Audit Scope and Goals

Summary: I was tasked as part of my ongoing curriculum within the Google Cybersecurity Certificate course to conduct a security audit of a fictional company (Botium Toys). I was initially provided with a Scope, goals, and risk assessment for Botium Toys (See appendix 1) and then asked to complete a controls and compliance checklist. I completed the controls and compliance checklist, and my findings are listed below along with a summary of appendix 1 and a list of recommendations.

Scope: The scope is defined 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.

Risk Assessment

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, 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, software, 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 description:
Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.

Control best practices:
The first of the five 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 1-10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to necessary compliance regulations and standards.

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 fines from governing bodies is high because Botium Toys does not have all 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 specific details:

Controls Assessment:

Administrative Controls			
Control name	**Control type and explanation**	**Needs to be implemented? (X)**	**Priority**
Password policies	Preventative: 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 letters and at least one number; special characters).	X	**High**
Password management system	Preventative: There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password	X	**High**
Least Privilege	Preventative: Access controls pertaining to least privilege and separation of duties have not been implemented.	X	**High**
Disaster recovery plans	Corrective: There are no disaster recovery plans currently in place, and the company does not have backups of critical data	X	**High**

Administrative Controls			
Separation of duties	Preventative: Access controls pertaining to least privilege and separation of duties have not been implemented."	X	High

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented? (X)**	**Priority**
Intrusion Detection System (IDS)	Detective: The IT department has not installed an intrusion detection system (IDS)."	X	High
Encryption	Deterrent: Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database."	X	Medium
Firewall	Preventative: The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules		Low
Backups	Corrective: The company does not have backups of critical data."	X	High
Antivirus Software	Detective: Antivirus software is installed and monitored regularly by the IT department		Low
Manual monitoring, maintenance, and intervention for legacy systems	Preventative: While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear	X	Medium

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Closed-circuit television (CCTV) surveillance	Preventative/detective: Has up-to-date closed-circuit television (CCTV) surveillance		Low
Locks	Preventative: The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks		Low
Fire detection/prevention (fire alarm, sprinkler system, etc.)	Preventative/Corrective: The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has... functioning fire detection and prevention systems		Low

General Data Protection Regulation (GDPR)

GDPR is a European Union (EU) general data regulation that protects the processing of EU citizens' data and their right to privacy in and out of EU territory. Additionally, if a breach occurs and an EU citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation: The organization needs to adhere to GDPR because we conduct business and collect personal information from people in the EU.

General Data Protection Regulation (GDPR) Controls			
Control Name	**Control type and explanation**	**Needs to be implemented? (X)**	**Priority**
E.U. customers' data is kept private/secured	Deterrent: Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII	X	Medium
There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	Corrective: The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach."		Low
Ensure data is properly classified and inventoried.	Preventative: Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.		Low

Enforce privacy policies, procedures, and processes to properly document and maintain data.	Preventative: Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.		Low

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation: The organization needs to adhere to PCI DSS because we store, accept, process, and transmit credit card information in person and online.

Payment Card Industry Data Security Standard (PCI DSS) Controls			
Control Name	**Control type and explanation**	**Needs to be implemented? (X)**	**Priority**
Only authorized users have access to customers' credit card information.	Preventative: Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII."	X	High
Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Deterrent: Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database	X	High
Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Deterrent: Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.	X	High
Adopt secure password management policies.	Preventative: 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 letters and at least one number; special characters)	X	High

Recommendations for Risk Mitigation and Security Improvement

1. Restrict Access to Sensitive Data
Issue: All employees have access to internally stored data, including cardholder data and PII/SPII.
Recommendation: Implement Role-Based Access Control (RBAC) to limit data access based on job responsibilities. This ensures that employees only access the information necessary for their roles, thereby reducing the risk of unauthorized data exposure.

2. Implement Data Encryption
Issue: No encryption is used for customers' credit card information.
Recommendation: Adopt strong encryption protocols (e.g., AES-256) for all data at rest and in transit to protect sensitive information from unauthorized access and ensure confidentiality.

3. Enforce Least Privilege and Separation of Duties
Issue: Lack of least privilege and separation of duties in access controls.
Recommendation: Develop and enforce policies that restrict user access to the minimum necessary to perform their job functions. Additionally, separate critical duties among different employees to prevent conflicts of interest and reduce the risk of fraud.

4. Deploy an Intrusion Detection System (IDS)
Issue: No IDS is installed.
Recommendation: Install and regularly monitor an IDS to detect and respond to suspicious activities on the network. This will help identify potential breaches and mitigate threats before they cause significant damage.

5. Develop and Implement Disaster Recovery Plans
Issue: No disaster recovery plans or data backups.
Recommendation: Create a comprehensive disaster recovery plan that includes regular backups of critical data. Store backups in multiple secure locations, and conduct periodic tests to ensure recovery procedures are effective and data integrity is maintained.

6. Strengthen Password Policies and Management
Issue: Current password policy lacks complexity and there is no centralized management.
Recommendation: Update the password policy to require longer, more complex passwords (e.g., at least 12 characters, including uppercase, lowercase, numbers, and special characters). Implement a centralized password management system to enforce these policies and streamline password resets, reducing the burden on IT staff and improving security.

7. Regularly Schedule Legacy System Maintenance
Issue: No regular schedule for monitoring and maintaining legacy systems.
Recommendation: Establish a routine maintenance schedule for legacy systems, including regular updates and security patches. Define clear intervention methods to ensure these systems remain secure and functional.

8. Improve Physical Security Measures
Issue: Physical security measures are in place but should be continuously evaluated.
Recommendation: Regularly review and update physical security protocols, ensuring that all access points are secure, and that surveillance and fire prevention systems are tested and maintained. Consider conducting security audits to identify and address potential vulnerabilities.

9. Enhance Employee Training and Awareness
Issue: General awareness and adherence to security practices.
Recommendation: Conduct regular training sessions for employees on data protection, privacy policies, and security best practices. Promote a culture of security awareness to ensure all employees understand their roles in protecting company assets.

10. Ensure Compliance with Regulatory Standards
Issue: Compliance with data protection regulations.
Recommendation: Continuously review and update policies to comply with relevant regulations such as GDPR, PCI-DSS, and others. Conduct periodic audits to ensure adherence and address any gaps in compliance.

By implementing these recommendations, Botium Toys can significantly reduce risks to its assets and improve its overall security posture, ensuring the protection of sensitive customer information and maintaining business continuity.