BOTIUM TOYS INTERNAL SECURITY AUDIT

Controls and Compliance Checklist

Compliance & Security Risk Summary

Regulation	Compliance Status	Key Risks Identified
GDPR	Partial Compliance	No encryption, lack of classification
PCI DSS	Non-Compliant	Credit card data exposure, weak password policies
SOC 2	Partial Compliance	No Least Privilege Access, missing IDS

Remediation Roadmap

Security Priorities & Action Plan

Security Issue	Action Plan	Priority Level	Deadline	Responsible Team
No MFA for Employees	Enforce MFA for all accounts	High	39 Days	IT Security
Unencrypted Customer Data	Implement AES-256 Encryption	High	60 Days	Database Team
No Data Classification	Deploy a Data Classification Policy	Medium	90 Days	Compliance Team
No Incident Response Plan Testing	Conduct breach simulation drills	High	30 Days	Security Team

Weak Password Policies	Implement strong password requirements and password manager	High	45 Days	IT Security
Lack of IDS for Network Monitoring	Install an IDS	High	60 Days	IT Infrastructure Team
PCI DSS Non-Compliance	Encrypt credit card data, segment payment systems, enforce least privilege access	High	90 Days	Security & Compliance Team

Detailed Recommendations for GDPR Compliance

1. Encrypt Customers’ Financial Data (High Priority - Immediate Action Required)

Issue: Customer financial data is not encrypted, violating GDPR confidentiality requirements.
Recommendation:

- Implement AES-256 encryption for customer data at rest within 30 days.
- Ensure TLS 1.3 encryption for data in transit by end of Q1.
- Use tokenization techniques for sensitive payment data to prevent unauthorized access.

2. Enhance Data Breach Response Plan (High Priority - Immediate Action Required)

Issue: A data breach notification plan exists but needs formal documentation and testing.
Recommendation:

- Conduct breach response drills to test notification processes quarterly.
- Automate incident detection with SIEM tools for quick response.
- Assign a Data Protection Officer (DPO) to oversee breach responses and ensure compliance.

3. Classify and Inventory Data Properly (Medium Priority - 90 Days)

Issue: Data assets are inventoried but not classified, making it difficult to apply security controls.
Recommendation:

- Implement a Data Classification Policy to categorize data based on sensitivity (Public, Internal, Confidential, Highly Confidential).
- Use automated tools like Data Loss Prevention (DLP) to tag and track sensitive data.

4. Strengthen Privacy Policy Enforcement (Medium Priority - 90 Days)

Issue: Privacy policies and procedures exist but should be reinforced across all employees.
Recommendation:

- Provide mandatory GDPR training for all employees handling customer data.
- Regularly audit compliance with privacy policies.
- Implement data minimization practices—only collect and store necessary customer information.

Detailed Recommendations for System and Organization Controls (SOC 1 & SOC 2)

5. Implement Least Privilege Access Controls (High Priority - 30 Days)

Issue: All employees have access to internally stored data, violating Least Privilege and Separation of Duties principles.
Recommendation:

- Apply Role-Based Access Control (RBAC) to ensure employees can only access data relevant to their job role.
- Use Multi-Factor Authentication (MFA) for administrative access.
- Regularly review and revoke unnecessary access rights.

6. Encrypt Personally Identifiable Information (PII & SPII) (High Priority - 60 Days)

Issue: Encryption is not used to protect sensitive Personally Identifiable Information (PII/SPII).
Recommendation:

- Encrypt PII/SPII data at rest and in transit (AES-256, TLS 1.3).
- Implement data masking techniques to protect displayed sensitive data.
- Enforce zero-trust architecture to limit exposure of PII/SPII.

7. Restrict Data Access to Only Authorized Employees (High Priority - 45 Days)

Issue: While data is available to all employees, access should be limited to only those who need it.
Recommendation:

- Implement a Data Access Policy that enforces strict permissions based on job function.
- Use Identity & Access Management (IAM) tools to monitor and control access.
- Conduct regular access reviews to ensure compliance with SOC standards.

Enhanced PCI DSS Compliance Recommendations

8. Implement Stronger PCI DSS Controls (High Priority - 90 Days)

Issue: Payment card data is not encrypted, and all employees currently have access to sensitive information.
Recommendation:

- Encrypt all credit card data using AES-256 encryption.
- Implement tokenization to replace stored card data with secure placeholders.
- Segment payment processing systems to isolate them from other company networks.
- Restrict credit card data access to only authorized employees through least privilege policies.
- Conduct quarterly vulnerability scans and penetration testing to ensure ongoing compliance.

Final Compliance Summary & Next Steps

Regulation	Current Compliance Status	Recommended Actions	Deadline
GDPR	Partial Compliance	Implement encryption, breach response testing, data classification	90 Days

PCI DSS	Non-Compliant	Encrypt card data, enforce least privilege access, conduct vulnerability scans	90 Days
SOC 2	Partial Compliance	Implement MFA, least privilege, and logging improvements	69 Days

Next Steps:

- Encrypt all sensitive data to align with GDPR and SOC 2 requirements.
- Enforce role-based access controls (RBAC) to limit internal data access.
- Test and refine the incident response plan for quick breach notifications.
- Implement MFA and password policies for stronger access control.
- Conduct regular security audits and penetration tests to ensure ongoing compliance.

Conclusion

This enhanced security audit provides a clear roadmap for strengthening security controls and compliance. Implementing the recommended controls will reduce risk, improve compliance posture, and enhance data protection for Botium Toys.