

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.



<https://offensiverhino.netlify.app>

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
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Least Privilege
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disaster recovery plans
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password policies
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separation of duties
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Intrusion detection system (IDS)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Backups
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Antivirus software
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Manual monitoring, maintenance, and intervention for legacy systems
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Encryption
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password management system
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Locks (offices, storefront, warehouse)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Closed-circuit television (CCTV) surveillance
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Only authorized users have access to customers' credit card information.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

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

and has been validated.

☐☒

Data is available to individuals authorized to access it.
