Scenario

Review the following scenario. Then complete the step-by-step instructions.

This scenario is based on a fictional company:

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy's online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She's worried about maintaining compliance and business operations as the company grows without a clear plan. She believes an internal audit can help better secure the company's infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

Your task is to review the IT manager's scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

Review of Botium Toys: Scope, goals, and risk assessment report

Scope and Goals of the Audit Scope:

- The audit will assess all assets and internal processes, including equipment, systems, software, services, and procedures related to controls and compliance best practices.

Goals:

- Assess current assets: Evaluate how well the company's assets are managed and protected.
- Complete the controls and compliance checklist: Determine which controls and compliance best practices need to be implemented to improve security.

Current Assets:

The assets managed by the IT department cover a broad range, including:

- On-premises equipment (e.g., office hardware)
- Employee equipment (desktops, smartphones, remote workstations)
- Storefront products (inventory and e-commerce platforms)
- Internal systems (e.g., accounting, database, security, inventory management)
- Internet access, internal network, and data storage systems
- Legacy system maintenance

Risk Assessment

Risk Description:

- Inadequate management of assets: There's a lack of comprehensive management of these assets, leading to potential security and compliance risks.
- Lack of controls: Key security measures are missing, and compliance with industry standards/regulations (such as PCI DSS or GDPR) is not fully ensured.

Risk Score:

- Risk Score: 8/10 – High risk, driven by inadequate controls and non-compliance with regulations.

Risk Impact:

- Medium impact from asset loss: Due to unknown risks related to asset loss.
- High risk from fines or penalties: Because of non-compliance and lack of data protection controls, especially regarding sensitive data like credit card info or personally identifiable information (PII).

Control Best Practices (NIST CSF – Identify function):

Asset Identification: Resources should be dedicated to identifying and classifying all assets. This is crucial for managing them properly and understanding the potential consequences of losing key assets.

Key Findings and Vulnerabilities

1. **Access Control Issues:** All employees have access to sensitive data, including cardholder data and customer PII. **Recommendation:** Implement least privilege access and separation of duties policies to restrict access to sensitive data based on roles.

2. **Lack of Encryption:** No encryption for credit card info - This is a major concern for protecting customer data and complying with PCI DSS. **Recommendation:** Implement end-to-end encryption (E2EE) for all payment-related data, both in transit and at rest.

3. Weak Password Policy: The password policy is insufficient and does not enforce modern best practices. **Recommendation:** Strengthen the password policy to require complex passwords (e.g., at least 8 characters, with a mix of letters, numbers, and symbols), and implement a centralised password management system for enforcing these policies.

4. No Intrusion Detection System (IDS): The lack of an IDS leaves the network vulnerable to undetected attacks. **Recommendation:** Install and configure an IDS to monitor and respond to suspicious network activity.

5. Lack of Backup and Disaster Recovery Plans: No disaster recovery plan or backups of critical data. **Recommendation:** Establish a comprehensive disaster recovery and business continuity plan, including regular backups of critical data.

6. Inadequate Legacy System Maintenance: Legacy systems are monitored but without a clear schedule or process for regular updates. **Recommendation:** Create a schedule for maintaining and upgrading legacy systems to reduce the risk of vulnerabilities from outdated technology.

7. Lack of Security Awareness: While there are privacy policies in place, there's no mention of security awareness training for employees, which is critical to prevent phishing and other attacks. **Recommendation:** Implement regular security training for all employees to improve awareness of threats and how to handle sensitive data.

