1. Audit Scope (Reviewed)

In scope

- IT infrastructure (on-premises systems)
- Online storefront and payment processing
- Customer and employee data
- Internal users and access controls
- Regulatory compliance (U.S. & E.U.)

Out of scope

- Third-party vendor internal systems (except payment processor responsibilities)

---

2. Audit Goals (Reviewed)

- Identify risks, threats, and vulnerabilities
- Evaluate effectiveness of existing security controls
- Determine regulatory compliance gaps
- Reduce likelihood of data breaches, outages, and fines

---

3. Controls & Compliance Checklist

A. Administrative Controls

Control	Implemented?	Notes
Security policies documented	❌ No	No formal written security policies
Risk management process	⚠️ Partial	Risk assessment performed but not recurring
Incident response plan	❌ No	No documented response or escalation plan
Employee security training	❌ No	Increases phishing and insider risk
Vendor management policy	❌ No	Payment and cloud vendors not formally assessed

---

B. Technical Controls

Control	Implemented?	Notes
Firewalls	⚠️ Partial	Basic firewall present, no monitoring
IDS/IPS	❌ No	Threats may go undetected

Control	Implemented?	Notes
Encryption (data at rest)	❌ No	High risk for customer data
Encryption (data in transit)	⚠️ Partial	HTTPS used, but not enforced everywhere
MFA for admin access	❌ No	Increases risk of credential compromise
Access control / least privilege	❌ No	Excessive permissions identified
Patch management	⚠️ Partial	Updates performed inconsistently
Backup systems	❌ No	No tested backup or recovery plan

C. Physical Controls

Control	Implemented?	Notes
Physical locks	✅ Yes	Basic door locks in place
Secure server/storage area	❌ No	IT assets stored in shared spaces
Surveillance (CCTV)	❌ No	Theft and tampering risk
Visitor access controls	❌ No	No sign-in or escort policy

---

4. Compliance Review

PCI DSS (Online Payments)

Requirement	Status	Risk
Secure cardholder data	❌ Non-compliant	Potential fines and loss of payment privileges
Access controls	❌ Non-compliant	Unauthorized access possible
Logging & monitoring	❌ Non-compliant	Breaches may go undetected

Overall PCI DSS Status: ❌ Non-compliant

GDPR (E.U. Customers)

Requirement	Status	Risk
Data minimization	❌ Non-compliant	Excess data retained
Encryption & protection	❌ Non-compliant	High breach impact

Requirement	Status	Risk
Breach notification process	❌ Non-compliant	Regulatory penalties
User data rights process	❌ Non-compliant	Legal exposure

Overall GDPR Status: ❌ Non-compliant

5. Key Risks Identified

- High likelihood of **data breach**
- Regulatory fines (PCI DSS, GDPR)
- Business disruption due to lack of backups
- Reputational damage and customer trust loss
- Increased exposure to phishing and credential attacks

6. High-Priority Recommendations

1. Develop and enforce **security policies**
2. Implement **encryption**, **MFA**, and **least privilege**
3. Establish **incident response** and **backup plans**
4. Begin **security awareness training**
5. Regularly reassess risks using **NIST CSF**
6. Align systems with **PCI DSS** and **GDPR** requirements

✔️ Audit Conclusion

Botium Toys currently has a **weak security posture** with **significant compliance gaps**. Immediate improvements are required to protect customer data, ensure regulatory compliance, and support secure business growth.