Controls and compliance checklist

By: Josué Eduardo Rodríguez Carrillo

This activity was carried out as part of the Google Cybersecurity Professional Certificate certification, and is called Portfolio Activity: Conduct a security audit. The information was obtained from the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

Controls assessment checklist

Yes	No	Control	Justification
□	☑	Least Privilege	At the moment, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
□	☑	Disaster recovery plans	There are no disaster recovery plans currently in place.
□	☑	Password policies	A password policy exists, but its requirements are nominal and not in line with current minimum password complexity requirements.
□	☑	Separation of duties	Separation of duties has not been implemented.
☑	□	Firewall	IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
□	☑	Intrusion detection system (IDS)	IT department has not installed an intrusion detection system (IDS).
□	☑	Backups	There are no disaster recovery plans currently in place, and the company

			does not have backups of critical data.
☑	□	Antivirus software	Antivirus software is installed and monitored regularly by the IT department.
□	☑	Manual monitoring, maintenance, and intervention for legacy systems	While legacy systems are monitored and maintained, there is no regular schedule in place and intervention methods are unclear.
□	☑	Encryption	Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
□	☑	Password management system	There is no centralized password management system that enforces the password policy's minimum requirements.
☑	□	Locks (offices, storefront, warehouse)	The store's physical locations have sufficient locks.
☑	□	Closed-circuit television (CCTV) surveillance	The store's physical locations have up-to-date closed-circuit television (CCTV) surveillance.
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)	They have functioning fire detection and prevention systems.

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Justification
□	☑	Only authorized users have access to customers' credit card information.	At the moment, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Encryption is not currently used to ensure confidentiality of customers' PII/SPII.
□	☑	Adopt secure password management policies.	Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Justification
□	☑	E.U. customers' data is kept private/secured.	Encryption is not currently used to ensure confidentiality of customers' PII/SPII.
☑	□	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach.

☐	☑	Ensure data is properly classified and inventoried.	There is inadequate management of assets.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Privacy policies, procedures, and processes have been developed and are enforced among IT department

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

Yes	No	Best practice	Justification
☐	☑	User access policies are established.	Access controls pertaining to least privilege and separation of duties have not been implemented.
☐	☑	Sensitive data (PII/SPII) is confidential/private.	At the moment, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	The IT department has ensured availability and integrated controls to ensure data integrity.
☐	☑	Data is available to individuals authorized to access it.	At the moment, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.

The internal security audit has identified a significant risk to Botium Toys, with an overall risk score of 8/10. This elevated score is directly attributable to critical gaps in the organization's security controls and a lack of adherence to key compliance best practices.

To effectively mitigate these risks, improve asset management, and achieve full compliance with U.S. and international regulations (specifically PCI DSS and GDPR), the following actions are recommended:

Recommendations

High-Priority Recommendations (Critical Risk Mitigation)

1. Implement Robust Access Controls: Immediately enforce the principles of Least Privilege and Separation of Duties. This is paramount to restrict unauthorized access to sensitive data, including cardholder data and customers' PII and SPII.
2. Deploy Enterprise-Wide Encryption: Introduce strong encryption protocols for all sensitive data, both at rest and in transit. You need to protect customer payment information and ensuring data confidentiality, directly addressing a critical failure in the current security posture.
3. Establish a Disaster Recovery & Backup Strategy: Develop, document, and implement a comprehensive Disaster Recovery Plan. Furthermore, initiate regular, automated backups of all critical data to ensure business continuity and data availability in the event of a system failure, cyber-attack, or other disruptive incidents.

Medium-Priority Recommendations (Strengthening Security Posture)

4. Enhance Password Security Policy: Revise and enforce a modern password policy that mandates complexity requirements (e.g., minimum length, character variety). Complement this by implementing a centralized password management system to enforce policy adherence, reduce help-desk overhead, and bolster account security.
5. Augment Network Defense: Complement the existing firewall by deploying an Intrusion Detection System (IDS) to provide continuous network monitoring, detect potential malicious activity, and enable a more proactive security stance.

6. Formalize Maintenance Procedures for Legacy Systems: Develop a scheduled maintenance program with clear intervention protocols for legacy systems.
7. Execute Asset Identification & Classification: Initiate the "Identify" function of the NIST CSF by conducting a complete asset inventory and data classification exercise.

Conclusion

The timely implementation of these recommendations is critical to protect the organization from severe financial penalties from regulatory bodies and to prevent significant reputational and operational damage that could result from a security incident. Addressing these gaps will solidify Botium Toys' security foundation and support its continued growth in a secure and compliant manner.