Internal Security Audit
Controls and compliance checklist

Overview:

Conducted a mock security audit focusing on System & Organization Controls to assess user access policies, data integrity, encryption practices & following regulatory compliances.

Objectives:

- Evaluate compliance with System and Organizations Controls
- Identify gaps in least privilege, access controls & data protection
- Recommended actional improvements to strengthen security posture

Tools & Skills used:

- NIST CSF (Framework knowledge)
- Risk assessment & control analysis

Source – Google Cybersecurity certification | ***Coursera***
Erick Leon | LinkedIn **|** Google Cybersecurity Professional Certificate | Coursera

Outcome:

Produces a report summarizing findings & recommendations for improving data confidentiality, access control policies & hardening security posture.

Botium Toys: Scope, goals, and risk assessment report

Does Botium Toys currently have this control in place?

Controls assessment checklist

Yes	No	Control	Explanation
□	☑	Least Privilege	*All employees have access to customer data; privilege needs to be limited to reduce the risk of a breach*
□	☑	Disaster recovery plans	*There are no disaster recovery plans in place. Needs to be implemented to ensure business continuity*
□	☑	Password policies	*Password requirements are minimal*

			which allows a threat actor to easily access secure data via employee devices or accounts
□	☑	Separation of duties	*Needs to be implemented to reduce fraud/access to critical data*
☑	□	Firewall	*Existing firewall blocks traffic based on defined set of security rules*
□	☑	Intrusion detection system (IDS)	*The IT deparmtned needs an IDS in place to help identify possible intrusions by threat actors*
□	☑	Backups	*Backups are vital. The IT department needs to have backups of critical data in the case of a breach & to ensure business continuity*
☑	□	Antivirus software	*Installed & monitored regularly by the IT department*
□	☑	Manual monitoring, maintenance and intervention for legacy systems	*Risk assessments indicates that the legacy systems are monitored & maintained but there isn't a regular schedule in place which could place these systems at a risk of a breach*
□	☑	Encryption	*Encryption is not currently being used. Implementing it would provide greater confidentiality or sensitive information*
□	☑	Password management system	*There is currently no password management system in place. Implementing this would improve IT department & other employee productivity In the case of password issues*
☑	□	Locks (offices, storefronts, warehouses)	*As stated, the physical location has sufficient locks*
☑	□	Closed-circuit television (CCTV) surveillance	*CCTV is installed & functioning at the store's physical location*
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*The physical location has a functioning fire detection & prevention system*

<u>Does Botium Toys currently adhere to this compliance best practice?</u>

Compliance checklist

<u>Payment Card Industry Data Security Standard (PCI DSS)</u>

<u>Yes</u>	**<u>No</u>**	**<u>Best practice</u>**	**<u>Explanation</u>**
□	☑	Only authorized users have access to customers' credit card information	*Currently, all employees* have *access to the company's internal data*
□	☑	Credit card information is stored, accepted, processed, and transmitted internally in a secure environment.	*Credit card information is not encrypted & all employees have access to that information*
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*Botium toys does not currently use encryption to better ensure confidentiality of customer financial information*
□	☑	Adopt secure password management policies.	*Current password policies are nominal & there is not a password management system in place*

<u>General Data Protection Regulation (GDPR)</u>

<u>Yes</u>	**<u>No</u>**	**<u>Best practice</u>**	**<u>Explanation</u>**
□	☑	E.U. customers' data is kept Private and secured.	*The company does not currently use encryption to better ensure the confidentiality of customers financial data*
☑	□	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*There is a plan to notify E.U customers within 72 hours of a data breach*
□	☑	Ensure data is properly classified and inventoried	*Current assets have been inventoried & listed but not classified*

☑	□	Enforce privacy policies, procedures and processes to properly document and maintain data.	*These all been developed & enforced among IT team members & other employees*

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	**No**	**Best practice**	**Explanation**
□	☑	User access policies are established.	*Principle of* least *privilege & separation of duties are not currently in place. All employees have access to internally stored data*
□	☑	Sensitive data (PII/SPII) is confidential and private.	*Encryption is not currently in place to better ensure the confidentiality of PII/SPII*
☑	☑	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is in place as the IT department ensured availability & integrated controls*
□	☑	Data is available to individuals authorized to access it.	*Authorization needs to be limited to only the users who need access to do their jobs*

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented on time.

