# Security Audit

# Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

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

**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.) |

---

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the controls, frameworks, and compliance reading.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

**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. |

---

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

**Recommendations (optional):** In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

## Recommendations for the IT Department

Based on the findings of the internal IT audit, the following recommendations are provided to reduce risk, improve security posture, and align Botium Toys with industry standards and regulatory requirements.

### 1. Implement Data Encryption

Encrypt all sensitive and critical data, including customer payment information and personally identifiable information (PII), during storage, processing, and transmission. This will protect data confidentiality and support compliance with PCI DSS and GDPR requirements.

---

### 2. Enforce Strong Access Controls

Implement least privilege and separation of duties to ensure employees only have access to the data and systems required to perform their job functions. This will reduce the risk of insider threats and unauthorized data access.

---

### 3. Deploy Intrusion Detection Capabilities

Install and maintain an Intrusion Detection System (IDS) to improve the organization's ability to detect malicious activity and security incidents in a timely manner.

---

### 4. Establish Disaster Recovery and Backup Procedures

Develop and implement a disaster recovery plan and ensure regular backups of critical data are performed and tested. This will improve system resilience and support business continuity.

---

### 5. Improve Password Security and Management

Implement a centralized password management system that enforces strong password policies, including complexity, length, and rotation requirements. This will enhance authentication security and reduce productivity issues related to password recovery.

---

### 6. Formalize Legacy System Monitoring and Maintenance

Create a documented schedule and clearly defined procedures for monitoring, maintaining, and intervening in legacy systems to reduce operational and security risks.

---

### 7. Strengthen Asset Management Practices

Identify, inventory, and classify all organizational assets. Determine the potential impact of asset loss on business continuity in alignment with NIST CSF guidelines.

---

### 8. Enhance Endpoint and Equipment Security

Ensure all employee devices and equipment are securely configured, regularly updated, and protected with appropriate security controls.

---

### 9. Address Physical and Infrastructure Constraints

If physical space limits secure technology operations, consider relocating or outsourcing technological infrastructure to a separate, secured location or expanding existing facilities to better protect assets.

---

### 10. Conduct Ongoing Risk Assessments

Perform regular assessments to identify risks, threats, and vulnerabilities across systems, processes, and infrastructure. Use findings to continuously improve security controls.

---

### 11. Develop Security Governance Documentation

Create and maintain formal security governance documentation, including policies, standards, procedures, and guidelines (PSPG), and compile them into a company security handbook for employees.

---

### 12. Implement Security Awareness and Training Program

Establish regular security awareness and training programs for all employees to ensure they understand security policies, recognize common threats (such as phishing and social engineering), and follow secure practices when handling sensitive data and systems. This supports the effectiveness of technical and administrative controls and reduces human-related security risks.

# Risk-Prioritized Recommendations (Highest → Lowest)

This ranking is based on **impact × likelihood × regulatory exposure**, exactly how auditors and CISOs think.

---

## 🔴 Critical Risk (Immediate – must be fixed first)

### 1. Encrypt sensitive and payment data

**Why #1:**

- Unencrypted cardholder data = **PCI DSS failure**
- Unencrypted EU customer data = **GDPR violation**
- Data breach here = fines + legal exposure + reputational damage

➡️ This is the single most dangerous gap.

---

### 2. Enforce least privilege & separation of duties

**Why #2:**

- All employees can access PII/card data → insider threat + breach risk
- Violates PCI DSS, GDPR, SOC principles

➡️ Even *with* encryption, excessive access is still a compliance failure.

---

### 3. Implement backups & disaster recovery plan

**Why #3:**

- No backups = total data loss risk
- No DR = business could fail after ransomware, fire, or system failure

➡️ This is about **business survival**, not just security.

---

# 🟠 High Risk (Next priority)

### 4. Deploy intrusion detection (IDS)

**Why:**

- No visibility into attacks
- Breaches could go undetected for long periods

➡️ Detection is essential once prevention fails (and it always does).

---

### 5. Implement centralized password management & strong password policy

**Why:**

- Weak passwords + no enforcement = easy compromise
- Productivity issues increase shadow IT risk

➡️ This reduces both **security risk and operational friction**.

---

### 6. Secure and harden all employee endpoints

**Why:**

- End-user devices are the most common attack vector
- Compromised endpoints bypass network controls

➡️ Especially critical with remote work and legacy systems.

---

## 🟡 Medium Risk (Should be addressed, but after core fixes)

### 7. Formalize legacy system monitoring & intervention

**Why:**

- Legacy systems are inherently risky
- Lack of schedule/procedure increases uncertainty

➡️ Not immediately catastrophic, but dangerous long-term.

---

### 8. Strengthen asset management & classification (NIST CSF – Identify)

**Why:**

- You can’t protect what you don’t know you have
- Poor asset awareness increases blast radius of incidents

➡️ This underpins all other controls.

---

# 🟢 Lower Risk / Strategic Improvements

### 9. Improve physical/infrastructure layout or outsource tech operations

**Why:**

- Physical security is already strong
- This is more about scalability and resilience

➡️ Important for growth, not urgent for risk reduction.

