SCENARIO:

This scenario is based on a fictional company.

OBJECTIVE:

Your task is to review the IT manager's scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

SCOPE AND GOALS:

The scope will focus on the (physical and digital) security infrastructure of Botium Toys, and the objectives will be to revise the security policies and suggest new ones if necessary.

RISK ASSESSMENT:

The physical security structure meets the requirements, as physical controls, such as locks, where only authorized persons have access to the keys, closed-circuit television (CCTV) and fire prevention help mitigate potential risks. On the part of technical controls, the firewall is well configured and the antivirus and software used in the store are always up to date, but they present many security flaws in administrative controls and some technical controls.

RECOMMENDATIONS:

Taking into consideration the objectives of the manager of Botium Toys for conducting business with the U.S., the company needs to comply with the GDPR and to ensure the security of its customers' data with PCI DSS.

Administrative Controls that need to be implemented: Least Privilege, Disaster recovery plans, Password policies, Access control policies and Separation of duties.

Technical Controls that need to be implemented: IDS/IPS, Encryption, Backups, Password management and Manual monitoring, maintenance, and intervention.