Controls and compliance checklist

Current assets

Assets managed by the IT Department include:

● On-premises equipment for in-office business needs
● Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
● Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse
● Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
● Internet access
● Internal network
● Data retention and storage
● Legacy system maintenance: end-of-life systems that require human monitoring

Controls assessment checklist

Yes	No	Control	Explanation as Per Scope, goals, and risk assessment report
☐	☑	Least Privilege	Access controls pertaining to least privilege and separation of duties have not been implemented.
☐	☑	Disaster recovery plans	There are no disaster recovery plans currently in place,

☑	☐	Password policies	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).
☐	☑	Separation of duties	Access controls pertaining to least privilege and separation of duties have not been implemented.
☑	☐	Firewall	The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
☐	☑	Intrusion detection system (IDS)	The IT department has not installed an intrusion detection system (IDS).
☐	☑	Backups	The company does not have backups of critical data.
☑	☐	Antivirus software	Antivirus software is installed and monitored regularly by the IT department.
☑	☐	Manual monitoring, maintenance, and intervention for legacy systems	While legacy systems are monitored and maintained, there is no regular the schedule in place for these tasks and intervention methods are unclear.
☐	☑	Encryption	Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.

☐	☑	Password management system	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.
☑	☐	Locks (offices, storefront, warehouse)	The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks,
☑	☐	Closed-circuit television (CCTV) surveillance	The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has up-to-date closed-circuit television (CCTV) surveillance,
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has functioning fire detection and prevention systems.

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Explanation as Per Scope, goals, and risk assessment report

☐	☑	Only authorized users have access to customers' credit card information.	Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Due to above explanation and encryption not being used, Botium Toys does not meet the requirements
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
☐	☑	Adopt secure password management policies.	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.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation as Per Scope, goals, and risk assessment report
☐	☑	E.U. customers' data is kept private/secured.	Due to above explanation and encryption not being used, Botium Toys does not meet the requirements
☑	☐	There is a plan in place to notify E.U. customers	The IT department has established a plan to notify E.U. customers within 72

		within 72 hours if their data is compromised/there is a breach.	hours if there is a security breach.
☐	☑	Ensure data is properly classified and inventoried.	All employees have access to internally classified and inventoried data.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Botium Toys have privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.

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

Yes	No	Best practice	Explanation as Per Scope, goals, and risk assessment report
☐	☑	User access policies are established.	User access policies are not established and need to be reviewed
☐	☑	Sensitive data (PII/SPII) is confidential/private.	all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	The IT department has ensured availability and integrated controls to ensure data integrity.
☐	☑	Data is available to individuals authorized to access it.	all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.

Recommendations:

Based on the information present in the Risk Assessment report and after the completion of the Controls and Compliance Checklist, below are my recommendations for enhancing the security and compliance posture of Botium Toys' IT department and management of assets, systems, and services:

1. Least Privilege:

- Implement access controls to ensure that employees have the minimum privileges required to perform their job functions. This principle helps limit the potential damage that could be caused by unauthorized access. Especially in this case where all Botium Toys' employees have access to internal, sensitive and potentially confidential data.

2. Disaster Recovery Plans:

- Develop and implement comprehensive disaster recovery plans to ensure business continuity in case of emergencies.

3. Password Policies:

- Update the password policy to align with current best practices, such as requiring passwords to be at least eight characters, a combination of letters and at least one number; special characters

4. Separation of Duties:

- Implement access controls (RBAC) and separation of duties to prevent conflicts of interest and unauthorized access.

5. Intrusion Detection System (IDS):

- Even though a firewall is installed, consider installing an intrusion detection system to monitor and detect potential security threats and breaches.

6. Backups:

- Develop and implement a backup strategy to ensure data recovery in case of data loss or system failures.

7. Manual Monitoring and Maintenance for Legacy Systems:

- Establish a regular schedule for monitoring and maintaining legacy systems and ensure that intervention methods are well-defined.

8. Encryption:

- Implement encryption to protect the confidentiality of customers' credit card information stored, accepted, processed, transmitted, and stored locally in the company's internal database.

9. Password Management System:

- Implement an improved centralized password management system to enforce password policy requirements and improve productivity of recovering and resetting of password

Compliance Recommendations:

1. Payment Card Industry Data Security Standard (PCI DSS):

- Limit access to customers' credit card information to authorized users only

- Implement data encryption procedures for credit card transaction touchpoints.

- Adopt secure password management policies.

2. General Data Protection Regulation (GDPR):

- Ensure that E.U. customers' data is kept private and secured.

- Properly classify and inventory data.

- Enforce privacy policies, procedures, and processes for data management.

3. System and Organizations Controls (SOC Type 1, SOC Type 2):

- Establish user access policies.

- Ensure that sensitive data (PII/SPII) is kept confidential and private.

- Implement data integrity controls.

- Restrict data access to authorized individuals.