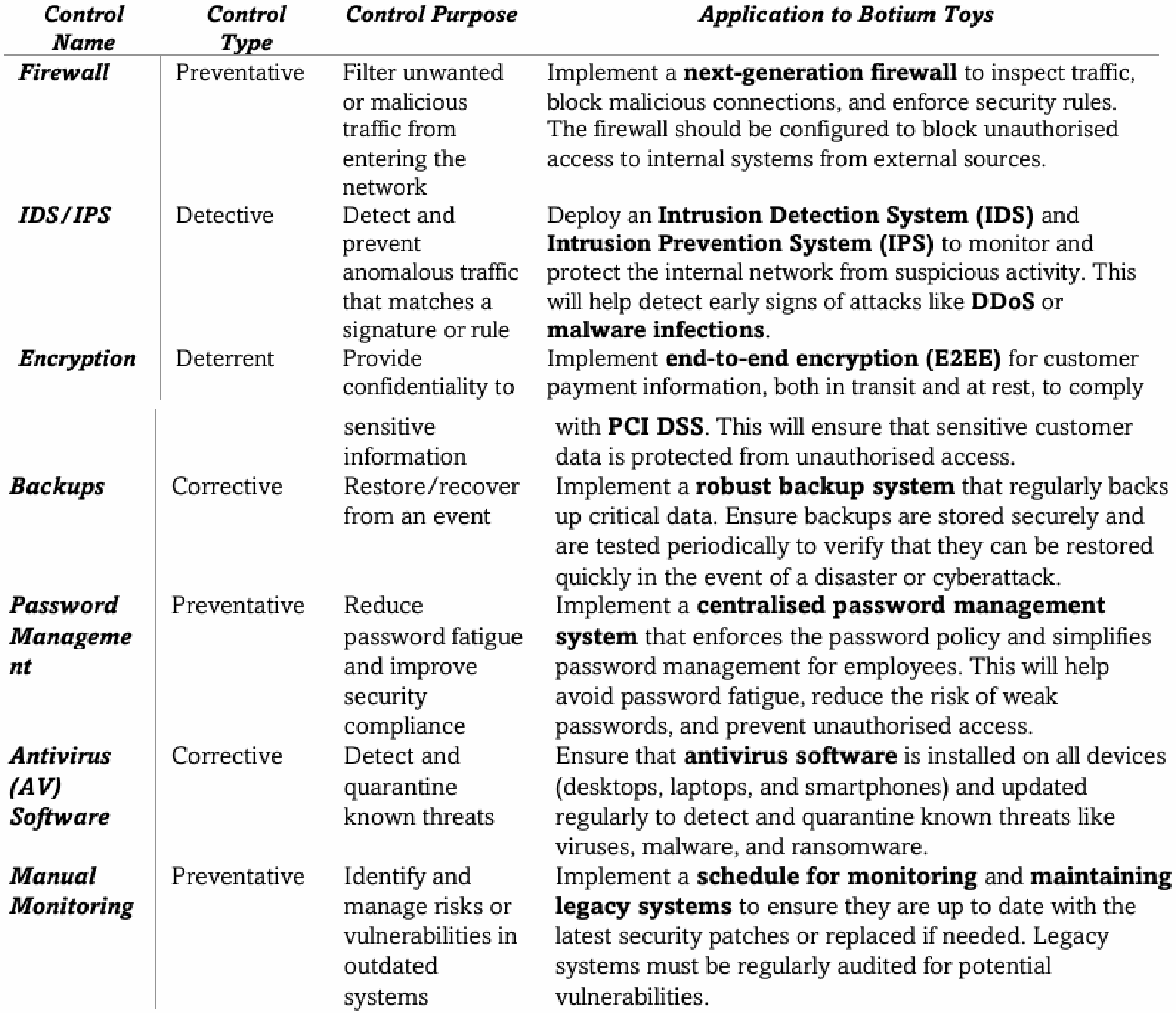
8. Physical Security: The company has good physical security with locks, CCTV, and fire detection systems. **Recommendation:** Continue to monitor and maintain these physical security measures, as they are essential for protecting both people and assets.

