Controls and Compliance Audit

Conducted By: Maxwell
Date: 09-02-2022
Client: (Details removed for privacy reasons)
Physical Address: (Details removed for privacy reasons)
Fwd To: (Details removed for privacy reasons)
Frameworks: **NIST CSF, PCI DSS, GDPR, SOC Type 1, SOC Type 2**

Controls Assessment

Yes	**No**	**Control**	***Explanation***
☐	☑	Least Privilege	*At present, five employees (Sales Floor Associates) possess access to customer data. It is crucial to restrict privileges in order to mitigate the risk of a potential breach.*
☐	☑	Disaster recovery plans	*Disaster recovery plans have not been established. It is imperative to implement these plans to guarantee uninterrupted business operations.*
☐	☑	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	*Implementation of measures is necessary to mitigate the risk of fraud and unauthorized access to critical data. This is especially crucial as the company CEO currently oversees day-to-day operations and manages the payroll.*
☑	□	Firewall	*The existing firewall effectively blocks traffic based on a well-defined set of security rules.*
□	☑	Intrusion detection system (IDS)	*The IT department requires an Intrusion Detection System (IDS) to be implemented to aid in the identification of potential intrusions by threat actors.*
□	☑	Backups	*It is essential for the IT department to establish backups of critical data to guarantee business continuity in the event of a breach.*
☑	□	Antivirus software	*The IT department has installed antivirus software and conducts regular monitoring to ensure its effectiveness.*

☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The list of assets includes legacy systems. The risk assessment highlights that while these systems are monitored and maintained, there is no established regular schedule for this task. Additionally, procedures and policies related to intervention are unclear, potentially putting these systems at risk of a breach.*
☐	☑	Encryption	*Currently, encryption is not utilized. Implementing encryption would significantly enhance the confidentiality of sensitive information.*
☐	☑	Password management system	*A password management system is not currently in place. Implementing this control would lead to improved productivity for both the IT department and other employees in the case of password-related issues.*
☑	☐	Locks (offices, storefront, warehouse)	*The physical location of the store, encompassing the main offices, store front, and product warehouse, is equipped with adequate locks for security.*
☑	☐	Closed-circuit television (CCTV) surveillance	*(CCTV) is installed and operational at the store's physical location.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location is equipped with a fully operational fire detection and prevention system.*

Compliance

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	*Explanation*
□	☑	Only authorized users have access to customers’ credit card information.	*At present, all employees have unrestricted access to the company's internal data.*
□	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*The credit card information is not encrypted, and all employees currently have access to internal data, including customers' credit card information. This poses a significant security risk and requires immediate attention.*
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company currently does not employ encryption to enhance the confidentiality of customers' financial information. This presents a notable security vulnerability that needs to be addressed.*
□	☑	Adopt secure password management policies.	*The existing password policies are minimal, and there is no password management system in operation. This poses a significant security risk and requires immediate attention.*

General Data Protection Regulation (GDPR)

Yes	**No**	**Best practice**	***Explanation***
□	☑	E.U. customers' data is kept private/secured.	*The company presently does not employ encryption to enhance the confidentiality of customers' financial information. This presents a notable security vulnerability that needs to be addressed.*
☑	□	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.*
□	☑	Ensure data is properly classified and inventoried.	*The current assets have been inventoried and listed, but they have not been classified yet. This classification step is crucial for effective management and protection of assets.*
☑	□	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been established and are being enforced among IT team members and other employees as necessary. This ensures compliance and protection of sensitive information.*

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	**No**	**Best practice**	***Explanation***
□	☑	User access policies are established.	*Controls for Least Privilege and Separation of Duties are currently not implemented. This means that all employees have unrestricted access to internally stored data. This presents a significant security risk and necessitates immediate attention.*
□	☑	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not presently utilized to enhance the confidentiality of Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). This poses a notable security vulnerability that requires prompt attention.*
☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity measures are already in place, ensuring the accuracy and reliability of the stored information.*
□	☑	Data is available to individuals authorized to access it.	*Although data is currently accessible to all employees, it is crucial to restrict authorization to only those individuals who require access to perform their job responsibilities. This will enhance data security and confidentiality.*

Recommendations:

To enhance (REDACTED) security posture and safeguard sensitive information, it is imperative to implement several key controls. These include:

Least Privilege
Disaster Recovery Plans
Password Policies
Separation of Duties
Intrusion Detection System (IDS)
Ongoing Legacy System Management
Encryption
Password Management System
Addressing compliance gaps necessitates the implementation of controls such as Least Privilege, Separation of Duties, and Encryption. Additionally, proper asset classification is essential to identify and apply additional controls that will further fortify the security posture and protect sensitive information.