Solution

Step 1 Access supporting materials (Listing the audit goals, scope, and risk assessment)

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.

Risk Assessment:

Risk Assessment:

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.

- **High risk**, 7 - 10 score
- **Medium risk**, 4-6 score
- **Low risk**, 0 - 3 score

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 le ers 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.

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

Step 2 Conduct the audit (Controls and compliance checklist)

Control categories:

Administrative 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 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 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:

When conducting the controls and compliance checklist, we should review the Botium Toys" Scope, Goal, and Risk Assessment report. Sldo when completing the checklist, the focus should be on:

- The assets currently managed by the IT department
- The "Additional Comments" in the Risk assessment section

Then, select "yes" or "no" to answer the question: Does Botium Toys currently have this control in place?

Risk Score is already mentioned in the "Additional Comments" Section of the Risk assessment section

Yes	**No**	**Control**
	X	Least Privilege
	X	Disaster recovery plans
X		Password policies

	X	Separation of duties
X		Firewall
	X	Intrusion detection system (IDS)
	X	Backups
X		Antivirus software
X		Manual monitoring, maintenance, and intervention for legacy systems
	X	Encryption
	X	Password management system
X		Locks (offices, storefront, warehouse)
X		Closed-circuit television (CCTV) surveillance
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Controls assessment checklist

Payment Card Industry Data Security Standard (PCI DSS)		
Yes	No	Best Practice
	X	Only authorized users have access to customers' credit card information.
	X	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	X	Implement data encryption procedures to better secure credit card transaction

Payment Card Industry Data Security Standard (PCI DSS)		
		touchpoints and data.
	X	Adopt secure password management policies.

Compliance checklist 1

General Data Protection Regulation (GDPR)		
Yes	No	Best Practice
	X	E.U. customers' data is kept private/secured.
X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
	X	Ensure data is properly classified and inventoried.
X		Enforce privacy policies, procedures, and processes to properly document and maintain data.

Compliance checklist 2

System and Organizations Controls (SOC type 1, SOC type 2)		
Yes	No	Best Practice
	X	User access policies are established.
	X	Sensitive data (PII/SPII) is confidential/private.
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
X		Data is available to individuals authorized to access it.

Compliance checklist 3

Recommendations:

With the current state of the company, there are multiple potential vulnerabilities. Some of these vulnerabilities can be fixed by:

- Implementing a proper RBAC (Role Based Access Control). **Risk 8/10**
    - Without a proper RBAC our employees will have access to specific privileges they shouldn't have permissions for.
    - Ensuring there is a Least Privileged role is implemented, therefore not everyone has the same permissions
    - Splitting up the tasks and roles to the authorized personnel of that role
- Implementing proper security measurements. **Risk 8/10**
    - Have a backup read to be implemented, and have it it updated frequently
    - Only allow authorized users to see PII/SPII
    - Start a Disaster Recovery Plan for any possible situations that the company can come across, and implement a IDS(Intrusion Detection System)
    - Proper encryption methods when storing SPII/PII
    - Proper password management and implement a more complex password requirement for employees and other kinds of users
    - Ensuring All kinds of customer data is kept private and secured

Thank you for taking the time and reading this assessment. I hope you take into consideration my recommendations. If you have any questions, feel free to email me.