Controls and compliance checklist

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.)

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.

Based on the assessment, here are the key recommendations for the IT manager at Botium Toys to prioritize implementing controls and compliance best practices to mitigate risks:

1. **Implement Least Privilege:** Restrict access to sensitive data such as cardholder information and PII/SPII to only authorized personnel. This reduces the risk of unauthorized access and potential data breaches.

2**. Establish Disaster Recovery Plans:** Develop comprehensive disaster recovery plans to ensure business continuity in the event of data loss or system failures. This includes regular backups of critical data and procedures for restoring operations quickly.

3. **Enhance Password Policies:** Strengthen password policies to enforce minimum complexity requirements, such as longer passwords with a combination of letters, numbers, and special characters. Implement a centralized password management system to enforce these policies consistently and efficiently.

4. **Implement Separation of Duties:** Define clear roles and responsibilities within the organization to prevent conflicts of interest and reduce the risk of fraud or errors. Ensure that sensitive tasks are divided among different individuals to provide checks and balances.

5. **Deploy Encryption:** Implement encryption protocols to secure sensitive data, especially credit card information, throughout its lifecycle, including storage, transmission, and processing. This helps prevent unauthorized access and data theft.

6. **Adopt Intrusion Detection System (IDS):** Install an IDS to monitor network traffic for suspicious activity and potential security breaches. This provides early detection and alerts IT staff to take proactive measures to mitigate risks.

7. **Establish Regular Backup Procedures:** Implement automated backup procedures for critical data to ensure data integrity and availability in case of system failures, disasters, or cyberattacks.

8. **Enhance Legacy Systems Maintenance:** Develop a regular schedule for monitoring and maintaining legacy systems to ensure they are up-to-date and secure. Clearly define intervention methods to address vulnerabilities and mitigate risks associated with outdated systems.

9. **Address GDPR Compliance:** Ensure compliance with GDPR requirements by implementing measures to protect the privacy and security of EU customers' data, including data classification, notification procedures in case of breaches, and enforcement of privacy policies and processes.

10. **Enhance Physical Security Measures:** Strengthen physical security measures, including access controls, surveillance systems (CCTV), and fire detection/prevention systems, to protect the company's premises and assets from unauthorized access, theft, and disasters.

Recommendations (optional): To enhance security and mitigate risks at Botium Toys, the IT manager should communicate key recommendations to stakeholders. These include implementing employee training on security best practices and multi-factor authentication for accessing sensitive systems. Regular security audits and incident response plans are crucial for identifying vulnerabilities and effectively responding to

security incidents. Strengthening vendor management practices and implementing patch management processes are essential for ensuring third-party compliance and timely installation of security updates. Network segmentation, robust logging, and monitoring systems help isolate sensitive data and detect suspicious activities. Providing security awareness training for customers and regularly updating security policies ensure alignment with emerging threats and regulatory requirements. Collaboration among stakeholders is vital for successful implementation.