Below is an example of my ability to participate in a security audit by completing the control and compliance assessment for a fictional company, Botium Toys. Everything above the control and compliance assessment was developed by my certification program as a sample for students to evaluate.

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 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-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 of 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 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 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. Review the following bullet points for specific 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 confidentiality of customers' credit card information that is accepted, processed, transmitted, 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 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 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 letters and at least one number; special characters).
- 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.
- 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 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.

Control and Compliance Assessment

Controls Checklist

Select "yes" or "no" to answer the question: *Does Botium Toys currently have this control in place?*

Yes	No	Control	Comments
	X	Least Privilege	Privileges to data must be limited to authorized users
	X	Disaster recovery plans	
	X	Password policies	Poor passwords are not to framework standards
	X	Separation of duties	Duties need to be defined, perhaps dedicated security professional would solve
X		Firewall	
	X	Intrusion detection system (IDS)	
	X	Backups	
X		Antivirus software	
	X	Manual monitoring, maintenance, and intervention for legacy systems	Must be scheduled and regular
	X	Encryption	
	X	Password management system	Automated password recovery would increase IT productivity
X		Locks (offices, storefront, warehouse)	

X		Closed-circuit television (CCTV) surveillance
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

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

Payment Card Industry Data Security Standard (PCI DSS)

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

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	X	E.U. customers’ data is kept private/secured.
X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
	X	Ensure data is properly classified and inventoried.
X		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
	X	User access policies are established.
	X	Sensitive data (PII/SPII) is confidential/private.
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
	X	Data is available to individuals authorized to access it.

Additional Comments

All PII/SPII and any other sensitive business information must be encrypted and only readily accessible to authorized users. While there is a user system in place, it needs updating to NIST CSF standards for password complexity. Legacy systems lacking any kind of scheduled maintenance or monitoring, no disaster plan, and no backups of any systems endanger stolen or lost data, thus loss of business, especially when working with legacy systems- importing all data from legacy and modern systems to an encrypted cloud service would solve this and allow legacy systems to properly phase out of business operations. It is important for Botium Toys to consider having a dedicated security position who can consistently monitor and enforce NIST guidelines, and utilize an intrusion detection system along with any other SIEM tools, if they plan on expanding business further.