BOTIUM TOYS INTERNAL IT AUDIT REPORT

1. Introduction

Purpose of the Audit: The purpose of this audit is to secure Botium Toys' IT infrastructure, identify and mitigate potential risks, threats, or vulnerabilities to critical assets, and ensure compliance with relevant regulations.

Scope of the Audit: This audit will cover Botium Toys' single physical location, including the main office, storefront, and warehouse, as well as their online presence and related IT infrastructure.

2. Identify the Scope of the Audit

Assets Managed by IT:

- **Servers:** Web servers, application servers, database servers.
- **Network devices:** Routers, switches, firewalls.
- **Databases:** Customer information databases, inventory databases.
- **Applications:** E-commerce platform, internal management tools.
- **Workstations and laptops:** Employee workstations and laptops.
- **Mobile devices:** Company-issued smartphones and tablets.
- **Physical security systems:** CCTV cameras, access control systems.
- **Payment processing systems:** Systems for processing online and in-store payments.

Goals Alignment:

- Ensure the security and compliance of Botium Toys' IT infrastructure.
- Support the growth of the online market while maintaining security standards.
- Protect customer data and comply with payment processing regulations.

Audit Frequency:

- Conduct the internal audit annually or whenever significant changes are made to the IT infrastructure.

Policy and Procedure Evaluation:

- Review existing organizational policies and procedures to ensure they are effective and properly implemented.

3. Complete a Risk Assessment

Identified Risks:

- Unauthorized access to sensitive data (e.g., customer PII, payment information).
- Inadequate network security measures (e.g., firewalls, intrusion detection systems).
- Non-compliance with regulations (e.g., PCI DSS, GDPR).
- Potential data breaches due to insufficient cybersecurity practices.
- Physical security vulnerabilities at the main office and warehouse.

Additional Comments:

- The IT department is under increasing pressure to support a growing online market.
- There is a need to comply with regulations related to online payments and business operations in the E.U.
- The company lacks a clear plan for maintaining compliance and business operations as it grows.

4. Conduct the Audit

Controls Categories:

- Review the Controls Categories document to evaluate the effectiveness of security controls in place.

Controls and Compliance Checklist:

Complete the checklist based on the gathered information.

Control Category	Question	Yes/No	Observations/Findings
Access Control	Are user accounts managed properly?	Yes	User accounts are managed, but need periodic reviews.
	Are multi-factor authentication (MFA) measures in place?	No	MFA is not implemented for all critical systems.
Data Protection	Is sensitive data encrypted at rest and in transit?	Yes	Data encryption is in place, but needs regular audits.
Network Security	Are firewalls and intrusion detection systems deployed?	Yes	Firewalls and IDS are deployed, but configuration reviews are needed.

	Are there regular network security assessments?	No	Network security assessments are not conducted regularly.
Physical Security	Are physical access controls in place at the main office and warehouse?	Yes	Physical access controls are implemented, but logs are not reviewed regularly.
Compliance	Is the company compliant with PCI DSS requirements?	No	PCI DSS compliance needs to be achieved.
	Is the company compliant with GDPR requirements?	No	GDPR compliance needs to be achieved.
Incident Response	Is there an incident response plan in place?	Yes	Incident response plan exists but needs testing and updating.

5. Create a Mitigation Plan

Mitigation Plan

1. Access Control

Issue: Periodic reviews of user accounts are not conducted.

- **Action**: Implement a regular review process for user accounts to ensure compliance with the principle of least privilege.
- **Timeline**: Within 1 month
- **Responsible Party**: IT Security Manager

Issue: Multi-Factor Authentication (MFA) is not implemented for all critical systems.

- **Action**: Deploy MFA for all critical systems, including email, internal applications, and remote access tools.
- **Timeline**: Within 3 months
- **Responsible Party**: IT Department

2. Data Protection

Issue: Regular audits of data encryption measures are not conducted.

- **Action**: Schedule and perform quarterly audits of data encryption at rest and in transit.
- **Timeline**: Within 1 month for initial audit, then quarterly
- **Responsible Party**: Data Protection Officer (DPO)

3. Network Security

Issue: Firewall and Intrusion Detection System (IDS) configurations need regular reviews.

- **Action**: Establish a schedule for regular review and update of firewall and IDS configurations.
- **Timeline**: Within 2 months for initial review, then bi-monthly
- **Responsible Party**: Network Security Team

Issue: Network security assessments are not conducted regularly.

- **Action**: Implement a schedule for regular network security assessments to be conducted quarterly.
- **Timeline**: Within 1 month for initial assessment, then quarterly
- **Responsible Party**: IT Security Analyst

4. Physical Security

Issue: Physical access logs are not reviewed regularly.

- **Action**: Set up a process for bi-monthly review of physical access logs and implement it.
- **Timeline**: Within 1 month
- **Responsible Party**: Physical Security Manager

5. Compliance

Issue: PCI DSS compliance is not achieved.

- **Action**: Initiate a project to address PCI DSS compliance gaps, including secure storage of payment card data and vulnerability management.
- **Timeline**: Within 6 months
- **Responsible Party**: Compliance Officer

Issue: GDPR compliance is not achieved.

- **Action**: Hire a GDPR consultant to identify compliance gaps and implement necessary measures, including data subject rights and breach notification procedures.
- **Timeline**: Within 6 months
- **Responsible Party**: Data Protection Officer (DPO)

6. Incident Response

Issue: Incident response plan exists but needs regular testing and updates.

