external data should be encrypted.
7. Backup power should be installed to the data closet as a UPS or generator.
8. Setup a HVAC to the data center and closet.

**Findings** (Should Be Addressed, but No Immediate Need):

1. Design employee training to review cybersecurity to prevent unwanted threats.
2. Passwords should be updated to 16 characters with upper, lowercase, and a symbol.
3. Signage should be displayed to signify video surveillance and where unauthorized personnel cannot go. This acts as a protective wall.
4. Video surveillance should be set up outside and inside the facility.
5. Develop a Business Continuity Plan.
6. Develop a disaster recovery plan.
7. Verify compliance with Gramm Leach Bliley and Payment Card Industry Data Security Standard.
8. A data closet should be set up to hold servers, cables, laptop, switches, and routers.

Summary/Recommendations:

In summary, the audit revealed critical findings that we recommend implementing soon. Other findings are not as critical but we recommend that action on these items be completed in the next 90 days. Completing these recommendations will enhance the security, compliance, and data retention.

Sincerely,

Austin Clinefelter

IT Specialist

XYZ Financial Services