Audit Scope and Goals

Summary: The internal audit needs 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 needs to 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 and compliance checklist

Controls assessment checklist

Yes	No	Control
	●	Least Privilege
	●	Disaster recovery plans
	●	Password policies *Yes, but not in line with current minimum password complexity requirements.*
	●	Separation of duties
●		Firewall
	●	Intrusion detection system (IDS)
	●	Backups
●		Antivirus software
	●	Manual monitoring, maintenance, and intervention for legacy systems *Yes, but no regular schedule in place and intervention method unclear.*
	●	Encryption
	●	Password management system
●		Locks (offices, storefront, warehouse)
●		Closed-circuit television (CCTV) surveillance
●		Fire detection/prevention (fire alarm, sprinkler system, etc.)

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. *Yes, but too available, needs to be limited to only the personnel who need access to do their jobs.*

Recommendations

Based on the identified gaps and risks in Botium Toys' current security program, the following recommendations are critical to reducing risk exposure, achieving compliance, and enhancing overall security posture:

1. Asset Identification and Management

- **Establish a formal asset inventory system** to identify, classify, and track all IT and physical assets, including end-user devices, systems, and data repositories.
- Regularly **review and update asset inventories** to ensure accuracy and assist in risk management and incident response planning.

2. Access Controls and Data Protection

- **Implement the principle of least privilege** to restrict access to sensitive data (e.g., credit card information, PII/SPII) based on job responsibilities.
- **Adopt separation of duties** to prevent conflicts of interest and reduce opportunities for fraud or error.
- **Deploy data encryption mechanisms** for data at rest and in transit, especially for customer credit card and personal data, to ensure confidentiality and meet **PCI DSS** and **GDPR** compliance

3. Password and Identity Management

- **Revise the existing password policy** to comply with current security standards, requiring:
    - Minimum 8 characters
    - Combination of uppercase, lowercase, numbers, and special characters
- **Implement a centralized password management system** that enforces password policies, supports multi-factor authentication (MFA), and reduces password reset requests and productivity loss.

4. Backup and Disaster Recovery Planning

- **Develop and implement a disaster recovery plan (DRP)** to ensure business continuity and rapid restoration of services following a disruptive event.
- **Establish regular backups** of all critical data, with secure off-site or cloud storage to protect against data loss or ransomware attacks.
- Periodically **test and update the disaster recovery plan** to address emerging threats and organizational changes.

5. Intrusion Detection and Monitoring

- **Implement an Intrusion Detection System (IDS)** to monitor network traffic for suspicious activities and provide timely alerts for potential security incidents.
- **Schedule regular monitoring and maintenance of legacy systems** to ensure they are secure and properly functioning. Develop a clear **intervention plan** for when issues are detected.

6. Compliance and Regulatory Adherence

- For **PCI DSS compliance**:
    - Limit access to cardholder data to only authorized personnel.
    - Encrypt credit card data throughout its lifecycle (storage, transmission, processing).
    - Conduct regular PCI DSS compliance assessments and audits.
- For **GDPR compliance**:
    - Ensure all E.U. customer data is classified, securely stored, and properly inventoried.
    - Enforce privacy policies and have a **tested breach notification plan** to alert customers within 72 hours.
- For **SOC 1 and SOC 2 compliance**:
    - Implement strong access control and data integrity measures.
    - Ensure that data is consistently available, accurate, and protected from unauthorized access.

7. Physical Security Enhancements

- Although current locks, CCTV, and fire detection/prevention systems are in place, **review and test these controls regularly** to ensure ongoing effectiveness.
- Integrate physical security monitoring with IT security incident response for a holistic approach to risk management.

8. Training and Awareness

- **Provide ongoing security awareness training** to all employees about their roles in protecting company assets and customer data.
- Include training on **data handling, password management, phishing recognition, and incident reporting** to minimize human error risks.

Conclusion

Addressing these recommendations will significantly reduce Botium Toys' risk profile, ensure compliance with relevant standards such as **PCI DSS**, **GDPR**, and **SOC**, and enhance customer trust. The IT manager should prioritize the implementation of high-risk controls, such as **encryption, access control, IDS deployment, and disaster recovery**, while developing a phased plan for broader compliance and security improvements.