Analysis of control categories and application to Botium Toys

Administrative/Managerial Controls

Control Name	*Control Type*	*Control Purpose*	*Application to Botium Toys*
Least Privilege	Preventative	Reduce risk and overall impact of malicious insiders or compromised accounts	Implement **role-based access controls** (RBAC) to ensure that employees only have access to data and systems necessary for their roles. For example, employees working in the warehouse should not have access to customer payment details or internal financial systems.
Disaster Recovery Plans	Corrective	Provide business continuity	**Disaster recovery** planning is critical. Since Botium Toys has no current plan, they need to establish one to restore operations after an incident, such as a system failure, data breach, or natural disaster. A **backup** system and a detailed recovery process should be in place.
Password Policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack techniques	Strengthen the **password policy** (minimum length, complexity requirements, and expiration). Implement a **centralised password management system** to enforce this policy and reduce risks like password reuse or weak passwords.
Access Control Policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data	Implement **access control lists (ACLs)** to define who can access and modify critical data like customer PII/SPII. Include **separation of duties** to ensure that no single individual has access to both customer data and the ability to modify payment details.
Account Management Policies	Preventative	Manage account lifecycle, reducing attack surface, and limiting impact from disgruntled employees	Implement **account management** procedures to ensure that accounts are promptly disabled when employees leave or change roles. Consider setting up **automated workflows** for account creation, modification, and deactivation to ensure that no unused accounts remain active.
Separation of Duties	Preventative	Reduce risk and overall impact of malicious insiders or compromised accounts	Enforce **separation of duties** between employees who handle customer service, financial transactions, and systems administration. For example, employees who manage the online store should not be able to access or modify payment processing systems.

