Internal Security Audit Summary – Botium Toys

Introduction

This internal security audit was conducted as part of my cybersecurity portfolio and coursework for Google's Cybersecurity Professional Certificate on Coursera, within the Play It Safe: Manage Security Risks module.

The goal of this audit is to assess the current security posture of Botium Toys a fictional toy company and align its practices with the NIST Cybersecurity Framework (NIST CSF), as well as applicable compliance regulations. This audit highlights high risk vulnerabilities, provides recommendations for mitigating threats, and proposes an overall strategy to strengthen the company's cybersecurity controls, support regulatory compliance, and ensure business continuity.

Scenario

Botium Toys is a U.S.based toy company operating from a single physical location with a growing global online presence. As international sales and customer data responsibilities increase, the company's IT department faces mounting pressure to protect both infrastructure and sensitive data.

Concerned about the lack of formal procedures and increasing regulatory requirements, the IT manager has initiated an internal security audit. The audit team was tasked with reviewing current asset management, evaluating security controls, and ensuring compliance with regulations such as PCI DSS, GDPR, and SOC 1/SOC 2.

Audit Goals

- Align practices with the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)
- Establish a foundation for policy and playbook development
- Implement the principle of least privilege across access controls
- Strengthen system level security controls
- Ensure readiness for GDPR, PCI DSS, and SOC compliance
- Identify high risk vulnerabilities and recommend prioritization

Controls Assessment

Detailed tables for Administrative, Technical, and Physical controls are included in the complete audit document. Each control was evaluated based on its necessity and priority to improve Botium Toys' cybersecurity posture.

Compliance Checklist

Botium Toys must align with the following standards:

GDPR: Botium handles international customer data, including E.U. citizens. It must implement encryption, breach notification plans, and access control.

PCI DSS: As Botium processes credit card payments, it must ensure secure storage, encryption, and restricted access to payment data.

SOC 1/SOC 2: The company must implement access policies and maintain data integrity, confidentiality, and availability across its systems.

Controls and Compliance Assessment

Controls Assessment Checklist

Yes	No	Control	Explanation
	☑	Least Privilege	Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.
	☑	Disaster Recovery Plans	There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.
	☑	Password Policies	Employee password requirements are minimal, increasing the likelihood of unauthorized access to secure systems.
	☑	Separation of Duties	The CEO currently manages daily operations and payroll; this increases the risk of internal misuse.
☑		Firewall	The existing firewall effectively blocks traffic based on well defined security rules.

	☑	Intrusion Detection System (IDS)	No IDS is in place; this tool is essential for identifying and mitigating threat actor activity.
	☑	Backups	The company lacks regular backups, which could jeopardize recovery during incidents.
☑		Antivirus Software	Antivirus software is installed and consistently monitored by IT staff.
	☑	Legacy System Monitoring	Legacy systems are monitored but lack a formal schedule and clear procedures.
	☑	Encryption	No encryption is in place, exposing sensitive information to confidentiality risks.
	☑	Password Management System	A password management system is missing, limiting IT and employee efficiency.
☑		Physical Locks	The facility has functional locks for office, storefront, and warehouse.
☑		CCTV Surveillance	CCTV systems are installed and operational at the physical location.
☑		Fire Detection Systems	Fire detection and suppression systems are properly installed.

Compliance Checklist

Payment Card Industry Data Security Standard (PCI DSS)

General Data Protection Regulation (GDPR)

System and Organization Controls (SOC 1 & SOC 2)

Yes	No	Best Practice	Explanation
	☑	Only authorized users have access to	Currently, all employees have

		customers’ credit card information.	access to internal customer data including credit card details.
	☑	Credit card information is accepted, processed, transmitted, and stored in a secure environment.	The lack of encryption and unrestricted access increases vulnerability to breaches.
	☑	Implement data encryption procedures for transaction points and stored data.	Encryption is not utilized, which could compromise customer financial data confidentiality.
	☑	Adopt secure password management policies.	Password policies are minimal, and a password management system is not in place.
Yes	No	Best Practice	Explanation
	☑	E.U. customers’ data is kept private/secured.	Currently, customer financial data is not encrypted, violating GDPR data protection expectations.
☑		There is a breach notification plan within 72 hours.	Botium has a notification plan aligned with GDPR timelines.
	☑	Ensure data is properly classified and inventoried.	Assets are listed but not classified, limiting data protection strategy.
☑		Enforce privacy policies, procedures, and processes.	Privacy protocols are in place for staff handling sensitive data.
Yes	No	Best Practice	Explanation
	☑	User access policies are established.	Least privilege and role based access are not enforced; access is unrestricted.
	☑	Sensitive data (PII/SPII) is kept confidential and private.	Without encryption, customer data is exposed to potential breaches.

☑		Data integrity is preserved (accurate, complete, validated).	Internal processes maintain accurate and validated datasets.
	☑	Data is available to authorized users only.	Access is granted to all employees, regardless of operational need.

Stakeholder Memo Summary

To: IT Manager, Stakeholders
From: Jeremiah Mendoza
Date: 4/22/2025
Subject: Internal Audit – Findings & Recommendations

Critical Findings

- Lack of disaster recovery, encryption, or access control policies
- No IDS, backups, or password management tools in place
- Unrestricted data access and poor legacy system oversight
- Gaps in PCI DSS and GDPR compliance

Recommendations

- Implement least privilege access and enforce separation of duties
- Introduce encryption, password policies, and IDS tools
- Establish formal disaster recovery and backup systems
- Improve physical security via locks, CCTV, and secure enclosures
- Align access controls with SOC 1/SOC 2 and comply with GDPR & PCI DSS

Conclusion

This audit highlights key areas where Botium Toys must improve its cybersecurity posture to minimize risk, comply with regulatory requirements, and support long term growth. By implementing these high priority controls and aligning to the NIST CSF, Botium Toys can establish a stronger foundation for protecting its data, systems, and customers.