# Controls and compliance checklist-RESOLVED

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.

Here is a summary of **critical recommendations** for the IT manager at **Botium Toys**, highlighting the controls and compliance best practices that need to be implemented to mitigate risks:

**1. Implement Least Privilege Access and Separation of Duties**

* **Risk**: Unauthorized access to sensitive systems and data, potentially leading to insider threats or data breaches.
* **Recommendation**: Enforce **least privilege access controls** and implement **separation of duties** to limit access based on job responsibilities.
* **Compliance**: Supports **PCI DSS** and **GDPR** compliance.
* **Timeliness**: Immediate action required to prevent malicious insiders or compromised accounts from gaining unauthorized access.

**2. Adopt Strong Data Encryption Procedures**

* **Risk**: Exposure of sensitive data (e.g., customer credit card information, PII) due to inadequate protection, which could lead to financial loss, customer trust issues, or regulatory penalties.
* **Recommendation**: Implement **encryption** for all sensitive data, both at rest and in transit, especially customer credit card data and personal information.
* **Compliance**: Ensures compliance with **PCI DSS** and **GDPR**.
* **Timeliness**: Critical to implement immediately to protect data and meet compliance requirements.

**3. Develop and Test Disaster Recovery and Backup Plans**

* **Risk**: Business disruption, data loss, and prolonged downtime in the event of a breach or system failure, causing operational and reputational damage.
* **Recommendation**: Establish a comprehensive **disaster recovery plan**, perform regular data **backups**, and test the recovery procedures periodically.
* **Compliance**: Supports **SOC 2** and **GDPR** (in case of data loss).
* **Timeliness**: High priority to ensure business continuity and to minimize downtime in the event of an incident.

**4. Strengthen Password Management and Authentication**

* **Risk**: Account compromise due to weak or mismanaged passwords, leading to unauthorized access and potential data breaches.
* **Recommendation**: Enforce strong password policies, ensure **password complexity**, and implement a **centralized password management system** to manage and enforce policies effectively.
* **Compliance**: Supports **SOC 2**, **PCI DSS**, and **GDPR**.
* **Timeliness**: Immediate implementation to secure user accounts and reduce the likelihood of brute force attacks.

**5. Install Intrusion Detection and Prevention Systems (IDS/IPS)**

* **Risk**: Malicious attacks, including unauthorized access or malware infiltration, which could compromise internal systems and data.
* **Recommendation**: Implement **IDS/IPS** to detect and prevent anomalous network traffic or potential threats in real time.
* **Compliance**: Aligns with **PCI DSS** and **SOC 2** security controls.
* **Timeliness**: High urgency to monitor network traffic and detect intrusions proactively.

**6. Classify and Secure Sensitive Data**

* **Risk**: Improper handling or exposure of **PII/SPII** or other sensitive customer data, which could lead to regulatory fines and reputational harm.
* **Recommendation**: **Classify** and **inventory** all sensitive data, ensuring proper access controls and encryption are applied. Regularly review data classification and inventory to ensure appropriate protections.
* **Compliance**: Directly supports **GDPR** and **SOC 2**.
* **Timeliness**: Immediate action required to ensure sensitive data is properly protected and compliant with privacy regulations.

**7. Enhance Incident Response and Breach Notification Procedures**

* **Risk**: Delay in response to a security incident, which could result in extensive data loss, compliance violations, or customer dissatisfaction.
* **Recommendation**: Establish and document an **incident response plan** and ensure procedures are in place to notify affected customers and authorities within the required timelines (e.g., 72 hours for **GDPR**).
* **Compliance**: **GDPR** (notification within 72 hours of a breach) and **PCI DSS**.
* **Timeliness**: Critical to establish and test the plan immediately to minimize response time and reduce risk during a security incident.

**8. Regularly Maintain Legacy Systems**

* **Risk**: Legacy systems may become a point of vulnerability if not properly maintained or updated, potentially exposing the organization to cyberattacks.
* **Recommendation**: Develop a **regular schedule for monitoring and maintaining legacy systems** to ensure they are updated with security patches and remain secure.
* **Compliance**: Aligns with **SOC 2** and other compliance standards requiring regular system reviews.
* **Timeliness**: High priority, especially for systems that store or handle sensitive data.

**9. Implement Regular Security Awareness Training**

* **Risk**: Employees falling victim to phishing or social engineering attacks, which could lead to unauthorized access or data loss.
* **Recommendation**: Implement **regular cybersecurity training** to raise awareness among employees about the latest threats, phishing attacks, and secure data handling practices.
* **Compliance**: Supports **SOC 2** and other industry standards by ensuring employee preparedness in securing data.
* **Timeliness**: Should be a continuous program, with immediate focus on onboarding new employees and conducting refresher training.

**10. Ensure Physical Security Controls Are Up-to-Date**

* **Risk**: Unauthorized physical access to network infrastructure, servers, or sensitive data that could lead to theft or sabotage.
* **Recommendation**: Review and **strengthen physical security** controls such as locks, CCTV, and access restrictions to critical areas.
* **Compliance**: **SOC 2**, **PCI DSS**.
* **Timeliness**: Immediate review needed, especially if security lapses are identified in physical access protocols.

