**Security Audit Compliance Requirements**

**Purpose of the Document:** This document outlines details on Implementing secure methodologies, and security controls and establishes Incident Response and Disaster Recovery plans to be compliant with GDPR (General Data Protection and Regulation), PCI-DSS (Payment Card Industry Data Security Standard), ECPA (Electronic Communications and Privacy Act) and Gramm-Leach-Bliley Act (GLBA) as Botium deals with an E-commerce website. We outline this information using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as a baseline framework.

**Background:** Botium is a toy company that is facing huge fines as it is non-compliant with the laws and regulations. To avoid fines, the organization is ready to revisit the policies already in place.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a voluntary framework designed to help organizations manage and improve their cybersecurity posture. This includes 5 Core functions. They are:

* Identify: Understand and prioritize assets, business processes, and risks.
* Protect: Implement safeguards to ensure the delivery of critical infrastructure services.
* Detect: Develop and implement activities to identify the occurrence of a cybersecurity event.
* Respond: Develop and implement appropriate actions to mitigate the impact of a detected cybersecurity event.
* Recover: Develop and implement activities to restore services impaired due to a cybersecurity event.

**Current State:**

* Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII.
* Encryption is not currently used to ensure the confidentiality of customers’ credit card information that is accepted, processed, transmitted, and stored locally in the company’s internal database.
* Access controls pertaining to least privilege and separation of duties have not been implemented.
* The IT department has ensured availability and integrated controls to ensure data integrity.
* The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
* Antivirus software is installed and monitored regularly by the IT department.
* The IT department has not installed an intrusion detection system (IDS).
* There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
* The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
* Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
* There is no centralized password management system that enforces the password policy’s minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
* While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
* The store’s physical location, which includes Botium Toys’ main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

**Recommendations:** Along with existing measures of CCTV Surveillance, Fire detection and Prevention systems, Firewalls, Antivirus software and a plan to notify EU members in 72 hours we recommend to include

**Preventive Measures:**

* Implement the Least-privilege principle for the employees along with Segregation of duties in place.
* Implement Two-person integrity for accessing Data Centers and Restricted Zones.
* Re-design the outside of the organization based on CPTED (Crime Detection through Environmental Design) and add access policy violations using geotagging and geofencing.
* Implement password policies with complexity requirements and include MFA (Multi-factor Authentication) and enforce on the current and future systems/assets.
* Perform salting and hashing on passwords while storing them in Databases.
* Enforce privacy policies, procedures, and processes to properly document and maintain data.
* Patch management and configuration management should be in place to avoid vulnerabilities in legacy systems.

**Corrective Measures:**

* Appropriate Incident Response, Business Continuity, and Disaster Recovery plans should be in place.
* Full, Incremental, and Differential backups can be taken to rely on during the incident and recovery process.
* Manual Monitoring, intervention, and maintenance are required along with strict rules for firewalls.
* CCTV Surveillance can reduce the risk of certain types of events from occurring and can be used after an event to inform on event conditions.

**Deterrent Measures:**

* Encrypt the card information before storing it in databases.
* Time-controlled safe and Alarms help in reducing attack surface along with the locks.

Detective Measures:

* Implement IDS and SIEM tools to monitor and detect the events/Incidents.