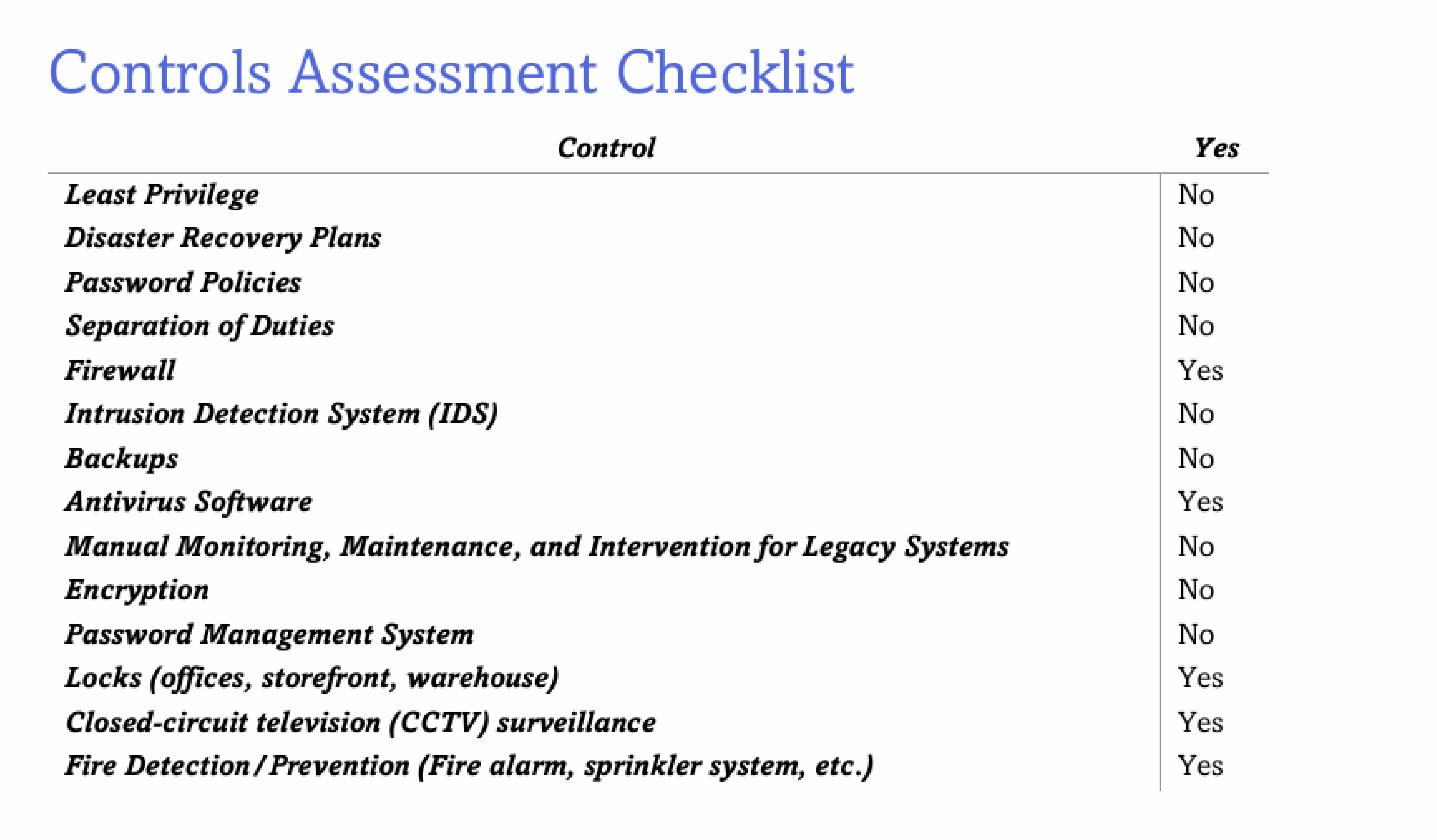
Technical Controls



Control Name	***Control Type***	***Control Purpose***	***Application to Botium Toys***
Firewall	Preventative	Filter unwanted or malicious traffic from entering the network	Implement a **next-generation firewall** to inspect traffic, block malicious connections, and enforce security rules. The firewall should be configured to block unauthorised access to internal systems from external sources.
IDS/IPS	Detective	Detect and prevent anomalous traffic that matches a signature or rule	Deploy an **Intrusion Detection System (IDS)** and **Intrusion Prevention System (IPS)** to monitor and protect the internal network from suspicious activity. This will help detect early signs of attacks like **DDoS** or **malware infections**.
Encryption	Deterrent	Provide confidentiality to sensitive information	Implement **end-to-end encryption (E2EE)** for customer payment information, both in transit and at rest, to comply with **PCI DSS**. This will ensure that sensitive customer data is protected from unauthorised access.
Backups	Corrective	Restore/recover from an event	Implement a **robust backup system** that regularly backs up critical data. Ensure backups are stored securely and are tested periodically to verify that they can be restored quickly in the event of a disaster or cyberattack.
Password Management	Preventative	Reduce password fatigue and improve security compliance	Implement a **centralised password management system** that enforces the password policy and simplifies password management for employees. This will help avoid password fatigue, reduce the risk of weak passwords, and prevent unauthorised access.
Antivirus (AV) Software	Corrective	Detect and quarantine known threats	Ensure that **antivirus software** is installed on all devices (desktops, laptops, and smartphones) and updated regularly to detect and quarantine known threats like viruses, malware, and ransomware.
Manual Monitoring	Preventative	Identify and manage risks or vulnerabilities in outdated systems	Implement a **schedule for monitoring** and **maintaining legacy systems** to ensure they are up to date with the latest security patches or replaced if needed. Legacy systems must be regularly audited for potential vulnerabilities.