**Conclusion**

Implementing these recommended controls and compliance practices is **crucial for Botium Toys** to reduce risk and improve its security posture. The **timeliness** of these actions is essential, as delays could lead to significant security vulnerabilities, non-compliance risks, potential data breaches, and operational disruptions. Prioritizing controls such as data encryption, access control enforcement, and disaster recovery planning will help secure Botium Toys’ critical assets and ensure regulatory compliance, protecting the company from financial, legal, and reputational damage.

**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.  
  
o reduce risks to assets and improve Botium Toys’ security posture, the IT manager could communicate the following recommendations to stakeholders:

**1. Implement Least Privilege and Access Controls**

* **Recommendation**: Establish and enforce **least privilege access** and **separation of duties** policies. Only grant access to sensitive data (like customer PII and credit card information) to authorized personnel based on their role.
* **Impact**: This will significantly reduce the risk of unauthorized access or malicious insider actions.

**2. Adopt Data Encryption Procedures**

* **Recommendation**: Implement **encryption** for all sensitive data, including customer credit card information, during storage, transmission, and processing.
* **Impact**: This will ensure that sensitive data is protected from unauthorized access, both internally and externally, and will help Botium Toys comply with PCI DSS and GDPR.

**3. Develop and Test Disaster Recovery Plans**

* **Recommendation**: Create a **disaster recovery plan** that includes regular backups, offsite storage, and testing of recovery procedures. Ensure that **critical data** (including financial and customer data) is regularly backed up and easily retrievable in the event of a breach or system failure.
* **Impact**: This will ensure business continuity in case of a breach or other disruption, mitigating the impact of data loss or system downtime.

**4. Enforce Strong Password Policies**

* **Recommendation**: Update the current **password policy** to enforce modern password requirements (e.g., at least 8 characters, a combination of letters, numbers, and special characters) and implement a **centralized password management system**.
* **Impact**: This will reduce the risk of account compromises due to weak passwords or poor password management practices.

**5. Introduce Intrusion Detection and Prevention Systems (IDS/IPS)**

* **Recommendation**: Install and configure an **intrusion detection system (IDS)** and **intrusion prevention system (IPS)** to monitor network traffic for anomalies and potential threats in real time.
* **Impact**: IDS/IPS will help detect and mitigate malicious activities such as unauthorized access attempts, reducing the risk of data breaches.

**6. Regularly Review and Classify Data**

* **Recommendation**: **Classify and inventory all data**, especially sensitive customer data (PII/SPII), and ensure that access controls are aligned with the classification. Implement regular reviews to ensure that data is categorized properly.
* **Impact**: Proper data classification ensures that sensitive data is protected with appropriate controls, minimizing the risk of mishandling or unintentional exposure.

**7. Strengthen Incident Response Procedures**

* **Recommendation**: Ensure that an **incident response plan** is in place and that all stakeholders are trained on how to respond in the event of a data breach or security incident. This includes implementing **breach notification protocols** in line with GDPR and other relevant regulations.
* **Impact**: This will help Botium Toys respond quickly and effectively to security incidents, reducing the impact on data integrity and minimizing potential regulatory penalties.

**8. Implement Antivirus and Endpoint Protection Software**

* **Recommendation**: Ensure that **antivirus software** and **endpoint protection** tools are installed and regularly updated on all employee devices, including remote workstations, to protect against malware, ransomware, and other malicious software.
* **Impact**: This will help prevent the spread of malware and reduce the risk of endpoint compromises.

**9. Implement Security Monitoring for Legacy Systems**

* **Recommendation**: Establish a regular monitoring and maintenance schedule for **legacy systems** to ensure they are secure, up-to-date, and monitored for vulnerabilities.
* **Impact**: Keeping legacy systems secure will prevent these systems from becoming a point of vulnerability in the organization’s overall security posture.

**10. Review and Update Physical Security Measures**

* **Recommendation**: While physical security measures like locks and CCTV are in place, ensure regular reviews and updates to ensure they are functioning optimally. Consider upgrading physical security systems if needed (e.g., badge readers, time-controlled safes).
* **Impact**: Strong physical security will prevent unauthorized personnel from accessing critical assets, including inventory and network infrastructure.

**11. Align with Compliance Regulations (e.g., PCI DSS, GDPR)**

* **Recommendation**: Work with the legal and compliance teams to ensure that **Botium Toys** meets all regulatory requirements such as **PCI DSS** (for payment card data) and **GDPR** (for European customers’ data). This includes adopting industry best practices, conducting regular compliance audits, and implementing necessary safeguards.
* **Impact**: Adhering to compliance standards will reduce legal risks and protect the company from regulatory fines and reputational damage.

**12. Continuous Training and Awareness Programs**

* **Recommendation**: Regularly conduct **cybersecurity awareness training** for all employees to educate them on the latest phishing threats, secure data handling practices, and their role in safeguarding company assets.
* **Impact**: A well-trained workforce is less likely to fall victim to social engineering attacks and will be better equipped to handle potential security incidents.

**13. Implement Centralized Logging and Monitoring**

* **Recommendation**: Set up centralized logging and monitoring for all systems and devices across the organization. This will include tracking user access, system events, and anomalies.
* **Impact**: Centralized monitoring will allow for quicker detection of potential threats and enable prompt response to suspicious activities.

By implementing these recommendations, Botium Toys will be better equipped to reduce risk, protect sensitive data, ensure compliance with industry standards, and improve the overall security posture.