Controls and compliance checklist response

Directions: To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

You will conduct the audit:

To complete the checklist, open the supporting materials provided in Step 1. Then:

1. Review Botium Toys: Scope, goals, and risk assessment report, with a focus on:
    1. The assets currently managed by the IT department
    2. The bullet points under "Additional comments" in the Risk assessment section
2. Consider information provided in the report using the Controls Categories document.
3. Then, review the Controls and compliance checklist and select "yes" or "no" to answer the question in each section *(note: the recommendations section is optional)*.*

When completed, double check that you have completed the activity:

4. "Yes" or "no" is selected to answer the question related to each control listed
5. "Yes" or "no" is selected to answer the question related to each compliance best practice
6. A recommendation is provided for the IT manager *(optional)*
7. Note: This assignment is a self-assessment for your controls and compliance checklist. You will use these statements to review your own work. The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your security audit.

Now, for this table below, select "yes" or "no" to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control
	●	Least Privilege
	●	Disaster recovery plans
	●	Password policies

	●	Separation of duties
●		Firewall
	●	Intrusion detection system (IDS)
	●	Backups
●		Antivirus software
	●	Manual monitoring, maintenance, and intervention for legacy systems
	●	Encryption
	●	Password management system
●		Locks (offices, storefront, warehouse)
●		Closed-circuit television (CCTV) surveillance
●		Fire detection/prevention (fire alarm, sprinkler system, etc.)

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the controls, frameworks, and compliance reading.

Then, select "yes" or "no" to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
	●	Only authorized users have access to customers' credit card information.
	●	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	●	Implement data encryption procedures to better secure credit card transaction touchpoints and data.

	●	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

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

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

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

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Recommendations (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys’ security posture.

My Response/Recommendation:

Based on the scenario of Botium Toys related to the controls / compliance needs, these are my recommendations for my IT manager to communicate with stakeholders to reduce risks to assets and improve Botium Toy's security posture. So far, Botium Toy's needs to implement several key security controls to strengthen its defenses to protect sensitive information since it lacks critical controls such as Least Privilege, where employees have broad access to sensitive data, and Disaster Recovery Plans, leaving the company vulnerable to data loss and downtime.

Firstly, the reasons why there is a problem with least privilege is because all employees have access to sensitive data, including customer information like credit card details and personal addresses. This is this one of the cons of Botium Toy since it has no implementation of least privilege and if someone with malicious or criminal intent gains access to an employee's credentials it could damage the company. The company must implement least privilege and limiting access to only specific users.

Secondly, the reasons why there is a problem with disaster recover plans is that the company does not have it implemented yet, which is crucial for being prepared for events like cyberattacks, data loss, or system failures. This is significant as a disaster recovery plan ensures that critical systems and data can be restored quickly, minimizing downtime and financial loss. For instance, in a worst-case scenario, if a ransomware attack locks the company out of its files, having a recovery plan can help restore everything from backups.

Thirdly, the company's password policies are too weak, where there is a high risk of unauthorized access, and there is no Separation of Duties, which can lead to fraud if one person has admin rights (highest control) over important tasks. Based on the checklist, the fact that the company implements minimal password policy but does not meet the security standard to prevent crackability and unauthorized risk demonstrates where this should be improved as well. As for the separation of duties, the company has no separation of duties implemented which would impact the decision making and managing tasks to reduce risk of fraud and errors. So far, the scenario and checklist demonstrate that the CEO does both high-level decisions and managing sensitive financial tasks like payroll, which is dangerous because it means one person can access everything, increasing the likelihood for fraud or errors. It is essential that Botium Toy's implement separation so duties to ensures that no single person has full control over sensitive functions, such as payroll and financial management to resolve these issues.

Fourthly, Botium Toys doesn't have an Intrusion Detection System (IDS) to detect potential breaches, nor its legacy systems are maintained often, which is makes it lacking security and defenses from attacks. It is curial that the company implements these as based on the definition, an IDS detects and alerts on unusual or suspicious activity within a network which allows the company to identify and respond to potential intrusions before they can cause significant damage. Without an IDS, Botium Toys may be unaware of cyberattacks until they have been breached, or worse, been through the worst-case scenario.

Based on these, the company needs to improve its ongoing legacy system management, encryption, and password management system. So far, Botium Toys is still using some old software that works, but it's not getting checked or updated regularly. Without a proper maintenance plan, these systems could crash or get hacked. This is why the company should implement regular checking's would help make sure everything's safe and working properly. As for the encryption issue, this company has an issue with the customer credit card info is stored without encryption, which is risky and does not secure the data. Meanwhile the company lacks implementing proper Encryption so even if someone steals it, they won't be able to read it. If this company implements encryption, it can help the company keep sensitive info secure. Lastly, the company doesn't have a good password management system which is a problem as employees waste time asking IT to reset passwords, and weak or reused passwords make everything more vulnerable. This company should also implement a password manager to make sure the employees use stronger passwords and reduce the chance of security breaches from simple mistakes.

Due to all of this, it is necessary that Botium implements proper secure controls (security and privacy) to reduce the risk of cyberattacks, improve operational resilience, and ensure compliance with regulations like PCI DSS (for payment data security) and GDPR (for data privacy). Without these measures, Botium Toys remains exposed to serious security threats and the potential for financial penalties, data breaches, and reputational damage. Therefore, by implementing these recommendations, Botium Toys will be better protected from cyberattacks, data breaches, and compliance violations, which can be expensive both in terms of money and reputation.

References:

Botium Toys: Scope, goals, and risk assessment report (audit)

Scope: The scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.
Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys' security posture.
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

Risk assessment
Risk description
Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.
Control best practices
The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.
Risk score
On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices.
Additional comments
The potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

- 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 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.

Control categories:
Controls within cybersecurity are grouped into three main categories:

- Administrative/Managerial controls
- Technical controls
- Physical/Operational controls

Administrative/Managerial controls address the human component of cybersecurity. These controls include policies and procedures that define how an organization manages data and clearly defines employee responsibilities, including their role in protecting the organization. While administrative controls are typically policy based, the enforcement of those policies may require the use of technical or physical controls.

Technical controls consist of solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV) products, encryption, etc. Technical controls can be used in a number of ways to meet organizational goals and objectives.

Physical/Operational controls include door locks, cabinet locks, surveillance cameras, badge readers, etc. They are used to limit physical access to physical assets by unauthorized personnel.

Control types

Control types include, but are not limited to:

1. Preventative
2. Corrective
3. Detective
4. Deterrent

These controls work together to provide defense in depth and protect assets. **Preventative controls** are designed to prevent an incident from occurring in the first place. **Corrective controls** are used to restore an asset after an incident. **Detective controls** are implemented to determine whether an incident has occurred or is in progress. **Deterrent controls** are designed to discourage attacks.