# 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** |
|  | **X** | Least privilege |
|  | **X** | Disaster recovery plans |
|  | **X** | Password policies |
|  | **X** | Separation of duties |
| **X** |  | Firewall |
|  | **X** | Intrusion detection system (IDS) |
|  | **X** | Backups |
| **X** |  | Antivirus software |
|  | **X** | Manual monitoring, maintenance, and intervention for legacy systems |
|  | **X** | Encryption |
|  | **X** | Password management system |
| **X** |  | Locks (offices, storefront, warehouse) |
| **X** |  | Closed-circuit television (CCTV) surveillance |
| **X** |  | 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** |
|  | **X** | Only authorized users have access to customers’ credit card information. |
|  | **X** | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
|  | **X** | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
|  | **X** | Adopt secure password management policies. |

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | **X** | E.U. customers’ data is kept private/secured. |
| **X** |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  | **X** | Ensure data is properly classified and inventoried. |
| **X** |  | 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** |
|  | **X** | User access policies are established. |
|  | **X** | 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. |

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.

* Backups need to be put in place, as there is currently a huge risk of data loss since all employees have access to the data.
* Encyption and more-than-nominal password policies need to be set up—this ensures that customer data is not immediately visible and that passwords are also secure. The following actions are required:
  + Implement data encryption procedures to better secure credit card transaction touchpoints and data.
  + Adopt secure password management policies.
  + Add a password management system.
* Next, credit card security should be prioritised—several shortcomings are in breach of PCI DSS and GDPR. Currently, all employees having access to internally stored data and customers’ PII/SPII is a huge risk. The following should be put in place:
  + Least privilege
  + Separation of duties

Further, while data is available to all employees, authorisation should be limited to only employees who need to access the information to do their job.

* A disaster recovery plan also needs to be implemented in the case of a data breach.
* There is currently not a regular schedule in place for regular maintenance and intervention for legacy systems. This could put legacy systems at risk of breach.
* An intrusion detection system (IDS) needs to be implemented.

Addendum: Control categories

Control categories

Controls within cybersecurity are grouped into three main categories:

* Administrative/Managerial controls
* Technical controls
* Physical controls

**Administrative/Managerial controls** address the human component of cybersecurity. These controls include policies and procedures that define how an organization manages data and clearly defines employee responsibilities, including their role in protecting the organization. While administrative controls are typically policy based, the enforcement of those policies may require the use of technical or physical controls.

**Technical controls** consist of solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV) products, encryption, etc. Technical controls can be used in a number of ways to meet organizational goals and objectives.

**Physical controls** include door locks, cabinet locks, surveillance cameras, badge readers, etc. They are used to limit physical access to physical assets by unauthorized personnel.

Control types

Control types include, but are not limited to:

1. Preventative
2. Corrective
3. Detective
4. Deterrent

These controls work together to provide defense in depth and protect assets. **Preventative controls** are designed to prevent an incident from occurring in the first place. **Corrective controls** are used to restore an asset after an incident. **Detective controls** are implemented to determine whether an incident has occurred or is in progress. **Deterrent controls** are designed to discourage attacks.

Review the following charts for specific details about each type of control and its purpose.

| **Administrative Controls** | | |
| --- | --- | --- |
| **Control Name** | **Control Type** | **Control Purpose** |
| Least Privilege | Preventative | Reduce risk and overall impact of malicious insider or compromised accounts |
| Disaster recovery plans | Corrective | Provide business continuity |
| Password policies | Preventative | Reduce likelihood of account compromise through brute force or dictionary attack techniques |
| Access control policies | Preventative | Bolster confidentiality and integrity by defining which groups can access or modify data |
| Account management policies | Preventative | Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage |
| Separation of duties | Preventative | Reduce risk and overall impact of malicious insider or compromised accounts |

|  |  |  |
| --- | --- | --- |
| **Technical Controls** | | |
| **Control Name** | **Control Type** | **Control Purpose** |
| Firewall | Preventative | To filter unwanted or malicious traffic from entering the network |
| IDS/IPS | Detective | To detect and prevent anomalous traffic that matches a signature or rule |
| Encryption | Deterrent | Provide confidentiality to sensitive information |
| Backups | Corrective | Restore/recover from an event |
| Password management | Preventative | Reduce password fatigue |
| Antivirus (AV) software | Corrective | Detect and quarantine known threats |
| Manual monitoring, maintenance, and intervention | Preventative | Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems |

|  |  |  |
| --- | --- | --- |
| **Physical Controls** | | |
| **Control Name** | **Control Type** | **Control Purpose** |
| Time-controlled safe | Deterrent | Reduce attack surface and overall impact from physical threats |
| Adequate lighting | Deterrent | Deter threats by limiting “hiding” places |
| Closed-circuit television (CCTV) | Preventative/Detective | Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions |
| Locking cabinets (for network gear) | Preventative | Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear |
| Signage indicating alarm service provider | Deterrent | Deter certain types of threats by making the likelihood of a successful attack seem low |
| Locks | Deterrent/Preventative | Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Detective/Preventative | Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc. |