<u>Review and Audit on the IT's manager scope, goals and assessment report on botium toys</u>

Ententire security program at Botium Toys

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.
Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements
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.

Assets managed by the IT Department include: On-premises equipment for in-office business needs
Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse
Internet access
Internal network
Data retention and storage
Legacy system maintenance: end-of-life systems that require human monitoring

Risk assessment

The risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices. 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.

Controls Assessment Checklist

There is no least privilege- privileges need to be limited to reduce the risk of a breach.

No Disaster recovery plans to ensure business continuity

No encryption- no *greater confidentiality of sensitive information.*

CCTV is installed/functioning at the store's physical location.

Botium Toys' physical location has a functioning fire detection and prevention

There is no compliance checklist

In terms of General Data Protection Regulation, there is a plan in place to notify E.U. customers within 72 hours if their data is compromised or breach

In terms of System and Organizations Controls (SOC type 1, SOC type 2), the practice of Data integrity to ensure that data is consistent, complete, accurate, and has been validated is in pace. There is no establishment of User access policies, Sensitive data (PII/SPII) is not confidential/private