**Botium-Toys-Security-Audit**

**Global Objective:**

Run a internal audit for a fictional company named "Botium Toys"

**Specific Objectives:**

1. Review the IT manager’s scope, goals, and risk assessment report.

2. Stick to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

3. Perform an internal audit by completing a controls and compliance checklist.

4. Secure system controls.

5. Hold a better posture on security matters for the internal network.

6. Look forward to meeting compliance requirements.

**Scenario:**

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy’s online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She's worried about maintaining compliance and business operations as the company grows without a clear plan. She believes an internal audit can help better secure the company’s infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

**Plan:**

1. Evaluate current assets.
2. Identify and sort out vulnerabilities.
3. Apply policies, protocols, and procedures to make sure they are working as intended and being implemented by employees.
4. Complete Controls assessment.
5. Complete Compliance checklist.
6. Apply policies, protocols, and procedures to make sure they are working as intended and being implemented by employees.
7. Consider how to summarize your recommendations clearly and concisely to stakeholders.

**Current Assets**

Assets managed by the IT Department include:

● On-premises equipment for in-office business needs

● Employee equipment: end-user devices (desktops/laptops, smartphones),

remote workstations, headsets, cables, keyboards, mice, docking stations,

surveillance cameras, etc.

● Storefront products available for retail sale on site and online; stored in the

company’s adjoining warehouse

● Management of systems, software, and services: accounting,

telecommunication, database, security, ecommerce, and inventory

management

● Internet access

● Internal network

● Data retention and storage

● Legacy system maintenance: end-of-life systems that require human monitoring

**Categorization of controls assessments**

| **Administrative/Managerial Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control Type and purpose** | **Rank** | **Implemented (yes or no)** |
| Least Privilege | Preventative. Reduce risk and overall impact of malicious insider or compromised accounts | High |  |
| Disaster recovery plans | Corrective. Provide business continuity | High |  |
| Password policies | Preventative. Reduce likelihood of account compromise through brute force or dictionary attack techniques | High |  |
| Access control policies | Preventative. Bolster confidentiality and integrity by defining which groups can access or modify data | High |  |
| Account management policies | Preventative. Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage | Medium |  |
| Separation of duties | Preventative. Reduce risk and overall impact of malicious insider or compromised accounts | High |  |

| **Technical Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control Type and purpose** | **Rank** | **Implemented** |
| Firewall | Preventative. To filter unwanted or malicious traffic from entering the network | High | Yes |
| IDS/IPS | Detective. To detect and prevent anomalous traffic that matches a signature or rule | Medium |  |
| Encryption | Deterrent. Provide confidentiality to sensitive information | High |  |
| Backups | Corrective. Restore/recover from an event |  |  |
| Password management | Preventative. Reduce password fatigue |  |  |
| Antivirus (AV) software | Preventative. Scans to detect and quarantine known threats |  |  |
| Manual monitoring, maintenance, and intervention | Preventative. Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems |  |  |

| **Physical/Operational Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control Type and purpose** | **Rank** | **Implemented** |
| Time-controlled safe | Deterrent. Reduce attack surface and overall impact from physical threats |  |  |
| Adequate lighting | Deterrent. Deter threats by limiting “hiding” places |  |  |
| Closed-circuit television (CCTV) | Preventative/Detective. Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions |  |  |
| Locking cabinets (for network gear) | Preventative. Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear |  |  |
| Signage indicating alarm service provider | Deterrent. Deter certain types of threats by making the likelihood of a successful attack seem low |  |  |
| Locks | Deterrent/Preventative. Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets |  |  |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative. Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc. |  |  |