# 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.

# Lista de verificación de controles y cumplimiento

Para completar la lista de verificación de evaluación de controles, consulte la información proporcionada en el informe de alcance, objetivos y evaluación de riesgos. Para obtener más detalles sobre cada control, incluido el tipo y el propósito, consulte el documento de categorías de control.

Luego, seleccione “sí” o “no” para responder la pregunta: ¿Botium Toys cuenta actualmente con este control?

**Lista de verificación de evaluación de controles**

|  |  |  |
| --- | --- | --- |
| Si | No | Control |
|  | X | Privilegios mínimos |
|  | X | Planes de recuperación ante desastres |
| X |  | Políticas de contraseñas |
|  | X | Separación de funciones |
| X |  | Cortafuegos |
|  | X | Sistema de detección de intrusiones (IDS) |
|  | X | Copias de seguridad |
| X |  | Software antivirus |
|  | X | Supervisión, mantenimiento e intervención manuales para sistemas heredados |
|  | X | Cifrado |
|  | X | Sistema de gestión de contraseñas |
| X |  | Cerraduras (oficinas, escaparates, almacenes) |
| X |  | Vigilancia por circuito cerrado de televisión (CCTV) |
| X |  | Detección/prevención de incendios (alarma contra incendios, sistema de rociadores, etc.) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Para completar la lista de verificación de cumplimiento, consulte la información proporcionada en el informe de alcance, objetivos y evaluación de riesgos. Para obtener más detalles sobre cada normativa de cumplimiento, revise los controles, los marcos y la lectura de cumplimiento.

Luego, seleccione “sí” o “no” para responder la pregunta: ¿Botium Toys se adhiere actualmente a esta práctica recomendada de cumplimiento?

**Lista de verificación de cumplimiento**

Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)

|  |  |  |
| --- | --- | --- |
| Si | No | Práctica recomendada |
|  | X | Solo los usuarios autorizados tienen acceso a la información de la tarjeta de crédito de los clientes. |
|  | X | La información de la tarjeta de crédito se almacena, acepta, procesa y transmite internamente, en un entorno seguro. |
|  | X | Implemente procedimientos de cifrado de datos para proteger mejor los puntos de contacto y los datos de las transacciones con tarjeta de crédito. |
|  | X | Adopte políticas de gestión de contraseñas seguras. |

Reglamento general de protección de datos (RGPD)

|  |  |  |
| --- | --- | --- |
| Sí | No | Práctica recomendada |
| X |  | Los datos de los clientes de la UE se mantienen privados/seguros. |
| X |  | Existe un plan para notificar a los clientes de la UE en un plazo de 72 horas si sus datos se ven comprometidos/hay una violación. |
| X |  | Asegúrese de que los datos estén clasificados e inventariados correctamente. |
| X |  | Aplique políticas, procedimientos y procesos de privacidad para documentar y mantener los datos correctamente. |

Controles de sistemas y organizaciones (SOC tipo 1, SOC tipo 2)

|  |  |  |
| --- | --- | --- |
| Si | No | Mejores prácticas |
|  | X | Se establecen políticas de acceso de usuarios. |
|  | X | Los datos confidenciales (PII/SPII) son confidenciales/privados. |
|  | X | La integridad de los datos garantiza que los datos sean consistentes, completos, precisos y hayan sido validados. |
| X? |  | Los datos están disponibles para las personas autorizadas a acceder a ellos. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Esta sección es opcional y se puede utilizar para proporcionar un resumen de recomendaciones al gerente de TI sobre qué controles y/o mejores prácticas de cumplimiento debe implementar Botium Toys, según el riesgo que se presente si no se implementan de manera oportuna.

**Recomendaciones (opcional):** En esta sección, proporcione recomendaciones relacionadas con los controles y/o las necesidades de cumplimiento que su gerente de TI podría comunicar a las partes interesadas para reducir los riesgos de los activos y mejorar la postura de seguridad de Botium Toys.

**-**

Para reducir los riesgos de los activos mejorando así la seguridad de la empresa Botium Toys se recomienda establecer plazos de cumplimiento y delegar a la persona/s encargada/s para ejecutar cada tarea como por ejemplo: proteger los datos PII y SPII, establecer un sistema de gestión de contraseñas seguras, establecer planes de monitoreos y mantenimiento de los sistemas heredados, entre otros, para mejoras de seguridad de la institución.

**-**