Risk Assessment Summary

Risk description

- Inadequate management of assets
- Not all proper controls are in place
- May not be fully compliant with U.S. and international regulations and standards

Control best practices

- Identify assets to properly manage them
- Classify existing assets
- Determine the impact of loss of assets (incl. systems) on business continuity

Risk score

- Risk score is 8/10
- Due to lack of controls and adherence to compliance best practices

Additional comments

- Potential impact from loss of an asset is medium
- Risk to asset is high
- Fines from governing bodies is high
- IT dept. does not know which assets are/would be at risk

Items that are in compliance

- IT dept. has ensured availability and integrated controls to ensure data integrity
- IT dept. has a firewall that blocks traffic based on appropriately defined set of security rules
- IT dept. has installed antivirus software that is monitored regularly
- IT dept. has a plan in place to notify E.U. customers within 72 hours of a security breach

- Privacy policies, procedures, and processes have been developed and are enforced to properly document and maintain data
- Store’s physical location has sufficient locks, CCTV surveillance, as well as functioning fire detection and prevention systems
- Legacy systems are monitored and maintained

Items not in compliance

- All Botium Toys employees have access to internally stored data, cardholder data, and customer’s PII/SPII
- Encryption is not currently used to ensure confidentiality of customer’s credit card information that is stored locally in the company’s internal database
- Access controls pertaining to least privilege and separation of duties have not been implemented
- IT dept. lacks and intrusion detection system (IDS)
- No disaster recovery plans in place
- No backups of critical data is present
- Password policy requirements are nominal and not in line with current minimum password complexity requirements
- No centralized password management system in place
- There is no schedule for legacy systems monitoring and intervention methods are unclear