Recommendation

Botium Toys must enforce various measures to enhance its security and safeguard sensitive data. These measures include adopting the principle of Least Privilege, formulating disaster recovery plans, implementing stringent password policies, ensuring separation of duties, deploying an Intrusion Detection System (IDS), managing legacy systems continuously, employing robust encryption, and establishing a comprehensive password management system.

To bridge compliance gaps, Botium Toys should prioritize the implementation of controls like Least Privilege, separation of duties, and encryption. It is also crucial for the company to accurately classify its assets, enabling the identification of additional controls necessary to fortify its security protocols and shield sensitive information.

. Implement controls to enforce least privilege and separation of duties.

. Introduce encryption for confidential data, especially credit card information.

. Install an intrusion detection system (IDS) for proactive threat detection.

. Develop and implement disaster recovery plans with regular backups.

. Enhance the password policy to meet current complexity requirements.

. Implement a centralized password management system.

. Establish a regular schedule for monitoring and maintaining legacy systems.  
  
Botium Toys faces significant cybersecurity risks stemming from inadequate controls and non-compliance. Immediate action is recommended to enhance the organization's security posture, protecting sensitive data and ensuring business continuity.