

Controls and compliance checklist

**Botium Toys: Scope, goals, and risk assessment report
for the Google Cybersecurity Course.**

Controls assessment checklist

Yes	No	Control
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Least Privilege
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disaster recovery plans
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Password policies
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separation of duties
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Intrusion detection system (IDS)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Backups
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Antivirus software
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Manual monitoring, maintenance, and intervention for legacy systems
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Encryption
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password management system
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Locks (offices, storefront, warehouse)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Closed-circuit television (CCTV) surveillance
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Only authorized users have access to customers' credit card information.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
<input checked="" type="checkbox"/>	<input type="checkbox"/>	E.U. customers' data is kept private/secured.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Ensure data is properly classified and inventoried.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	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
<input checked="" type="checkbox"/>	<input type="checkbox"/>	User access policies are established.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sensitive data (PII/SPII) is confidential/private.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Data integrity ensures the data is consistent, complete, accurate,

and has been validated.

- ☒ ☐ Data is available to individuals authorized to access it.
-

Recommendations

Based on the completed checklists, here are some recommendations for the IT manager to communicate to stakeholders:

Implement least privilege access control. This ensures only authorized users have access to the data they need for their jobs.

Develop and implement a disaster recovery plan. This plan should outline the steps to take in case of a system outage or data breach.

Improve password complexity requirements. Passwords should be at least 12 characters long and include a combination of upper and lowercase letters, numbers, and symbols.

Implement a centralized password management system. This will help enforce password policies and reduce the burden on IT staff for password resets.

Encrypt all customer data, including credit card information. This will protect sensitive data at rest and in transit.

Develop a regular schedule for monitoring, maintaining, and patching legacy systems. This will help to identify and address vulnerabilities before they can be exploited.

Implement data security measures for PII/SPII in accordance with GDPR. This may include data encryption and access controls.

Consider pursuing SOC 2 compliance. This will demonstrate Botium Toys' commitment to data security and controls.

By implementing these recommendations, Botium Toys can significantly improve its security posture and reduce the risk of a data breach or other security incident.