Recommendations (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

Security Recommendations to Strengthen Botium Toys' Security Posture

1. Access Control & Centralized Identity Management

- Implement Active Directory (AD) & Entra ID

This would establish centralized user authentication, authorization, security groups, device management & password management

- Apply the Principle of Least Privilege

This ensures employees only have access to the data & systems required for their job role

- **<u>Introduce Role-Based Access Control</u> (RBAC)**

Used to separate duties & minimize insider misuse or any disgruntled employees

- **<u>Enable Multi-Factor Authentication </u>(MFA)**

Multi-Factor Authentication (MFA) is not optional anymore. It is a compliance requirement. Enabling MFA would be for all privileged accounts and remote access. ***<u>PCI DSS v4.0</u>*** requires MFA for all personnel with administrative access & anyone accessing the Cardholder Data Environment (CDE). This applies to on-premises & remote access. Since Botium Toys processes credit cards, SOC 2 (Trust Services Criteria), MFA is expected under "Security" and "Confidentiality" principles for protecting access to sensitive data.

---

2. <u>Data Protection & Encryption</u>

- **<u>Encrypt all sensitive data</u> (PII/SPII, credit card data)**

Encrypt both **at rest and in transit** using AES-256 or equivalent standards.

- **<u>Implement tokenization</u>**

For payment card data to comply with PCI DSS.

- **<u>Use SSL/TLS certificates</u>**

This protects data transmitted between systems & applications

- **<u>Restrict direct access</u>**

production databases that contain sensitive data.

---

3. <u>Backup and Disaster Recovery</u>

- **<u>Establish a robust data backup solution</u>**

I recommend **daily incremental backups,** which will capture only data changes to reduce storage use and speed up recovery. Then, **weekly full backups** that copy all critical data for full restoration. A good **on-site storage location option** for data backups would be a Network-Attached Storage, which automates backups from multiple systems, supports RAID & automates daily incremental backups. Another option is a dedicated backup server for quick access.

- **<u>Backup Location</u> (Off-site locations/Cloud)**

Use **Microsoft Azure Backup** or **AWS S3 Glacier** for disaster recovery.

- **<u>Data security controls:</u>**

Encrypt confidential data. All backups are encrypted **at rest (AES-256)** & **in transit (TLS 1.2 or higher)**. Limit access to backup data using **role-based access controls (RBAC)** & perform quarterly restore test to verify backup integrity.

- **<u>Implement a Disaster Recovery (DR) plan</u>**

Outlining clear **RTO** (Recovery Time Objective) and RPO (Recovery Point Objective) & **test the DR plan regularly** to ensure business continuity in case of system failure or cyberattack.

---

4. Monitoring & Threat Detection

- Deploy an Intrusion Detection/Prevention System (IDS/IPS)

Implementing an IDS/IPS will monitor network activity for malicious behavior and prevent any unknown or unauthorized access.

- **Implement centralized logging (SIEM system)**

Use a centralized logging system like Splunk to collect, correlate, and analyze security events across servers, endpoints, and network devices.

- **Perform regular vulnerability scans and penetration testing**

Penetration testing will identify and remediate security weaknesses

---

5. Security Policies & Governance

- Develop and enforce security policies

Include Acceptable Use Policy, Data Classification Policy, Access Control Policy, Encryption Policy, Password Policy & Incident Response Policy

- Train employees on security awareness

Conduct regular internal training requiring all employees to complete to reduce the risk of data breaches & threats. These also include reporting security issues or concerns, phishing emails, data handling & social engineering risks

- Conduct regular audits

This ensures compliance with standards like **NIST CSF**, **PCI DSS** & **ISO 27001**.

---

6. Network Security

- Segment internal networks

Segmentation isolates sensitive systems, databases & payment systems from general user networks

- Use firewalls and network access control (NAC)

Using firewalls will prevent unauthorized internal or external access. You can filter incoming/outgoing traffic & create network rules for any specific alerts

- Regularly update and patch

All operating systems, mobile devices & applications need to be up-to-date to reduce exploitable vulnerabilities. Implement centralized patch management using tools such as Microsoft Intune or Windows Server Update Services (WSUS) to automatically deploy updates and security patches to all endpoints. This ensures that all Windows, macOS, and mobile devices receive critical updates on a scheduled basis, reducing vulnerabilities & maintaining compliance

Thank you.

Erick Leon
10/29/25