Control and Compliance Checklist Exemplar

Control assessment checklist:

|  |  |
| --- | --- |
| **Control Name** | **Explanation** |
| Least Privilege | Currently, all employees have  access to customer data;  privileges need to be limited  to reduce the risk of a breach. |
| Disaster recovery plans | There are no disaster recovery plans in place. These need to be implemented to ensure business continuity. |
| Password policies | Employee password  requirements are minimal,  which could allow a threat  actor to more easily access  secure data/other assets via  employee work  equipment/the internal  network. |
| Separation of duties | Needs to be implemented to  reduce the possibility of  fraud/access to critical data,  since the company CEO  currently runs day-to-day  operations and manages the  payroll. |

|  |  |
| --- | --- |
| **Control Name** | **Control Purpose** |
| Firewall | The existing firewall blocks  traffic based on an  appropriately defined set of  security rules. |
| IDS/IPS | The IT department needs an  IDS in place to help identify  possible intrusions by threat  actors. |
| Encryption | Encryption is not currently  used; implementing it would  provide greater confidentiality of sensitive information. |
| Backups | The IT department needs to  have backups of critical data,  in the case of a breach, to  ensure business continuity. |
| Password management | There is no password  management system currently in place; implementing this  control would improve IT  department/other employee  productivity in the case of  password issues. |
| Antivirus (AV) software | Antivirus software is installed  and monitored regularly by the IT department. |
| Manual monitoring, maintenance, and intervention | The list of assets notes the use of legacy systems. The risk assessment indicates that  these systems are monitored  and maintained, but there is  not a regular schedule in place for this task and procedures/policies related to intervention are unclear, which could place these systems at risk of a breach. |

|  |  |
| --- | --- |
| **Control Name** | **Explanation** |
| Closed-circuit television (CCTV) | CCTV is installed/functioning  at the store’s physical location. |
| Locks | The store’s physical location, which includes the company’s main offices, store front, and warehouse of products, has sufficient locks. |
| Fire detection and prevention (fire alarm, sprinkler system, etc.) | Botium Toys’ physical location has a functioning fire  detection and prevention  system. |

|  |  |  |  |
| --- | --- | --- | --- |
| **General Data Protection Regulation** | **Best Practice** | **Explanation** | |
| No | E.U. customers’ data is kept  private/secured. | The company does not currently  use encryption to better ensure the  confidentiality of customers’  financial information. | |
| Yes | There is a plan in place to notify  E.U. customers within 72 hours  if their data is  compromised/there is a  breach. | There is a plan to notify E.U.  customers within 72 hours of a  data breach. | |
| No | Ensure data is properly  classified and inventoried. | Current assets have been  inventoried/listed, but not  classified. | |
| Yes | Enforce privacy policies,  procedures, and processes to  properly document and  maintain data. | Privacy policies, procedures, and  processes have been developed  and enforced among IT team  members and other employees, as  needed. |

|  |  |  |
| --- | --- | --- |
| **System and Organizations Controls (SOC type 1, SOC type 2)** | **Best Practice** | **Explanation** |
| No | User access policies are  established. | Controls of Least Privilege and separation of duties are not currently in place; all  employees have access to  internally stored data. |
| No | Sensitive data (PII/SPII) is confidential/private. | Encryption is not currently used to better ensure the  confidentiality of PII/SPII. |
| Yes | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | Data integrity is in place. |
| No | Data is available to individuals authorized to access it. | While data is available to all  employees, authorization  needs to be limited to only the individuals who need access to it to do their jobs. |