# Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc). For more details about each control, including the type and purpose, refer to the [control categories](https://docs.google.com/document/d/1btezuy_bMKWoK8pd97ZuzdWB9y6au_zfkrpkfVf8ktI/template/preview) document.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

**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.) |

To complete the compliance checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview). For more details about each compliance regulation, review the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) reading.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

**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. |

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 in a timely manner.

**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.

### **Recommendations for the IT Manager of Botium Toys Inc.**

1. **Strengthen Data Encryption Framework:**
   * Implement a robust encryption framework to safeguard customer, employee, and sensitive personal data from cybercriminals. This framework should ensure data confidentiality and integrity, mitigating risks of data breaches.
2. **Develop a Comprehensive Disaster Recovery Plan:**
   * Establish a thorough disaster recovery strategy to protect employees and maintain business continuity during natural disasters or emergencies.
   * Conduct regular evacuation drills and mandatory training to educate employees on disaster recovery protocols and safety measures.
   * Include advanced survival training to ensure mental and physical stability during crises.
   * Use multiple data backup methods:
     + Daily cloud backups for secure, scalable data storage.
     + Portable hardware backups stored securely off-site.
     + Off-site recovery points for quick restoration and seamless continuation of operations.
3. **Enforce Strict Access Control Mechanisms:**
   * Implement strong access control policies to regulate user permissions and ensure separation of duties.
   * Minimize vulnerabilities by applying the principle of least privilege to all employees.
   * Establish clear group policies that differentiate access levels for regular users and administrators to reduce insider threats and human errors.
4. **Deploy Advanced Intrusion Detection and Prevention Systems (IDS/IPS):**
   * Install high-performance IDS and IPS to monitor, detect, and block potential cyber threats.
   * Ensure systems are updated regularly and monitored 24/7 by a combination of AI and human oversight to respond proactively to threats.
5. **Enhance Password Management Practices:**
   * Use trusted password management tools like "LastPass" to generate and store strong, unique passwords.
   * Incorporate multi-factor authentication (MFA) and CAPTCHA verification for an additional layer of security.
   * Regularly reset passwords (e.g., monthly) to minimize the risk of unauthorized access.
   * Deploy AI-driven tools to detect and block potential cyberattacks targeting user credentials.
6. **Strengthen Legacy System Monitoring:**
   * Schedule regular audits and monitoring for legacy systems to identify vulnerabilities.
   * Implement real-time threat detection and response mechanisms to mitigate risks promptly during security breaches.

By adopting these measures, Botium Toys Inc. can enhance its overall cybersecurity posture, protect critical data assets, and ensure operational resilience against both digital and physical threats.