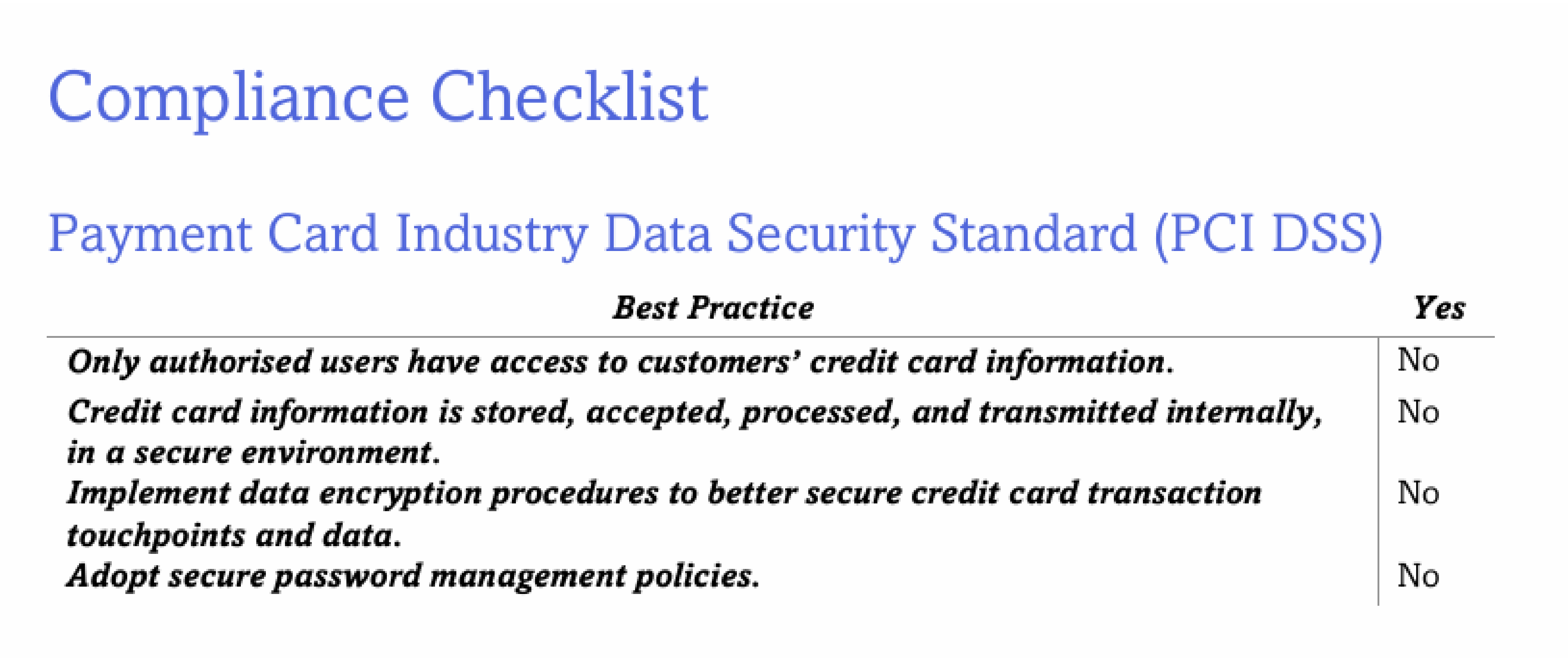
Physical/Operational Controls

Control Name	***Control Type***	***Control Purpose***	***Application to Botium Toys***
Time-controlled Safe	Deterrent	Reduce attack surface and impact from physical threats	Store sensitive items like customer payment information or inventory in a **time-controlled safe** to restrict access during off-hours or outside of authorised periods.
Adequate Lighting	Deterrent	Deter threats by limiting "hiding" places	Ensure **adequate lighting** around the **physical location**, especially in the parking lot and less visible areas, to reduce the likelihood of break-ins or theft.
CCTV (Closed-circuit television)	Preventative/ Detective	Reduce risk of incidents and detect suspicious activity	Install **CCTV cameras** in strategic areas (entrances, exits, sensitive locations) to monitor for security threats, deter criminal activity, and provide evidence for any potential investigations.
Locking Cabinets (Network Gear)	Preventative	Prevent unauthorised physical access to network gear	Use **locked cabinets** to store network hardware and servers to protect them from unauthorised access or tampering.
Locks	Deterrent/ Preventative	Prevent unauthorised physical access to assets	Ensure **locks** are installed on all entry points (doors, windows) to sensitive areas like server rooms, data storage rooms, and warehouse storage.
Fire Detection and Prevention	Detective/ Preventative	Detect fire and prevent damage to physical assets like inventory and servers	Maintain and regularly test **fire detection and prevention** systems (e.g., alarms, sprinklers) to safeguard physical assets, including inventory and sensitive data storage.



