Security Audit

Introduction

This presentation covers three key aspects of the project: the scenario, the notes used, and the final result. The scenario outlines the project goals, the notes provide guidance, and the final project demonstrates how these elements were applied.

Scenario:

Scenario

Review the following scenario. Then complete the step-by-step instructions.

This scenario is based on a fictional company:

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy's online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. She believes an internal audit can help better secure the company's infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

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.

Notes:

Botium Toys: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope: The scope is de ned as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys' security posture.

Current assets

Assets managed by the IT Department include:

- On-premises equipment for in-o ce business needs Employee equipment: end-user devices (desktops/laptops, smartphones),
- remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc. Storefront products available for retail sale on site and online; stored in the
- company's adjoining warehouse
  Management of systems, so ware, and services: accounting,
- telecommunication, database, security, ecommerce, and inventory management 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 controls in place and may not be fully compliant with U.S. and international regulations and standards.

Control best practices

The rst of the ve functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

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 adherence to compliance best practices.

Additional comments

The potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be at risk. The risk to assets or nes 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. Review the following bullet points for speci c details:

- Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
- Encryption is not currently used to ensure con dentiality of customers' credit card information that is accepted, processed, transmi ed, and stored locally in the company's internal database.
- 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 rewall that blocks tra c based on an appropriately de ned set of security rules.
- Antivirus so ware 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 data.
- The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
- Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of le ers and at least one number; special characters).
- There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes a ects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
- While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
- The store's physical location, which includes Botium Toys' main o ces, store front, and warehouse of products, has su cient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning re detection and prevention systems.

Control categories

Control categories

Controls within cybersecurity are grouped into three main categories:

- Administrative/Managerial controls
- Technical controls
- Physical/Operational controls

Administrative/Managerial controls address the human component of cybersecurity. These controls include policies and procedures that de ne how an organization manages data and clearly de nes employee responsibilities, including their role in protecting the organization. While administrative controls are typically policy based, the enforcement of those policies may require the use of technical or physical controls.

Technical controls consist of solutions such as rewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV) products, encryption, etc. Technical controls can be used in a number of ways to meet organizational goals and objectives.

Physical/Operational controls include door locks, cabinet locks, surveillance cameras, badge readers, etc. They are used to limit physical access to physical assets by unauthorized personnel.

Control types

Control types include, but are not limited to:

1. Preventative
2. Corrective
3. Detective
4. Deterrent

These controls work together to provide defense in depth and protect assets. **Preventative controls** are designed to prevent an incident from occurring in the rst place. **Corrective controls** are used to restore an asset a er an incident. **Detective controls** are implemented to determine whether an incident has occurred or is in progress. **Deterrent controls** are designed to discourage a acks.

Review the following charts for speci c details about each type of control and its purpose.

Administrative/Managerial Controls		
Control Name	**ControlType**	**ControlPurpose**
Least Privilege	Preventative	Reduceriskandoverall impact of malicious insider or compromised accounts
Disaster recovery plans	Corrective	Providebusiness continuity
Password policies	Preventative	Reducelikelihoodof account compromise through brute force or dictionary a ack techniques
Access control policies	Preventative	Bolstercon dentialityand integrity by de ning which groups can access or modify data
Account management policies	Preventative	Managingaccount lifecycle, reducing a ack surface, and limiting overall impact from disgruntled former employees and default account usage
Separation of duties	Preventative	Reduceriskandoverall impact of malicious insider or compromised accounts

Technical Controls		
Control Name	**Control Type**	**Control Purpose**
Firewall	Preventative	To lter unwanted or malicious tra c from entering the network
IDS/IPS	Detective	To detect and prevent anomalous tra c that matches a signature or rule
Encryption	Deterrent	Provide con dentiality to sensitive information
Backups	Corrective	Restore/recover from an event
Password management	Preventative	Reduce password fatigue
Antivirus (AV) so ware	Corrective	Detect and quarantine known threats
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Physical/Operational Controls		
Control Name	**ControlType**	**ControlPurpose**
Time-controlled safe	Deterrent	Reducea acksurfaceand overall impact from physical threats

Adequate lighting	Deterrent	Deter threats by limiting “hiding” places
Closed-circuit television (CCTV)	Preventative/Detective	Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used a er an event to inform on event conditions
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful a ack seem low
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets
Fire detection and prevention (re alarm, sprinkler system, etc.)	Detective/Preventative	Detect re in physical location and prevent damage to physical assets such as inventory, servers, etc.

Final Project:

Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, ~~including the type and purpose, refer to~~ the control categories document.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☐	☑	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus so ware
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☑	☐	Locks (o ces, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance

☑	☐	Fire detection/prevention (re alarm, sprinkler system, etc.)

To complete the compliance checklist, refer to the information provided in the ~~scope, goals, and risk assessment report~~. For more details about each compliance regulation, review the ~~controls, frameworks, and compliance~~ reading.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Compliance checklist

~~Payment Card Industry Data Security Standard (PCI DSS)~~

Yes	No	Best practice
☐	☑	Only authorized users have access to customers’ credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmi ed internally, in a secure environment.
☐	☑	Implement data encryption procedures to be er secure credit card transaction touchpoints and data.
☐	☑	Adopt secure password management policies.

~~General Data Protection Regulation (GDPR)~~

Yes	No	Best practice
☐	☑	E.U. customers’ data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classi ed and inventoried.

☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

~~System and Organizations Controls (SOC type 1, SOC type 2)~~

Yes	No	Best practice
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is con dential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☐	☑	Data is available to individuals authorized to access it.

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Recommendations (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.