- **Action**: Schedule regular testing of the incident response plan every 6 months and update it based on test results.
- **Timeline**: Within 1 month for initial test, then every 6 months
- **Responsible Party**: Incident Response Team Leader

Summary of Action Items

Issue	**Action**	**Timeline**	**Responsible Party**
Periodic reviews of user accounts not conducted	Implement regular review process	Within 1 month	IT Security Manager
MFA not implemented for all critical systems	Deploy MFA for all critical systems	Within 3 months	IT Department
Regular audits of data encryption measures not conducted	Schedule and perform quarterly audits of data encryption	Within 1 month, then quarterly	Data Protection Officer (DPO)
Firewall and IDS configurations need regular reviews	Establish schedule for regular review and update of firewall and IDS configurations	Within 2 months, then bi-monthly	Network Security Team
Network security assessments not conducted regularly	Implement schedule for regular network security assessments	Within 1 month, then quarterly	IT Security Analyst
Physical access logs not reviewed regularly	Set up process for bi-monthly review of physical access logs	Within 1 month	Physical Security Manager

PCI DSS compliance not achieved	Initiate project to address PCI DSS compliance gaps	Within 6 months	Compliance Officer
GDPR compliance not achieved	Hire GDPR consultant to identify gaps and implement necessary measures	Within 6 months	Data Protection Officer (DPO)
Incident response plan needs regular testing and updates	Schedule regular testing of incident response plan every 6 months and update it based on results	Within 1 month, then every 6 months	Incident Response Team Leader

6. Communicate Results to Stakeholders

Detailed Report:

Compile all findings, observations, and mitigation strategies into a comprehensive report.

Suggested Improvements for Botium Toys

Based on the audit findings and risk assessment, the following improvements are recommended to enhance Botium Toys' IT security and ensure compliance with relevant regulations:

1. Access Control

- Implement Periodic Reviews of User Accounts: Establish a quarterly review process for user accounts to ensure compliance with the principle of least privilege and to deactivate any unnecessary accounts.

- **Deploy Multi-Factor Authentication (MFA):** Implement MFA for all critical systems, including email, internal applications, and remote access tools, to enhance access security and reduce the risk of unauthorized access.

2. Data Protection

- **Conduct Regular Data Encryption Audits:** Schedule and perform quarterly audits of data encryption measures to ensure that sensitive data is encrypted both at rest and in transit. This will help in identifying and addressing any gaps in encryption protocols.
- **Enhance Data Loss Prevention (DLP) Measures:** Implement DLP solutions to monitor and protect sensitive data from unauthorized access and leaks. This includes monitoring data transfers and applying encryption or blocking sensitive data transfers as needed.

3. Network Security

- **Regularly Review Firewall and IDS Configurations:** Establish a bi-monthly review process for firewall and intrusion detection system (IDS) configurations to ensure they are up-to-date and effective against current threats.
- **Implement Regular Network Security Assessments:** Conduct quarterly network security assessments to identify and mitigate vulnerabilities in the network infrastructure. This should include penetration testing and vulnerability scanning.

4. Physical Security

- **Review Physical Access Logs Regularly:** Set up a bi-monthly process for reviewing physical access logs to detect any unauthorized access attempts and ensure physical security controls are effective.

- **Upgrade Physical Security Measures:** Consider upgrading physical security measures, such as installing additional CCTV cameras, improving access control systems, and training employees on physical security best practices.

5. Compliance

- **Achieve PCI DSS Compliance:** Initiate a project to address gaps in PCI DSS compliance, including secure storage of payment card data, implementing robust access controls, and conducting regular vulnerability assessments. Engage with a Qualified Security Assessor (QSA) to guide the compliance process.

- **Achieve GDPR Compliance:** Hire a GDPR consultant to identify compliance gaps and implement necessary measures, such as data subject rights management, data protection impact assessments (DPIAs), and breach notification procedures. Regularly review and update GDPR compliance practices to stay current with regulations.

6. Incident Response

- **Test and Update Incident Response Plan:** Schedule regular testing of the incident response plan every six months. Update the plan based on test results and lessons learned from any incidents. Ensure all employees are aware of their roles and responsibilities during an incident.

- **Improve Incident Detection and Response Capabilities:** Invest in advanced security monitoring tools, such as Security Information and Event Management (SIEM) systems, to enhance the detection and response to security incidents. Train the incident response team on the latest threat detection and mitigation techniques.

7. Employee Training and Awareness

- **Conduct Regular Security Training:** Implement a comprehensive security training program for all employees. This should include training on phishing awareness, password management, data protection practices, and incident reporting procedures.

- **Promote a Security-First Culture:** Encourage a culture of security within the organization by regularly communicating the importance of security practices and recognizing employees who demonstrate good security behaviours.

8. Vendor and Third-Party Management

- **Evaluate Third-Party Security Practices:** Conduct regular assessments of third-party vendors and service providers to ensure they meet Botium Toys' security standards. This includes reviewing their security policies, conducting security audits, and ensuring they comply with relevant regulations.

- **Implement Vendor Risk Management Program:** Establish a vendor risk management program to continuously monitor and manage the security risks associated with third-party vendors.

9. Data Backup and Recovery

- **Enhance Data Backup Procedures:** Ensure that data backup procedures are robust and regularly tested. Implement off-site backups and ensure that backups are encrypted and securely stored.

- **Develop and Test Disaster Recovery Plan:** Create a comprehensive disaster recovery plan and conduct regular tests to ensure that the organization can quickly recover from any data loss or system failure.

Stakeholder Presentation:

Prepare a presentation summarizing the audit findings and recommendations for senior management and relevant stakeholders.

Conclusion

By following the outlined steps and completing the controls and compliance checklist, Botium Toys can significantly improve its security posture, reduce risks, and ensure compliance with relevant regulations. Regular audits and proactive risk management will support the company's growth and safeguard its assets and customer data.