Controls Assessment Checklist

Control	***Yes***
Least Privilege	No
Disaster Recovery Plans	No
Password Policies	No
Separation of Duties	No
Firewall	Yes
Intrusion Detection System (IDS)	No
Backups	No
Antivirus Software	Yes
Manual Monitoring, Maintenance, and Intervention for Legacy Systems	No
Encryption	No
Password Management System	No
Locks (offices, storefront, warehouse)	Yes
Closed-circuit television (CCTV) surveillance	Yes
Fire Detection / Prevention (Fire alarm, sprinkler system, etc.)	Yes



Compliance Checklist

Payment Card Industry Data Security Standard (PCI DSS)

Best Practice	***Yes***
Only authorised users have access to customers' credit card information.	No
Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	No
Implement data encryption procedures to better secure credit card transaction touchpoints and data.	No
Adopt secure password management policies.	No

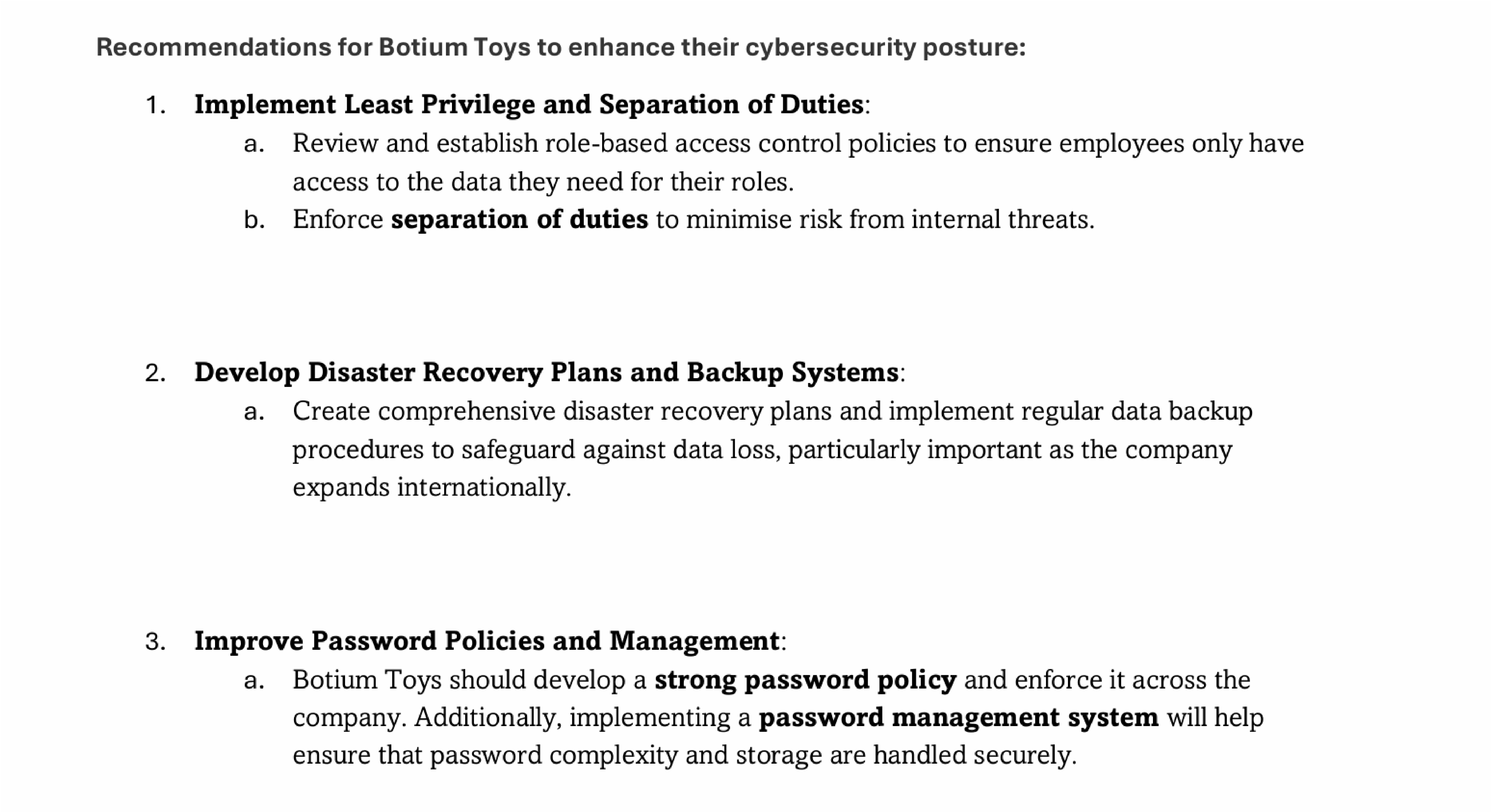
General Data Protection Regulation (GDPR)

