Botium Toys: Audit scope and goals

1. Scope:

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.

2. Goals:

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

3. Controls assessment

3.1. Administrative Control

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**	**Very 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**	**Medium**
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**	**Very High**
Account management	Preventative; reduce attack surface		

Administrative Controls			
policies	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**	**High**

3.2. **Technical Controls**

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		**N/A**
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	**X**	**Low**
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**	**Medium**
Password management system	Corrective; password recovery, reset, lock out notifications	**X**	**High**
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**

3.3. **Physical Controls**

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**	**Low**
Adequate lighting	Deterrent; limit “hiding” places to deter threats		
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	**X**	**Very High**
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	**X**	**Very High**
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low		**N/A**
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**

4. 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: The establishment and operation of the Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC) are imperative due to the potential disturbances that may arise within the electric line caused by Botium Toys, despite its classification as a small-scale U.S. business.

☑ **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:

The implementation and enforcement of the General Data Protection Regulation (GDPR) are essential in order to establish a fail-safe mechanism that effectively addresses any potential data breaches, as it offers valuable assistance in mitigating and resolving such incidents.

☐ **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:

Considering the current operational context of Botium Toys, where the majority of transactions are conducted through cheques and cash, with card payments being infrequent, the immediate necessity of implementing the Payment Card Industry Data Security Standard (PCI DSS) is not apparent. However, it is crucial to acknowledge that if the volume of card transactions were to substantially increase in the future, the consideration of adopting PCI DSS could become pertinent to ensure the security of such transactions.

☑ **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:

Health information holds significant importance as it pertains to sensitive and highly personal details of an individual's well-being. Therefore, the implementation of The Health Insurance Portability and Accountability Act (HIPAA) serves as a crucial measure in preventing the unauthorized sharing of an employee's health-related information without their explicit consent. HIPAA's provisions play a pivotal role in safeguarding the

confidentiality and privacy of such sensitive data, ensuring that individuals maintain control over the disclosure and dissemination of their personal health information.

☑ **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 Boston Toys endeavors to establish a system that adheres to the principle of least permissions in user credential management and fulfills the necessary compliance requirements, the implementation of System and Organization Controls (SOC type 1 and SOC type 2) would be instrumental in fortifying the system to achieve both objectives. The adoption of SOC type 1 and SOC type 2 assessments provides a robust framework for evaluating and verifying the effectiveness of internal controls, risk management practices, and operational processes. By undergoing these assessments, Boston Toys can enhance the integrity and security of their system, ensuring that user credentials are managed in a manner that aligns with the principle of least permissions and complies with relevant regulations and standards.