# Controls and compliance checklist

Based on the audit findings described in the attached PDF file entitled: "Controls and compliance checklist", it is recommended that Botium Toys:

* Establish a strong password policy that aligns with current minimum password complexity requirements.
* Implement a password management system to enforce password policies and reduce the productivity impact.
* Consider the implementation of a disaster recovery plan to ensure business continuity in the event of an incident.
* Explore the use of encryption to enhance data security, particularly for customers’ credit card information.
* Prioritize the implementation of least privilege and separation of duties controls.
* Initiate a plan for intrusion detection system (IDS) installation and monitoring.
* Develop and document regular maintenance and monitoring schedules for legacy systems.
* Evaluate and adopt data encryption procedures and secure password management policies to comply with PCI DSS requirements.
* Establish processes for classifying and inventorying data to align with GDPR guidelines.
* Enforce privacy policies, procedures, and processes to ensure data is properly documented and maintained.
* Consider the adoption of System and Organizations Controls (SOC) best practices to enhance user access policies, data confidentiality, data integrity, and authorized data access.

These recommendations will contribute to a stronger security posture and ensure compliance with regulatory requirements, reducing risks to the organization's assets and critical data.