Controls and compliance checklist

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.)

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.

Recommendations: 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.

Controls Assessment Recommendations:

- Currently, the principle of least privilege is not properly implemented, as is demonstrated by the fact that all employees can access cardholder data and customer PII/SPII. This can be remedied by reviewing employee access permissions and restricting access to information that is unnecessary for the performance of their day-to-day operations.
- The lack of disaster recovery plans and backups of critical data is also of concern. This analyst recommends several steps to mitigate loss of data in the event of disasters such as, but not limited to, power loss, natural disasters, fires, theft, etc..
    - First, implementation of an sufficiently capable uninterruptible power supply (UPS) would provide the IT staff with enough time to backup any critical data stored before the organization's computers and servers become inaccessible.
    - Next, it is recommended to configure the organization's data storage devices in a RAID configuration that implements mirroring or parity at the minimum (configurations such as RAID 1, RAID 5, or RAID 10 would accomplish this effect). This configuration ensures that in the event of hardware failure, there is a readily accessible backup of the data, and the faulty device can be swapped out for a functional one, the data copied back over to it, and allow for operations to resume uninterrupted.
    - Finally, this analyst recommends conducting incremental data backups to an off-site storage device or optionally to cloud storage, in order to minimize the

potential negative impact of a natural disaster, fire, theft, or other scenario that results in the loss of hardware. The nature of incremental backups will require a somewhat significant time investment to create the initial full backup of relevant data, however subsequent backups will not require the same amount of time, as they will only backup data that has been added since the previous update. To ensure a properly updated backup of important data, the frequency of the given backups will be important. This analyst believes this decision can be made when considering the overall volume of business conducted within a given timeframe, and this is not a decision that can accurately be made in this audit, by this analyst.

- While password policies are currently in place, it is the belief of this analyst that they are not sufficient to properly prevent attacks from threat actors targeting password authentication. In order to properly ensure password security, this analyst recommends updating the password policy to require at least 12 characters, at least one of which is capitalized, at least one of which is a special character, and at least one of which is a number. Relatedly, password management software is not currently implemented, and if properly implemented would allow a reduction in the overall workload of the IT department, reduce delays employees who need to recover their passwords experience, and, depending on the management software chosen, can suggest strong passwords meeting the provided suggested criteria. Additionally, this analyst believes that more stringent account management policies would prove beneficial to improving overall security posture by creating account lifecycle regulations such as password expiration that would require passwords to be updated regularly, limiting the impact a threat actor with access to a given password could have.
- As stated in the additional comments section of the risk assessment report, separation of duties policies are not implemented effectively. These policies would serve to limit the impact a hypothetical malicious insider threat actor or otherwise compromised account could have, as they would only have access to so many given permissions.
- It is recommended to implement robust intrusion detection/prevention software (IDS/IPS) to act as a second line of defense in tandem with the existing network firewall. This type of software would serve to analyze activity on the internal company network and alert the security team to any activity flagged as relevant by the security team. Such alerts could include unrecognized devices on the network, concerning network traffic, and other concerning activity.

- Regarding legacy systems, it is recommended to create a scheduling outlining when maintenance should occur. Additionally, ensuring all analysts tasked with working with the legacy systems should be given proper training regarding intervention in the event of an incident relating to these legacy systems.
- As outlined in the risk assessment document, encryption is not currently implemented to ensure the confidentiality of cardholder and customer information. Relevant encryption methods should be implemented as soon as possible to ensure that unauthorized access to this data would provide as little benefit to the threat actor as possible.
- While the physical controls implemented at the organization's locations are currently robust (locks, CCTV, and fire prevention systems) as the business continues to grow implementation of additional physical controls such as alarm systems, security guards at locations such as the warehouse at least, ensuring adequate exterior lighting, and time-controlled safes could become relevant.

Payment Card Industry Data Security Standard (PCI DSS):

- The concerns pertaining to cardholder and payment data confidentiality can be largely remedied through the broad application of previously recommended methods. Currently, all employees at the organization have access to this type of data, which implementation of least privilege would remedy. The concern regarding the proper storage, transmission, and accessibility of cardholder data can be solved via the previously mentioned implementation of least privilege policies for internal accounts and data encryption to ensure the confidentiality of the data. The implementation of more robust password policies, such as password requirements, expirations, etc., also factor into ensuring that only authorized individuals have access to cardholder data, and limits the attack surface area available to threat actors seeking to access this information.

General Data Protection Regulation (GDPR):

- Currently, the organization does not fully comply with the regulations set forth by the GDPR. In order to meet the regulatory requirements of this act, the organization will need to ensure that only authorized individuals have access to customer's PII/SPII. The implementation of least privilege policies will serve to solve this problem, along with reducing attack surface area pertaining to authentication methods such as passwords. Most other regulations set forth by the GDPR are currently met by the organization, such

as notification to customers within 72 hours of a data breach and proper inventory, documentation, and classification of customer data.

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

- While the data collected by the organization is ensured to be available and controls are in place to ensure data integrity, currently the fact that any employee can access this data, along with any threat actor who manages to obtain an account password, presents the largest vulnerability. Implementing least privilege policies and more robust password and account lifetime policies will be very effective at remedying this issue.