---

### 10. Conduct regular full risk assessments

**Why:**

- Necessary for long-term governance
- Less urgent than fixing known gaps

➡️ Ongoing maturity activity.

---

### 11. Create PSPG documentation & employee handbook

**Why:**

- Policies don’t stop breaches alone
- They support enforcement and audits

➡️ Needed for compliance and consistency, but ineffective without controls.

---

## Priority summary (one line)

**Fix confidentiality first → then access → then resilience → then detection → then governance.**

## Executive Summary

The internal IT audit of Botium Toys identified significant gaps in access control, data protection, monitoring, and business continuity that expose the organization to high operational and regulatory risk. The most critical findings include the lack of encryption for sensitive customer data, excessive employee access to confidential information, and the absence of disaster recovery and backup capabilities.

These deficiencies place Botium Toys at risk of non-compliance with PCI DSS and GDPR requirements and increase the likelihood of data breaches, financial loss, and business disruption. While certain baseline controls such as firewalls, antivirus software, and physical security measures are in place, they are insufficient to mitigate the identified risks.

To improve the organization’s security posture, immediate priority should be given to implementing encryption, enforcing least privilege and separation of duties, and establishing disaster recovery and backup processes. Additional improvements should focus on enhancing detection capabilities, strengthening authentication and endpoint security, formalizing legacy system management, and improving asset classification in alignment with the NIST Cybersecurity Framework. Long-term efforts should include developing comprehensive security governance documentation and conducting ongoing risk assessments to support continuous improvement.

# Incident Response Plan (IRP)

## Purpose

The purpose of this Incident Response Plan (IRP) is to establish a structured approach for detecting, responding to, containing, and recovering from security incidents at Botium Toys. This plan aims to minimize the impact of incidents on business operations, protect sensitive data, and ensure compliance with regulatory and legal requirements.

---

## Scope

This Incident Response Plan applies to:

- Security incidents affecting IT systems, networks, and applications
- Incidents involving customer or employee data (PII/SPII)
- Payment card data security incidents
- Incidents impacting availability, integrity, or confidentiality of systems
- Physical security incidents that affect IT assets

---

## Incident Response Objectives

- Detect security incidents quickly and accurately
- Contain and limit the impact of incidents
- Eradicate the root cause of incidents
- Recover systems and resume normal operations
- Meet regulatory notification requirements (e.g., GDPR 72-hour rule)
- Document incidents and improve future security posture

---

## Roles and Responsibilities

- **IT Manager**
    - Oversees incident response activities
    - Makes escalation and communication decisions
    - Coordinates with legal and management
- **IT Department / Incident Response Team**
    - Detects, analyzes, and responds to incidents
    - Executes containment, eradication, and recovery steps
    - Preserves evidence when required
- **Management**
    - Provides decision-making support
    - Communicates with external stakeholders when necessary
- **Employees**
    - Report suspected security incidents immediately
    - Follow guidance during incident response activities

---

# Incident Response Phases

## 1. Preparation

- Establish incident response procedures and communication channels
- Ensure logging, monitoring, antivirus, firewall rules, and IDS are operational
- Train employees on how to recognize and report security incidents
- Maintain up-to-date asset inventories and contact lists

---

## 2. Detection and Analysis

- Monitor systems, logs, antivirus alerts, firewall events, and IDS alerts
- Identify indicators of compromise or suspicious activity
- Classify the incident based on severity and impact
- Determine whether sensitive data (PII, payment data) is affected

---

## 3. Containment

- Isolate affected systems to prevent further damage
- Disable compromised accounts or credentials
- Apply temporary fixes to stop ongoing attacks
- Preserve logs and evidence for investigation

---

## 4. Eradication

- Remove malware, malicious accounts, or unauthorized access
- Patch vulnerabilities exploited during the incident
- Reset credentials and strengthen affected controls
- Validate that threats have been fully eliminated

---

## 5. Recovery

- Restore systems and data from secure backups
- Verify system functionality and data integrity
- Monitor systems closely for signs of recurrence
- Gradually return systems to production

---

## 6. Post-Incident Review

- Document the incident, response actions, and outcomes
- Identify lessons learned and areas for improvement
- Update security controls, policies, and procedures as needed
- Report findings to management and relevant stakeholders

---

## Communication and Notification

- Notify internal stakeholders (IT, management) promptly
- If personal data is compromised, notify affected customers and authorities as required
- Comply with GDPR breach notification requirements (within 72 hours)
- Coordinate external communications through management and legal channels

---

## Testing and Maintenance

- Test the Incident Response Plan periodically (e.g., tabletop exercises)
- Update the plan after incidents or significant system changes
- Ensure alignment with the Disaster Recovery Plan and business continuity efforts

---

## Compliance and Framework Alignment

This Incident Response Plan supports:

- **NIST Cybersecurity Framework** – Respond and Recover functions
- **PCI DSS** incident response requirements
- **GDPR** breach notification and data protection obligations
- **SOC 2** security and availability principles