Botium Toys: Scope, goals, and risk assessment report

Scope and goals of the audit:

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 related to the implementation of controls and compliance best practices.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices 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 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 with 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 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 is 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:

1. Administrative/Managerial controls: These 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.

2. Technical controls: These 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 several ways to meet organizational goals and objectives.

3. Physical/Operational controls: These 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 controls are designed to prevent an incident from occurring in the first place.
2. Corrective controls are used to restore an asset after an incident.
3. Detective controls are implemented to determine whether an incident has occurred or is in progress.
4. Deterrent controls are designed to discourage attacks.

These controls work together to provide defense in depth and protect assets.

Review the following charts for specific details about each type of control and its purpose.

Administrative/Managerial Controls		
Control Name	**Control Type**	**Control Purpose**
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts
Disaster recovery plans	Corrective	Provide business continuity
Password policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack

Administrative/Managerial Controls		
		techniques
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts

Technical Controls		
Control Name	**Control Type**	**Control Purpose**
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule
Encryption	Deterrent	Provide confidentiality to sensitive information
Backups	Corrective	Restore/recover from an event
Password management	Preventative	Reduce password fatigue
Antivirus (AV) software	Corrective	Detect and quarantine known threats
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Physical/Operational Controls		
Control Name	**Control Type**	**Control Purpose**
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical threats
Adequate lighting	Deterrent	Deter threats by limiting “hiding” places
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
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets
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.

Controls and compliance checklist

The below controls assessment checklist is prepared after referring to the information provided in the Scope, Goals and Risk Assessment report mentioned in the above part of this report.

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.)

The below compliance checklist is prepared after referring to the information provided in the Scope, Goals and Risk Assessment report and controls assessments checklist mentioned in the above part of this report.

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.

Recommendations: This section provides recommendations on controls and actions that can be taken by IT Manager, Botium Toys, and safeguard their assets and data. Also be compliant with industry standards.

1. There are certain best practices to be established such as
    a. Principle of Least Privilege: Limited users must be given access to data, assets or other resources.
    b. Disaster recovery Plans: Proper backup plans need to be employed on assets, data, etc.
    c. Password Policies: Passwords must be according to the rules and guidelines stated by password policies. E.g. minimum characters, upper/lower case, numbers and so on.
    d. Separation of duties: Different types of tasks should be assigned to respective personnel, instead of a single person/limited user.
    e. IDS: Implement any one detective software that checks for weak points/defects in an IT System.
    f. Encryption: Store/transmit data in an encrypted manner so that anyone outside the network/organization cannot read it.
    g. Password Management System: Implement a system that can take quicker actions on password reset/password renew queries.

2. The above controls should be implemented to stay compliant with the regulations like PCIDSS, for maintaining credit card details of users and processing them.
3. A proper classification of the assets is needed to better understand the IT Infrastructure and its weak points and to quickly isolate the impacted systems or assets during a breach.