**Botium Toys Security Audit1**

**Scope:** 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.

**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

**The biggest risks are :**

* Inadequate management of assets
* Proper controls are not in place
* May not be compliant with U.S. and international regulations and guidelines
* Current risk score is 8/10 (high), due to a lack of controls and adherence to compliance regulations and standards

**Controls that must be taken immediately versus in the future:**

Physical controls

Technical controls

Administrative controls

**Standards/Regulations to be complied:**

1.NST Cyber security Framework –Botium toys needs to comply to the NST cybersecurity framework so as to secure the company’s infrastructure and help identify and mitigate potential risks, threats or vulnerabilities to critical assets

2. GDPR-Botium toys needs to comply with the GDPR because the general data protection regulation protects information of all our customers in the European

3. PCI DSS- Botium toys needs to comply with PCI DSS because this standard protects information of our online users and handles payment card security for all users.

# **Controls assessment4,**

## 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 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 | HIGH/MEDIUM |
| 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 | 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 | 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 | LOW |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | MEDIUM |
| 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 |