Botium Toys: Audit scope and goals

Audit 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.

Audit Goals:

- 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

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, 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

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	**X**	High

Administrative Controls			
	restoration		
Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	**X**	High/Med
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**	High
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain	**X**	High

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	NA	NA
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**	Med
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	**X**	High/Med

Password management system	Corrective; password recovery, reset, lock out notifications	**X**	High
Antivirus (AV) software	Corrective; detect and quarantine known threats	**X**	High/Med
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**	Med
Adequate lighting	Deterrent; limit “hiding” places to deter threats	**X**	Low
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation - Already present		NA
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	**X**	Med
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 - Already in place	NA	NA
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; a system to detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.	NA	NA

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: NA

☒ **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 needs to adhere to GDPR because they conduct business and collect personal information from people worldwide, including the E.U.

☒ **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 PCI DSS because they store, accept, process, and transmit credit card information in person and online.

☐ **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: NA

☒ **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 establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.

Summary:

Based on the audit scope and goals, it is critical for Botium Toys to prioritize the implementation of least privilege, disaster recovery plans, and strong password policies. Strengthening access control and account management policies should also be given high priority. Additionally, implementing separation of duties will enhance security. It is recommended to implement an intrusion detection system (IDS), encryption for confidential data, regular backups, and antivirus software. Manual monitoring, maintenance, and intervention for legacy systems should continue. These recommendations align with the audit goals, NIST CSF, and compliance requirements. By addressing these findings and implementing the recommended measures, Botium Toys can fortify its security controls, ensure compliance, and enhance overall cybersecurity posture.

Adhering to compliance regulations and standards is crucial for Botium Toys for several reasons:

1. Legal requirements: Compliance regulations and standards are often established by governing bodies and regulatory authorities to ensure the protection of sensitive information, customer data, and privacy. Failure to comply with these regulations

can result in legal consequences, fines, and legal actions against the company. Adhering to these regulations helps Botium Toys avoid legal liabilities and maintain a positive reputation.

2. Data protection and privacy: Compliance regulations and standards often focus on data protection and privacy, aiming to safeguard customer information from unauthorized access, data breaches, and misuse. By adhering to these regulations, Botium Toys demonstrates its commitment to protecting customer data, which enhances trust and confidence among customers, partners, and stakeholders.
3. Industry best practices: Compliance regulations and standards are typically based on industry best practices and frameworks established by cybersecurity experts and organizations. Following these standards helps Botium Toys align its security practices with the industry's recommended approaches, ensuring that the company adopts effective security measures and mitigates potential vulnerabilities.
4. Risk management: Compliance regulations and standards assist in identifying and managing risks associated with cybersecurity. They provide guidelines and requirements for implementing controls, conducting risk assessments, and developing incident response plans. By adhering to these standards, Botium Toys can proactively identify and address security vulnerabilities, reducing the likelihood of security incidents and their potential impact on the business.
5. Competitive advantage: Adhering to compliance regulations and standards can provide Botium Toys with a competitive advantage in the market. Demonstrating compliance shows potential customers, partners, and investors that the company takes cybersecurity seriously and has implemented robust security measures. This can enhance the company's reputation, attract new customers, and open opportunities for partnerships and collaborations.

Overall, adherence to compliance regulations and standards is essential for Botium Toys to protect sensitive information, maintain legal compliance, mitigate risks, build trust with stakeholders, and gain a competitive edge in the industry.