# Controls and compliance checklist

Internal Security Audit for: *Botium Toys*

**Controls assessment checklist**

| 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. |

- [ ] [x] Data integrity ensures the data is consistent, complete, accurate, and has been validated.
- [x] [ ] Data is available to individuals authorized to access it.

---

**Recommendations (optional):** Based on my assessment, I would suggest prioritizing several key security improvements. First and foremost, ensuring full compliance with all legal requirements. Given the company's expanding global presence, upholding legal standards is essential to maintain a positive reputation and protect the interests of a diverse clientele. Additionally, it is important to address the security of customers' Personally Identifiable Information (PII) and Sensitive Personal Identifiable Information (SPII). These data assets are highly valuable and currently lack adequate protection. Addressing this area is critical, as any compromise could result in significant harm to both the company and the customers. Lastly, it is recommended to implement stricter access controls within your staff. Presently, every employee has unrestricted access to all company resources. To mitigate risks, you should limit access to specific information according to job roles and responsibilities.

Considering the company's state of being a start up, it's vital to establish a strong security foundation. Begin by implementing fundamental security measures that are typically foundational for any organization. There are additional security concerns to address, I have focused on these three key recommendations as they represent the most pressing issues. Please be aware that there is a considerable amount of work ahead to strengthen your overall security posture.