Google certificate project

Cybersecurity Audit report of Botium Toys (Academic Simulation)

Realized by:

Nada Maach

August 11, 2025

Contents

1 Scope & Limitations

This audit was conducted solely for academic purposes as part of a cybersecurity coursework project. It is not an official professional audit and does not fully align with any specific cybersecurity framework (e.g., ISO 27001, NIST CSF). The scope, methodology, and findings are limited to the resources and simulated scenarios provided in the academic setting, and may not reflect the complete security posture of the organization in a real-world context.

2 Executive Summary

This report has been prepared for Botium Toys as part of the portfolio project for the Google Coursera Professional Certificate. The audit aims to assist the executive team in developing a robust cybersecurity strategy by identifying gaps, assessing current controls, and providing actionable recommendations.

Recommendations are categorized as:

- **Non-Technical (NT)** – Policies, governance, and awareness.
- **Technical (T)** – Tools, systems, and configurations.
- **Physical (P)** – Facility and hardware security.

Implementation of these recommendations will strengthen the company's security posture, reduce risk, and ensure compliance with applicable regulations such as PCI DSS, GDPR, and SOC requirements.

3 Summary of Recommendations

3.1 Governance and Risk Management (NT)

- Assign clear accountability for cybersecurity to designated personnel or teams.
- Implement Role-Based Access Control (RBAC) with Zero Trust and Least Privilege principles to ensure only authorized users can access sensitive information, including customers' credit card data (PCI DSS, SOC).
- Apply Separation of Duties (SoD) to prevent fraud and operational errors.
- Maintain an up-to-date asset register covering hardware, software, data, processes, people, and third parties.
- Adopt an information classification and labeling policy based on sensitivity levels, including classification of personal data and payment card information to support GDPR and PCI DSS compliance.

- Conduct formal risk assessments at least annually, following ISO/IEC 27001 methodology.
- Establish a continuous improvement process with regular reviews of policies, risks, and controls.

3.2 Policies, Procedures, and Awareness (NT)

- Document all security policies, processes, and work instructions, including policies specific to data privacy and payment security.
- Develop and enforce a legacy system management policy, ensuring regular monitoring, maintenance, and timely upgrades.
- Implement a formal Change Management Policy for controlled updates to systems and software.
- Provide cybersecurity awareness training during onboarding and refreshers annually.
- Include password security education, phishing simulations, and incident reporting procedures in training programs.
- Educate staff on compliance requirements regarding handling of EU customer data (GDPR) and payment card information (PCI DSS).

3.3 Incident, Recovery, and Continuity Planning (T/NT)

- Maintain and regularly test an Incident Response Plan (IRP) defining roles, escalation paths, and communication channels.
- Document Disaster Recovery (DR) and Business Continuity (BC) Plans, including:
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
  - Maximum Tolerable Downtime (MTD)
- Define and track additional metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to enhance incident management effectiveness.

3.4 Key Technical Controls (T)

- Implement and enforce a password policy supported by a password management system.
- Deploy Multi-Factor Authentication (MFA) for critical systems and sensitive accounts.
- Establish secure baseline configurations and maintain patch management for all systems.
- Encrypt all sensitive data at rest and in transit using industry standards (e.g., AES-256, TLS 1.3) to protect cardholder data and personal information (PCI DSS, GDPR).
- Conduct regular vulnerability scans and penetration tests using tools such as Nessus or SolarWinds.
- Deploy and maintain Intrusion Detection/Prevention Systems (IDS/IPS) integrated with incident response processes.
- Implement centralized Security Information and Event Management (SIEM) for log aggregation and advanced threat detection, supporting SOC compliance for monitoring and audit trails.

3.5 Access and Identity Management (T)

- Maintain a documented Access Control Policy, ensuring user access aligns with business needs and compliance requirements (SOC).
- Perform periodic access reviews and promptly revoke unused or inactive accounts.

3.6 Data Management and Storage (NT/T/P)

- Implement a Data Retention Policy aligned with legal and business requirements, clarifying retention duration and secure deletion methods in accordance with GDPR and PCI DSS.
- Apply secure deletion and device disposal procedures to prevent data leakage.
- Classify and protect sensitive data, including Personally Identifiable Information (PII) and Sensitive Personal Information (SPII), according to confidentiality, integrity, and availability requirements.

- Maintain a detailed data inventory to ensure accurate tracking of all personal and payment card data, supporting GDPR data subject rights and PCI DSS requirements.

3.7 Physical Security (P)

- Secure server rooms, offices, and storage areas.
- Enforce a clear desk and clear screen policy.
- Control visitor access and maintain physical access logs.

3.8 Legal, Regulatory, and Third-Party Compliance (NT)

- Prepare for compliance with EU GDPR and other relevant regulations.
- Assign a Data Protection Officer (DPO) or equivalent compliance role if applicable.
- Conduct third-party supplier risk assessments and enforce contractual security requirements, ensuring that third parties handling sensitive or payment data comply with PCI DSS, GDPR, and SOC standards.

4 Conclusion

By implementing these recommendations, Botium Toys can significantly improve its cybersecurity posture, enhance operational resilience, and maintain compliance with applicable laws and standards including PCI DSS, GDPR, and SOC requirements. The organization should prioritize actions based on risk severity, resource availability, and regulatory deadlines, with progress reviewed at regular governance meetings.