Controls and compliance checklist

On

Botium Toys

Offensive Rhino

December 9, 2024

OFFENSIVE RHINO

ASSESSMENT INFORMATION

Offensive Rhino Details

Account Executive
Offensive Rhino
https://offensiverhino.netlify.app

Pentesting Team
Offensive Rhino
Hamim Mahamud Hamy
CEO | Founder
hmmahmud145@outlook.com
+8801755-069752
https://hamilio.netlify.app

Offensive Rhino
Al Nahian
Sr. Pentester
alnah14n@gmail.com

Offensive Rhino
Ratul Saha
Team Lead
ratulsahaanu@gmail.com

Client Details

Botium Toys

Contact Information
Botium Toys

About Offensive Rhino Company

Offensive Rhino provides best-in-class security solutions, managed security services, and manual penetration testing to enterprises for a complete security approach that detects, protects, and remediates cyber attacks.

Controls assessment checklist is based on the Botium Toys: Scope, goals, and risk assessment report. To check the authenticity of this checklist. You can visit the Botium Toys: Scope, goals, and risk assessment report.

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

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
☐	☑	Only authorized users have access to customers' credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☐	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

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

and has been validated.

☐ ☑ Data is available to individuals authorized to access it.

General Security Controls Recommendations

1. **Implement Least Privilege Policies**
    - **Restrict access to customer and sensitive data based on roles and responsibilities. This reduces the risk of unauthorized access or insider threats.**
2. **Develop and Enforce Disaster Recovery Plans**
    - **Create a detailed disaster recovery plan to ensure business continuity during disruptions. Include periodic testing and employee training on these plans.**
3. **Strengthen Password Policies**
    - **Require employees to use complex passwords that expire regularly. Introduce multi-factor authentication (MFA) to further secure access to systems.**
4. **Enforce Separation of Duties**
    - **Divide critical tasks among different individuals (e.g., payroll, financial management) to minimize fraud risks and reduce the likelihood of insider threats.**
5. **Deploy an Intrusion Detection System (IDS)**
    - **Implement an IDS to monitor network traffic for potential threats, integrate it with a SIEM solution for automated alerts, and regularly review reports.**
6. **Establish Regular Backups**

- **Automate backups of critical data and verify their integrity through periodic restoration tests. Store backups securely, both on-site and off-site.**

7. **Enhance Monitoring and Maintenance for Legacy Systems**
    - **Schedule regular monitoring, maintenance, and security updates for legacy systems. Where feasible, plan to upgrade or replace outdated systems to reduce vulnerabilities.**
8. **Adopt Data Encryption**
    - **Encrypt sensitive data at rest and in transit, including customer credit card information and personally identifiable information (PII).**
9. **Introduce a Password Management System**
    - **Use a centralized password management tool to securely store and share passwords, reducing the risk of password-related breaches.**

Compliance Recommendations

PCI DSS Compliance

1. **Restrict Access to Credit Card Information**
    - **Limit access to authorized personnel by applying role-based access controls and logging all access attempts.**
2. **Secure the Processing Environment**
    - **Use end-to-end encryption and tokenization for credit card data processing, and segregate this environment from other systems.**
3. **Adopt Secure Password Policies**
    - **Align password policies with PCI DSS requirements, including mandatory complexity rules, periodic changes, and MFA for all access points.**

GDPR Compliance

1. Enhance Data Security for E.U. Customers
    - Use encryption and anonymization techniques to ensure the confidentiality of E.U. customers' data.
2. Classify and Inventory Data
    - Create a robust classification system for data, labeling it based on sensitivity (e.g., PII, SPII). Implement access controls aligned with these classifications.

SOC Compliance (Type 1 & Type 2)

1. Establish User Access Policies
    - Implement least privilege and separation of duties policies, ensuring only authorized users access specific types of data.
2. Secure Sensitive Data (PII/SPII)
    - Encrypt sensitive data to ensure its confidentiality and align with SOC requirements. Monitor and audit access logs to maintain data integrity.
3. Limit Data Access to Authorized Individuals
    - Use RBAC and identity management solutions to control data access, ensuring availability only to those with explicit authorization.

Proposed Investments

- **Technology Upgrades: Invest in IDS, encryption tools, and password management systems.**
- **Training: Educate employees on security best practices and compliance requirements.**
- **Policies and Procedures: Develop detailed policies for access control, disaster recovery, and data classification.**