Best Practice	***Yes***
E.U. customers' data is kept private/secured.	No
There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	Yes
Ensure data is properly classified and inventoried.	No
Enforce privacy policies, procedures, and processes to properly document and maintain data.	Yes

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

Best Practice	***Yes***
User access policies are established.	No
Sensitive data (PII/SPII) is confidential/private.	No
Data integrity ensures the data is consistent, complete, accurate, and has been validated.	No
Data is available to individuals authorised to access it.	Yes

Summary of Recommendations



Recommendations for Botium Toys to enhance their cybersecurity posture:

1. **Implement Least Privilege and Separation of Duties**:
    a. Review and establish role-based access control policies to ensure employees only have access to the data they need for their roles.
    b. Enforce **separation of duties** to minimise risk from internal threats.

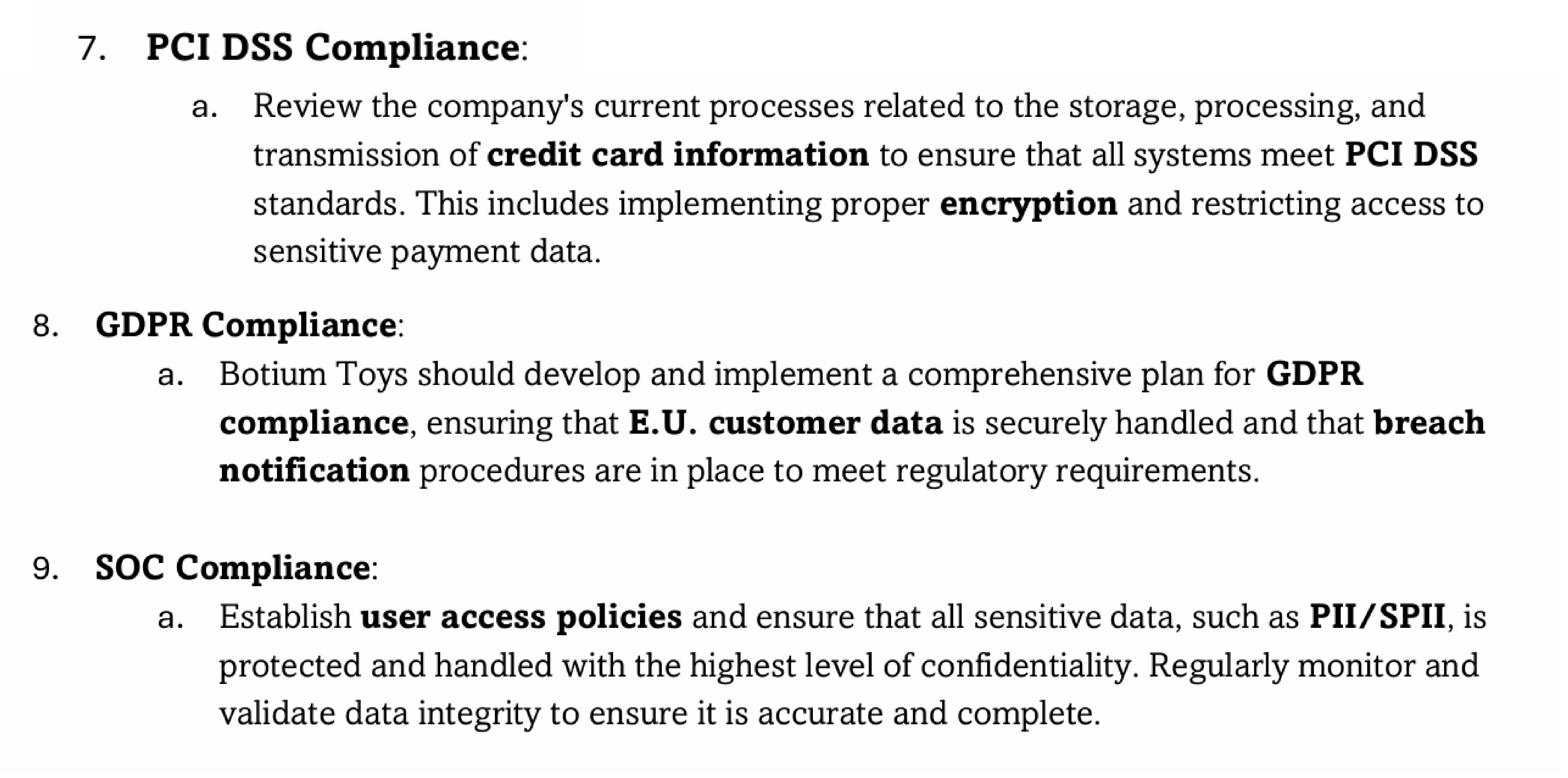
2. **Develop Disaster Recovery Plans and Backup Systems**:
    a. Create comprehensive disaster recovery plans and implement regular data backup procedures to safeguard against data loss, particularly important as the company expands internationally.

3. **Improve Password Policies and Management**:
    a. Botium Toys should develop a **strong password policy** and enforce it across the company. Additionally, implementing a **password management system** will help ensure that password complexity and storage are handled securely.

