**Scenario**

*This scenario is based on a fictional company:*

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.

Your 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.

# Step #1 - Analyze the Audit scope and goals and Risk Assessment

# Botium Toys: Audit scope and goals

**Summary:** Perform an audit of Botium Toys’ cybersecurity program. The audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as “high risk,” and present an overall strategy for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

**Scope:** (*Note that the scope is not constant from audit to audit. However, once the scope of the audit is clearly defined, only items within scope should be audited. In this scenario, the scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures*).

Botium Toys internal IT audit will assess the following:

* Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
* Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
* Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
* Ensure current technology is accounted for. Both hardware and system access.

**Goals:** (*The goal of an audit is the desired deliverables or outcomes. The goal of an audit can be to achieve compliance, to identify weaknesses or vulnerabilities within an organization, and/or to understand failures in processes and procedures and correct them. In this scenario, the IT manager set the goals. He is expecting a report of the current security posture of the organization and recommendations for improving the security posture of the organization, as well as justification to hire additional cybersecurity personnel.)*

The goals for Botium Toys’ internal IT audit are:

* To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
* Establish a better process for their systems to ensure they are compliant
* Fortify system controls
* Implement the concept of least permissions when it comes to user credential management
* Establish their policies and procedures, which includes their playbooks
* Ensure they are meeting compliance requirements

# Botium Toys: Risk assessment

## 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.
* 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

## Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have the proper controls in place and may not be compliant with U.S. and international regulations and standards.

## Control best practices

The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to managing assets. Additionally, they will need to determine the impact of the loss of existing assets, including systems, on business continuity.

## Risk score

On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to necessary compliance regulations and standards.

## 

## Additional comments

The potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be lost. The likelihood of a lost asset or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not adhering to required regulations and standards related to keeping customer data private.

# Step #2 - Conduct the audit - Controls Assessment

# Controls assessment

## Current assets

Assets managed by the IT Department include:

* On-premises equipment for in-office business needs
* Employee equipment: end-user devices (desktops/laptops, Smartphone's), 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

| **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 | MEDIUM |
| Access control policies | Preventative; increase confidentiality and integrity of data | X | MEDIUM |
| Account management policies | Preventative; reduce attack surface and limit overall impact from disgruntled/former employees | X | HIGH |
| 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 | X | HIGH |
| 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 | HIGH |
| 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 | LOW |

| **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 | HIGH |
| Adequate lighting | Deterrent; limit “hiding” places to deter threats | X | HIGH |
| 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 | HIGH |
| Signage indicating alarm service provider | Deterrent; makes the likelihood of a successful attack seem low | X | HIGH |
| 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 | HIGH |

# Step #3 - Conduct the audit - Compliance checklist

# Compliance 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

* **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 Toys is a small toy making company in the US and as per the instructions given it is accepting orders from abroad also i.e. which may include European countries so for sure Botium Toys should follow the guidelines, procedures and standard of GDPR.

* **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:** As per the instructions given, **Botium Toys** is accepting orders from abroad using electronic card payments so definitely this company should adhere to PCI DSS rules and regulations.

* **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:**

* **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:** As per the instructions given assessing user permissions is also considered. So assessing how user permissions are handled and what permissions do the users have (cross checking) are part of the assessment. Hence Botium Toys should adhere to System and Organizations Controls (SOC type1, SOC type2) rules and regulations.