Botium Toys Scope Goals and Risk Assessment

Botium Toys: Scope, goals, and risk assessment report
Scope and goals of the audit
Scope: The scope is defined as the entire security program at Botium Toys. This means all assets need to be a
Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls
Current assets
Assets managed by the IT Department include:
On-premises equipment for in-office business needs
Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cable
Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse
Management of systems, software, and services: accounting, telecommunication, database, security, ecommer
Internet access
Internal network
Data retention and storage
Legacy system maintenance: end-of-life systems that require human monitoring
Risk assessment
Risk description
Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper
Control best practices
The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to id
Risk score
On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adhere
Additional comments
The potential impact from the loss of an asset is rated as medium, because the IT department does not know w
Currently, all Botium Toys employees have access to internally stored data and may be able to access cardhold
Encryption is not currently used to ensure confidentiality of customers' credit card information that is accep
Access controls pertaining to least privilege and separation of duties have not been implemented.
The IT department has ensured availability and integrated controls to ensure data integrity.
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.
The IT department has not installed an intrusion detection system (IDS).
There are no disaster recovery plans currently in place, and the company does not have backups of critical dat
The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breac
Although a password policy exists, its requirements are nominal and not in line with current minimum password
There is no centralized password management system that enforces the password policy's minimum requireme
While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and i
The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of product