Botium Toys

Internal Security Audit

Jason Ash
Security Analyst at Botium Toys

Google Cybersecurity Certification

Course 2, Module 2

Portfolio Activity

24 December, 2025

Background

Botium toys is a fictional, small U.S. toy developer, manufacturer, and distributor. We have been experiencing rapid growth at our single physical location that serves as our main office, storefront, and warehouse. Our Website has enabled our business to attract customers throughout the U.S. and internationally. Our Information Technology (IT) Department is an integral part to supporting our online presence as we expand to markets worldwide.

To this end, our Chief Information Officer (CIO) has scheduled an internal security audit to be conducted. Concerns include regulatory compliance and ensuring efficient business operations, and these issues will be addressed with a clear, unified, updated policies and procedures in collaboration with managerial and executive stakeholders who will receive recommendations at the conclusion of this audit. The goals and focus of this audit will center around mitigating potential risks, threats, and vulnerabilities to critical assets managed by the IT Department and company infrastructure. Particular areas of concern are compliance with accepting and online payments by adhering to Payment Card Industry Data Security Standard (PCI DSS) standards and EU GDPR data protection and privacy laws.

The CIO additionally will review our compliance with implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Consequently, the major sections of the audit are its scope and goals, a listing of assets managed by IT, and a risk assessment. The overarching goal of this audit is to provide an overview of the risks that create liability for Botium Toys if our current security posture continues unimproved.

Scope and goals

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.

Summary of Current IT Assets

- On-premises office equipment (desktop computers and monitors, LAN-line phones, scanners, copiers, fax machines, and coffee makers)
- Mobile office equipment for on-premises and remote use: laptops, smartphones, and docking stations
- Peripherals: Headsets, keyboards, and mice
- Infrastructure assets: Security cameras, cables, etc.
- Management of systems, software, and services: accounting, telecommunication, database, security, e-commerce, and inventory management
- Storefront products stored in our adjoining warehouse available for sale to retail partners and third-party vendors and directly through our Website
- Internet access and network: Servers, firewalls, SIEM tools, and network monitoring tools
- Data retention and storage: Local servers, safes, and file cabinets
- Legacy systems (especially in the manufacturing, warehouse, shipping workstations that will have to be continually manually monitored since they are end-of-life and no longer receiving security updates)

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. 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.

Controls Assessment Checklist

Does Botium Toys currently have this control in place?

Control	Yes	No	Comment
Least privilege		X	Access controls pertaining to least privilege and separation of duties have not been implemented.
Disaster recovery plans		X	There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
Password policies		X	Although a password policy exists, its requirements are nominal (such as your current password cannot be the same as

Control	Yes	No	Comment
			your last three passwords, it cannot contain more than the same digit or letter repeated three times in a row, and it cannot match a word found in most English dictionaries). These requirements are not consistent with current best practice complexity requirements.
Separation of duties		X	Access controls pertaining to least privilege and separation of duties have not been implemented.
Firewall	X		The IT Department has a firewall that blocks traffic based on an appropriately defined set of security rules.
Intrusion detection system		X	The IT Department has not yet installed an intrusion detection system (IDS).
Backups		X	The company does not have backups of critical data.
Antivirus software	X		Antivirus software is installed and monitored regularly by the IT Department.
Manual monitoring, maintenance, and interventions for legacy systems		X	While legacy systems are monitored and maintained, no regular schedule is in place for these tasks and intervention methods are unclear.
Encryption		X	Encryption is not currently used to ensure the confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
Password management system		X	No centralized password management system that enforces the password policy's minimum requirements is in place. Moreover, when employees and vendors submit a ticket to the IT Department to recover and reset their password, lack of a centralized password management system results in significant delays and negatively impacts productivity.
Locks (office, storefront, warehouse, shipping, and distribution)	X		Locks are sufficient for building security.
Closed-circuit television (CCTV) surveillance	X		The closed-circuit television (CCTV) surveillance system is up-to-date with the caveat that security footage is not backed up off site.
Fire detection/prevention (fire alarm, sprinkler system, etc.)	X		The fire detection and prevention systems are fully functional and are regularly inspected by the municipal Fire Department.

Compliance Checklist

Does Botium Toys currently adhere to this compliance best practice?

Payment Card Industry Data Security Standard (PCI DSS)			
Best Practice	**Yes**	**No**	**Comment**
Only authorized users have access to customers' credit card information.		X	Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.		X	Encryption is not currently used to ensure the confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
Data encryption procedures are implemented to secure credit card transactions and data.		X	
Adopt secure password management policies.		X	Current password requirements are inadequate for access and authentication controls. Moreover, no centralized password management system that enforces the password policy's minimum requirements is in place making policies impossible to enforce.
General Data Protection Regulation (GDPR)			
A plan is in place to notify E.U. customers within 72 hours if their data is compromised or a breach occurs.	X		Although the IT Department has established a plan to notify E.U. customers within 72 hours if there is a security breach and privacy policies, procedures, and processes have been developed and are enforced by the IT Department to properly document and maintain data, lack of PCI DSS encryption and backups means the company is not yet in full compliance with GDPR regulations.
Ensure data is properly classified and inventoried	X		
Enforce privacy policies, procedures and processes to properly document and maintain data.	X		
The data of customers in the E.U. is kept private and secure		X	
System and Organizations Controls (SOC type 1, SOC type 2)			
User access policies are established		X	Currently, all employees have access to stored data, cardholder data, and customers' PII/SPII. Least privilege and separation of duties has not been implemented. An IDS does not yet exist. Password policy is weak. Locks are adequate for controlling building access.
Data is available to individuals authorized to		X	

access it			
Sensitive data (PII/SPII) is confidential and private		X	All employees have access to stored data, cardholder data, and customers' PII/SPII. Least privilege and separation of duties has not been implemented. An IDS does not yet exist. Password policy is weak. Encryption is not used to process and store credit card information.
Data integrity ensures data is consistent, complete, accurate, and has been validated	X*		The IT Department has ensured availability and integrated controls to ensure data integrity with the caveats and security risks mentioned above. *Although this compliance item technically qualifies to be checked as 'yes', with the current security risk is should be a no.

Recommendations

Recommendation	Priority
Access controls that create a separation of duties with least privilege, thereby, only giving employees access to systems and information required to perform their jobs	High
Disaster recovery plans to ensure business continuity including encrypted offsite and cloud backups (where appropriate)	High
Stringent password requirements that passwords must contain a minimum of eight characters, need to include one number and one symbol, and cannot be shared between employees	High
Installing an intrusion detection system (IDS)	High
PCI DSS encryption to ensure the confidentiality of customers' credit card information	High
A centralized password management system that enforces the password policy's minimum requirements	High
Regular schedule and standardized intervention for legacy systems	Medium
Continue to ensure that firewall and antivirus programs meet business and security needs	Medium
Access key cards to enter building and clock in and out of the timekeeping system.	Medium