Annual Internal Security Audit
Botium Toys

Summary: The goal of this internal audit is to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as “high risk,” and present an overall strategy to improve the security posture of the organization. The audit team will document their findings, provide remediation plans and efforts, and communicate with stakeholders.

Scope: The internal IT audit will assess the following:

- Assess user permissions
- Identify existing controls, procedures, and system protocols
- Account for technology currently in use

Goals: The goals for the internal IT audit are:

- Adhere to the NIST Cybersecurity Framework (CSF)
- Establish policies and procedures to ensure compliance with regulations
- Fortify system controls

Controls assessment checklist

Select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

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, which could allow a threat actor to more easily access secure data/other assets via employee work equipment or the internal network.*
☐	☑	Separation of duties	*Needs to be implemented to reduce the possibility of fraud/access to critical data, since the company CEO currently runs day-to-day operations and manages the payroll.*
☑	☐	Firewall	*The existing firewall blocks traffic based on an appropriately defined set of security rules.*
☐	☑	Intrusion detection system (IDS)	*The IT department needs an IDS in place to help identify possible intrusions by threat actors.*
☐	☑	Backups	*The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.*
☑	☐	Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear, which could place these systems at risk of a breach.*

☐	☑	Encryption	*Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.*
☐	☑	Password management system	*There is no password management system currently in place; implementing this control would improve IT department/other employee productivity in the case of password issues.*
☑	☐	Locks (offices, storefront, warehouse)	*The store's physical location, which includes the company's main offices, store front, and warehouse of products, has sufficient locks.*
☑	☐	Closed-circuit television (CCTV) surveillance	*CCTV is installed/functioning at the store's physical location.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location has a functioning fire detection and prevention system.*

Compliance checklist

Select "yes" or "no" to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	***Explanation***
☐	☑	Only authorized users have access to customers' credit card information.	*Currently, all employees have access to the company's internal data.*

☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted and all employees currently have access to internal data, including customers' credit card information.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
☐	☑	Adopt secure password management policies.	*Password policies are nominal and no password management system is currently in place.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	***Explanation***
☐	☑	E.U. customers' data is kept private/secured.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised or there is a breach.	*There is a plan to notify E.U. customers within 72 hours of a data breach.*
☐	☑	Ensure data is properly classified and inventoried.	*Current assets have been inventoried/listed, but not classified.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees, as needed.*

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*Controls of Least Privilege and separation of duties are not currently in place; all employees have access to internally stored data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not currently used to better ensure the confidentiality of PII/SPII.*
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is in place.*
☐	☑	Data is available to individuals authorized to access it.	*While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.*

Recommendations:

Multiple controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information, including: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy system management, encryption, and a password management system.

To address gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. The company also needs to properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.

Remediation Roadmap for Botium Toys:

Short-Term (0–3 months) – Immediate Risk Reduction

Goal: Close the highest-risk gaps quickly.

- **Access Controls & Permissions**
  - Implement **Least Privilege** and **role-based access control (RBAC)**.
  - Restrict access to customer/credit card data to only authorized staff.
- **Authentication & Passwords**
  - Enforce strong **password policies** (length, complexity, rotation).
  - Roll out a **password management system** for staff.
  - Enable **multi-factor authentication (MFA)** on admin accounts.
- **Encryption**
  - Deploy **encryption for data in transit** (TLS/HTTPS everywhere).
  - Begin rollout of **disk/database encryption** for sensitive data.
- **Compliance Fixes (PCI DSS & GDPR)**
  - Encrypt cardholder data.
  - Limit who can access payment data.
  - Draft and approve **data breach notification procedures**.
- **Incident Response**
  - Develop a **basic Incident Response Plan (IRP)** with defined roles and a 72-hour reporting workflow (for GDPR).

Mid-Term (3–9 months) – Build Resilience

Goal: Strengthen detection, monitoring, and compliance frameworks.

- **Monitoring & Detection**
  - Deploy **Intrusion Detection/Prevention System (IDS/IPS)**.
  - Implement **centralized logging/SIEM** with alerting.
- **Disaster Recovery & Backups**
  - Implement **regular, automated backups** (onsite + cloud).
  - Define **Recovery Time Objectives (RTOs)** and **Recovery Point Objectives (RPOs)**.
  - Conduct first **tabletop disaster recovery drill**.
- **Separation of Duties**
  - Reassign payroll and financial duties so they are not managed by the CEO alone.
- **Data Governance**
  - Classify all assets and data by sensitivity (PII, SPII, financial, operational).
  - Update policies for **data retention and destruction**.
- **Training & Awareness**
  - Launch an **employee cybersecurity awareness program** (phishing, passwords, social engineering).

Long-Term (9–18 months) – Mature Security Posture

Goal: Build a sustainable, compliant, and auditable security framework.

- **Policy & Governance**
  - Establish a **formal Information Security Policy** approved by leadership.
  - Launch a **vendor risk management program** to assess third-party providers.
  - Perform regular **internal audits** mapped to **NIST CSF**.
- **Technology Hardening**
  - Migrate/replace **legacy systems** that cannot be secured.
  - Expand **encryption to all systems** (at rest, in use, in transit).
  - Enable **network segmentation** for sensitive data zones (e.g., PCI environment).
- **Advanced Monitoring & Testing**
  - Expand SIEM with anomaly detection.
  - Conduct **annual penetration tests** and vulnerability scans.
- **Business Continuity**
  - Mature **Disaster Recovery Plan** into a full **Business Continuity Plan (BCP)**.
  - Run **annual BCP drills** with cross-department participation.
- **Certifications & Compliance**
  - Prepare for **SOC 2 Type 2 audit readiness**.
  - Continue PCI DSS annual validation.
  - Ensure GDPR compliance through ongoing audits and privacy impact assessments.