Botium Toys

Controls and compliance checklist

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☐	☑	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☑	☐	Locks (offices, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
□	☑	Only authorized users have access to customers' credit card information.
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
□	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
□	☑	E.U. customers' data is kept private/secured.
☑	□	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
□	☑	Ensure data is properly classified and inventoried.
☑	□	Enforce privacy policies, procedures, and processes to properly document and maintain data.

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

Yes	**No**	**Best practice**
□	☑	User access policies are established.
□	☑	Sensitive data (PII/SPII) is confidential/private.
□	☑	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
□	☑	Data is available to individuals authorized to access it.

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Recommendations

Administrative/Managerial Controls			
Control Name	**Control Type**	**Control Purpose**	**Recommended Action**
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts	Identify what the least amount of access is needed for a user to perform their work.
Disaster recovery plans	Corrective	Provide business continuity	Create a DR plan and process. Perform simulations to prepare for it.

Administrative/Managerial Controls			
Password policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack techniques	Bolster password complexity requirements for internal team and customers.
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data	Conduct an access review and only grant necessary permissions for users.
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage	Create full user MAC processes, which includes onboarding, changes, offboarding for users and customers.
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts	Identify clear responsibilities of roles within the company and create and assign the relevant access groups to users.

Technical Controls			
Control Name	**Control Type**	**Control Purpose**	**Recommended Action**
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network	Regularly review set firewall rules and adjust when necessary.
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule	Implement an IDS ASAP to mitigate risk and become GDPR compliant. This should also be accompanied with the use of a SIEM tool.
Encryption	Deterrent	Provide confidentiality to sensitive information	Implement encryption for all customer and user information to mitigate SPII breach and identity theft.
Backups	Corrective	Restore/recover from an event	Conduct regular backups and take snapshots of existing data, rules, configs for at least the critical data first.
Password management	Preventative	Reduce password fatigue	Implement the use of 1 centralized password management system.

Antivirus (AV) software	Preventative	Scans to detect and quarantine known threats	Ensure your AV is reliable and up to date. There should be regular processes for monitoring and parsing logs.
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems	Since legacy systems are being used and monitored, their needs to be methods in place for intervention when needed.

Physical/Operational Controls			
Control Name	**Control Type**	**Control Purpose**	**Recommended Action**
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical threats	If storing valuables in a safe, ensure the safe is industry standard and time controlled.
Adequate lighting	Deterrent	Deter threats by limiting “hiding” places	Implement industry security lighting to eliminate low lit areas. These can be solar powered for the lights outside the store.

Closed-circuit television (CCTV)	Preventative/Detective	Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions	Regularly check if cameras are online and recording. Ensure backups of footage are being stored and protected. Ensure you're complying with government laws on CCTV usage.
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear	All switches, routers, servers, UPS, need to be in an airflow optimised locking cabinet.
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low	Display signage indicating surveillance and monitoring of the store.
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets	Regularly check locks are in good condition and have no sign of attempted picking. Replace locks when needed. This includes doorknobs and padlocks.

Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.	Regularly maintain and check all fire systems. Get a third party to come on site and test.

Resources

Case Study

Botium Toys: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope: The scope of this audit is defined as the entire security program at Botium Toys. This includes their assets like employee equipment and devices, their internal network, and their systems. You will need to review the assets Botium Toys has and the controls and compliance practices they have in place.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices that need to be implemented to improve Botium Toys' security posture.

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.

- Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Data retention and storage
- Legacy system maintenance: end-of-life systems that require human monitoring

Risk assessment

Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully 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 identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and 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 compliance best practices.

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 at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

- Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
- Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
- Access controls pertaining to least privilege and separation of duties have not been implemented.
- The IT department has ensured availability and integrated controls to ensure data integrity.
- The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
- Antivirus software is installed and monitored regularly by the IT department.
- The IT department has not installed an intrusion detection system (IDS).
- There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
- The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
- Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight

characters, a combination of letters and at least one number; special characters).

- There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
- While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
- The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

Control Categories

Controls within cybersecurity are grouped into three main categories:

- Administrative/Managerial controls
- Technical controls
- Physical/Operational controls

Administrative/Managerial controls address the human component of cybersecurity. These controls include policies and procedures that define how an organization manages data and clearly defines employee responsibilities, including their role in protecting the organization. While administrative controls are typically policy based, the enforcement of those policies may require the use of technical or physical controls.

Technical controls consist of solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV) products, encryption, etc.

Technical controls can be used in a number of ways to meet organizational goals and objectives.

Physical/Operational controls include door locks, cabinet locks, surveillance cameras, badge readers, etc. They are used to limit physical access to physical assets by unauthorized personnel.

Control types

Control types include, but are not limited to:

1. Preventative
2. Corrective
3. Detective
4. Deterrent

These controls work together to provide defense in depth and protect assets. **Preventative controls** are designed to prevent an incident from occurring in the first place. **Corrective controls** are used to restore an asset after an incident. **Detective controls** are implemented to determine whether an incident has occurred or is in progress. **Deterrent controls** are designed to discourage attacks.