Security Controls and Compliance Audit Form

Uzair Khan, Cybersecurity Analyst – Google Cybersecurity Professional Certificate

Used the following documentation to complete the security audit form:
scope, goals, and risk assessment report
control categories
controls, frameworks, and compliance

Does Botium Toys currently have this control in place?

Controls Assessment Checklist

Yes	No	Control
	N	Least Privilege
	N	Disaster recovery plans
	N	Password policies
	N	Separation of duties
Y		Firewall
	N	Intrusion detection system (IDS)
	N	Backups
Y		Antivirus software
Y		Manual monitoring, maintenance, and intervention for legacy systems. Note: There is no regular schedule for legacy system maintenance and monitoring. This needs to be defined.
	N	Encryption
	N	Password management system
Y		Locks (offices, storefront, warehouse)
Y		Closed-circuit television (CCTV) surveillance
Y		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Does Botium Toys currently adhere to this compliance best practice?

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
	N	Only authorized users have access to customers' credit card information. Note: Urgent need.
	N	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. Note: While data is on-prem, there is no encryption.
	N	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
	N	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	N	E.U. customers' data is kept private/secured.
Y		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
	N	Ensure data is properly classified and inventoried.
Y		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
	N	User access policies are established.
	N	Sensitive data (PII/SPII) is confidential/private.
Y		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
	N	Data is available to individuals authorized to access it.

High Priority Recommendations

Written by **Uzair Khan**, Cybersecurity Analyst – Google Cybersecurity Professional Certificate

After carefully reviewing the security posture and security controls of Botium Toy's, I have listed the most urgent security recommendations in phases for easier implementation.

1. Ensure PCI DSS Compliance – Failure to comply with PCI DSS exposes businesses to severe financial, legal, and reputational risks. It is of utmost importance to use encryption for locally stored, processed, and transmitted credit card information. Ensure identity and access management (IAM) principles like role-based access control (RBAC), so that each role only has access to information that it needs for daily tasks. No employee should be able to access customer financial data. Refer to PCI Security Standards Council for more information here.

2. Basic Security Hygiene – Enforce secure password management, authentication, and authorization. Implement strong password policies with length, complexity, and time-based requirements, multi-factor authentication (MFA), account lockout configurations, and deploy an enterprise-grade password manager. Create backups of critical data.

3. Defense in Depth – Develop a secure-by-design and comprehensive security posture. Implement an IDS/IPS and/or SIEM tool for intrusion detection/prevention & log monitoring and analysis. Develop a comprehensive disaster recovery plan that incorporates the preexisting E.U. plan. Implement a periodic backup policy and schedule legacy system maintenance windows. Adopt zero-trust and principal of least-privilege architecture ensuring embedded security moving forward.