Controls and compliance checklist

Controls assessment checklist

Yes	No	Control	Remarks
	√	Least Privilege	No implementation of access controls for least privilege (all employees have access to stored data).
	√	Disaster recovery plans	No disaster recovery plans or critical data backups are in place.
	√	Password policies	Policy exists but does not meet minimum complexity standards.
	√	Separation of duties	Access controls for separation of duties are not implemented.
√		Firewall	Firewall in place with defined security rules.
	√	Intrusion detection system (IDS)	No IDS currently installed.
	√	Backups	No backups for critical data.
√		Antivirus software	Installed and monitored regularly.
	√	Manual monitoring, maintenance, and intervention for legacy systems	Legacy systems are monitored but without a regular schedule or clear intervention procedures.
	√	Encryption	Encryption is not used for stored cardholder data.
	√	Password management system	No centralized password management system; productivity issues reported.
√		Locks (offices, storefront, warehouse)	Physical location secured with sufficient locks.
√		Closed-circuit television (CCTV) surveillance	CCTV surveillance is operational and up-to-date.
√		Fire detection/prevention (fire alarm, sprinkler system, etc.)	Functioning fire detection and prevention systems in place.

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Remarks
	√	Only authorized users have access to customers' credit card information.	All employees have access to cardholder data.
	√	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Not stored securely; lacks encryption.
	√	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Encryption is currently not implemented.
	√	Adopt secure password management policies.	Current password policy is weak and not enforced through a centralized system.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Remarks
	√	E.U. customers' data is kept private/secured.	No evidence encryption or least privilege policies are implemented.
√		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	Plan exists for breach notification.
	√	Ensure data is properly classified and inventoried.	Asset classification and inventorying is not in place.
√		Enforce privacy policies, procedures, and processes to properly document and maintain data.	Policies exist and are enforced among employees.

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

Yes	No	Best practice	Remarks
	√	User access policies are established.	No access policy for limiting data access to specific roles.
	√	Sensitive data (PII/SPII) is confidential/private.	Lack of encryption and access controls jeopardizes confidentiality.
√		Data integrity ensures the data is consistent, complete, accurate, and has been validated.	Controls for data integrity have been integrated by IT.
	√	Data is available to individuals authorized to access it.	No access control restrictions lead to unregulated access.

Recommendations and guidelines:

Least Privilege:
Botium Toys should implement Role-Based Access Control (RBAC) and regularly review user access rights to ensure the principle of least privilege.

> **NIST 800-53 controls:**
> AC-6: Least Privilege
> AC-2(7): Privileged User Accounts

Disaster Recovery Plans:
A formal contingency plan should be developed, tested regularly, and include recovery objectives for system continuity.

> **NIST 800-53 controls:**
> CP-2: Contingency Plan
> CP-4: Contingency Plan Testing
> CP-10: System Recovery and Reconstitution

Password Policies:
Botium Toys should revise its password policy to align with modern security practices, including minimum complexity, length, and expiration requirements.

> **NIST 800-53 controls:**
> IA-5: Authenticator Management
> IA-5(1): Password-based Authentication

Separation of Duties:
Separation of critical tasks should be enforced to reduce fraud and operational risk by ensuring that no one individual has full control over key processes.

> **NIST 800-53 controls:**
> AC-5: Separation of Duties

Firewall:
Maintain and regularly update firewall rules to prevent unauthorized access and support boundary protection.

> **NIST 800-53 controls:**
> SC-7: Boundary Protection
> SC-7(5): Deny by Default — Allow by Exception

Intrusion Detection System (IDS):
Botium Toys should implement an IDS to detect and respond to suspicious network activity and security breaches.

> **NIST 800-53 controls:**
> SI-4: System Monitoring
> SI-4(1): System-wide Intrusion Detection
> SI-4(4): Inbound and Outbound Communications Traffic

Backups:
A data backup solution must be implemented and include regular testing to verify recoverability of critical data.

NIST 800-53 controls:
CP-9: System Backup
CP-9(1): Testing for Reliability and Integrity
CP-9(4): Protection from Unauthorized Modification

Antivirus Software:
Continue using centrally managed antivirus software that is regularly updated and monitored to prevent malicious code.

NIST 800-53 controls:
SI-3: Malicious Code Protection
SI-3(1): Central Management
SI-3(2): Automatic Updates

Legacy Systems:
Define a formal maintenance schedule and clear intervention methods for legacy systems to minimize risk exposure.

NIST 800-53 controls:
MA-6: Timely Maintenance
CM-2: Baseline Configuration
CM-2(6): Development and Test Environments

Encryption:
Encryption must be applied to sensitive data, especially customer credit card information, both in transit and at rest.

NIST 800-53 controls:
SC-12: Cryptographic Key Establishment and Management
SC-28: Protection of Information at Rest
SC-12(2): Symmetric Keys
SC-28(1): Cryptographic Protection

Password Management System:
Implement a centralized password management system to enforce policies and assist users in secure password resets.

NIST 800-53 controls:
IA-5(6): Protection of Authenticators
IA-5(18): Password Managers

Locks (Offices, Storefront, Warehouse):
Maintain current physical security with locks to prevent unauthorized access to facilities.

NIST 800-53 controls:
PE-3: Physical Access Control

Closed-Circuit Television (CCTV) Surveillance:
Maintain CCTV systems to monitor physical access and deter potential security violations.

NIST 800-53 controls:
PE-6: Monitoring Physical Access
PE-6(3): Video Surveillance

Fire Detection and Prevention Systems:
Continue using fire alarms and suppression systems and conduct regular inspections to ensure functionality.

NIST 800-53 controls:
PE-13: Fire Protection
PE-13(1): Detection Systems — Automatic Activation and Notification
PE-13(2): Suppression Systems — Automatic Activation and Notification