# A Security Audit conducted for a Fictional Company named Botium Toys

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location. However, its online presence has grown, attracting customers in the U.S. and abroad. 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 expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. 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 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, and completing a risk assessment. The goal of the audit is to provide an overview of the risks the company might experience due to the current state of their security posture. The IT manager wants to use the audit findings as evidence to obtain approval to expand his department.

**My task is to review the IT manager’s scope, goals, and risk assessment. Then, perform an internal audit to complete a controls assessment and compliance checklist.**

## Current assets of Botium Toys

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.
* Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
* Internet access
* Internal network
* Vendor access management
* Data center hosting services
* Data retention and storage
* Badge readers
* Legacy system maintenance: end-of-life systems that require human monitoring

**Controls assessment**

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented (X)** | **Priority** |
| Least Privilege | Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs | X | High |
| Disaster recovery plans | Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration | X | High |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High |
| Access control policies | Preventative; increase confidentiality and integrity of data | X | High |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees | X | Medium |
| Separation of duties | Preventative; ensure no one has so much access that they can abuse the system for personal gain | X | Medium |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Firewall | Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network | Not Applicable (N/A) | Not Applicable (N/A) |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly | X | High |
| Encryption | Deterrent; makes confidential information/data more secure (e.g., website payment transactions) | X | Medium |
| Backups | Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan | X | High |
| Password management system | Corrective; password recovery, reset, lock out notifications | X | Medium |
| Antivirus (AV) software | Corrective; detect and quarantine known threats | X | High |
| Manual monitoring, maintenance, and intervention | Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities | X | High |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Time-controlled safe | Deterrent; reduce attack surface/impact of physical threats | X | Medium |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | Medium |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | High |
| Locking cabinets (for network gear) | Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear | X | Medium |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low | X | Low |
| Locks | Preventative; physical and digital assets are more secure | X | High |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative; detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc. | X | Medium |

**Compliance Assessment Checklist**

* **The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

**Explanation:** Not Applicable (N/A)

* **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 a E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident.

**Explanation:** Botium company needs to adhere to this regulation because if they are not transparent about the data they are holding about an E.U. citizen and why they are holding the data, this is an infringement that will result to Botium Toys organization been fined.

* **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

**Explanation:** Botium Toys needs to adhere to this because many of their customers will be purchasing toys online via their credit cards and Botium toys adherence to this compliance standard will help reduce Credit card fraud

* **The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients’ health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

**Explanation:** Not Applicable (N/A)

* **System and Organizations Controls (SOC type 1, SOC type 2)**

The SOC1 and SOC2 are a series of reports that focus on an organization’s user access policies at different organizational levels. They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

**Explanation:** Botium Toys needs to adhere to this to mitigate risks.