4. **Implement Encryption for Sensitive Data**:
    a. Encryption should be applied to all sensitive customer information, including credit card details and personally identifiable information (PII). This will help meet **PCI DSS** and **GDPR** requirements.

5. **Deploy Intrusion Detection and Prevention (IDS/IPS)**:
    a. Install an **IDS/IPS** system to detect and block suspicious or malicious network traffic, providing an additional layer of security for Botium Toys' IT infrastructure.

6. **Enhance Physical Security**:
    a. Ensure that all **physical locations**, including the office, storefront, and warehouse, have secure access controls, including **locks** and **CCTV** surveillance to prevent unauthorised access and safeguard physical assets.



7. **PCI DSS Compliance**:
   a. Review the company's current processes related to the storage, processing, and transmission of **credit card information** to ensure that all systems meet **PCI DSS** standards. This includes implementing proper **encryption** and restricting access to sensitive payment data.

8. **GDPR Compliance**:
   a. Botium Toys should develop and implement a comprehensive plan for **GDPR compliance**, ensuring that **E.U. customer data** is securely handled and that **breach notification** procedures are in place to meet regulatory requirements.

9. **SOC Compliance**:
   a. Establish **user access policies** and ensure that all sensitive data, such as **PII/SPII**, is protected and handled with the highest level of confidentiality. Regularly monitor and validate data integrity to ensure it is accurate and complete.