# Controls and compliance checklist exemplar

### Controls assessment checklist

Yes	No	Control	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.
	<b>▽</b>	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.
		Firewall	The existing firewall blocks traffic based on an appropriately defined set of security rules.

		Intrusion detection system (IDS)	The IT department needs an IDS in place to help identify possible intrusions by threat actors.
	✓	Backups	The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.
$\checkmark$		Antivirus software	Antivirus software is installed and monitored regularly by the IT department.
		Manual monitoring, maintenance, and intervention for legacy systems	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.
	✓	Encryption	Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.
	<b>▽</b>	Password management system	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.
$\checkmark$		Locks (offices, storefront, warehouse)	The store's physical location, which includes the company's main offices, store front, and warehouse of products, has

		sufficient locks.
$\checkmark$	Closed-circuit television (CCTV) surveillance	CCTV is installed/functioning at the store's physical location.
V	Fire detection/prevention (fire alarm, sprinkler system, etc.)	Botium Toys' physical location has a functioning fire detection and prevention system.

## Compliance checklist

## Payment Card Industry Data Security Standard (PCI DSS)

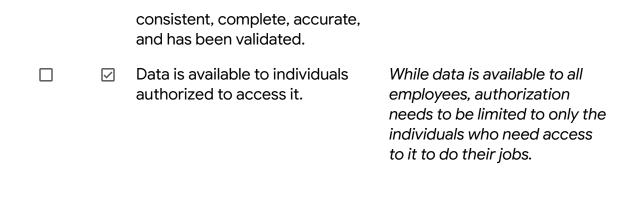
Yes	No	Best practice	Explanation
	$\checkmark$	Only authorized users have access to customers' credit card information.	Currently, all employees have access to the company's internal data.
	$ \vee $	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	Credit card information is not encrypted and all employees currently have access to internal data, including customers' credit card information.
	<b>V</b>	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	The company does not currently use encryption to better ensure the confidentiality of customers' financial information.
	$\checkmark$	Adopt secure password management policies.	Password policies are nominal and no password management system is currently in place.

### General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
	$\checkmark$	E.U. customers' data is kept private/secured.	The company does not currently use encryption to better ensure the confidentiality of customers' financial information.
✓		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.
	$\checkmark$	Ensure data is properly classified and inventoried.	Current assets have been inventoried/listed, but not classified.
✓		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)

Yes	No	Best practice	Explanation
	✓	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.
	<b>✓</b>	Sensitive data (PII/SPII) is confidential/private.	Encryption is not currently used to better ensure the confidentiality of PII/SPII.
$\checkmark$		Data integrity ensures the data is	Data integrity is in place.



## Recommendations for Improved Security Posture at Botium Toys

Here are some key recommendations that the IT manager can communicate to stakeholders to reduce risks and enhance Botium Toys' security posture:

- 1. Implement a Comprehensive Asset Management Program:
  - Conduct a thorough inventory of all IT assets, including hardware, software, and data.
  - Classify assets based on criticality to business operations.
  - Establish clear ownership and accountability for each asset.
  - Track asset lifecycle from acquisition to disposal.
- 2. Strengthen Access Controls:
  - Implement the principle of least privilege, granting users access only to the resources they require for their job functions.
  - Enforce separation of duties to prevent individuals from having excessive control over critical data or processes.
  - Regularly review and update user access privileges.
  - Consider multi-factor authentication (MFA) for additional access security.

#### 3. Encrypt Sensitive Data:

- Encrypt all customer data at rest and in transit, including credit card information, PII, and SPII.
- Implement a robust key management strategy to protect encryption keys.

#### 4. Enhance Network Security:

- Install and configure an intrusion detection system (IDS) to monitor network traffic for malicious activity.
- Regularly update security software (firewalls, antivirus, etc.) with the latest patches.
- Segment the network to isolate critical systems and data from less sensitive areas.

#### 5. Develop a Disaster Recovery Plan:

- Create a comprehensive disaster recovery plan that outlines procedures for recovering critical systems and data in case of an outage or security incident.
- Regularly test the disaster recovery plan to ensure its effectiveness.
- Implement a secure data backup strategy with regular backups stored offsite.

#### 6. Strengthen Password Policy and Management:

- Enforce a strong password policy with minimum complexity requirements (length, character types).
- Implement a centralized password management system to enforce password policy and reduce password fatigue.
- Educate employees on password security best practices, including avoiding password reuse and phishing scams.

#### 7. Address Legacy System Vulnerabilities:

- Develop a schedule for regular maintenance and patching of legacy systems.
- Consider upgrading or replacing outdated systems that are no longer supported by vendors.

#### 8. Compliance Considerations:

- Identify relevant data privacy regulations that Botium Toys needs to comply with (e.g., GDPR, CCPA).
- Implement controls and procedures to ensure compliance with these regulations.
- Regularly review and update compliance policies as regulations evolve.

#### Communication Strategy:

When presenting these recommendations to stakeholders, the IT manager should:

- Focus on business impact: Explain how weak security controls can disrupt operations, damage reputation, and result in financial losses.
- Quantify risks where possible: Use data breaches or cyberattacks impacting similar companies to illustrate potential costs.
- Present solutions in a cost-effective manner: Highlight the long-term benefits of security investments compared to the potential costs of a security incident.

By implementing these recommendations and effectively communicating the importance of security to stakeholders, Botium Toys can significantly reduce risks and build a more robust security posture.