Proposed Scenario:

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location. However, its online presence has grown, attracting customers in the U.S. and abroad. 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 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, and completing a risk assessment. The goal of the audit is to provide an overview of the risks the company might experience due to the current state of their security posture. The IT manager wants to use the audit findings as evidence to obtain approval to expand his department.

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

Botium Toys: Audit Scope and Goals
Botium Toys: Risk Assessment

Internal Audit:

Summary

The biggest risk that Botium Toys has to the organization is the inadequate management of assets. This company does not have the proper controls in place to manage their various assets such as employee equipment and proper permissions for management of systems, software, and databases. This lack of asset management also puts Botium Toys in risk of non-compliance with various US and internationa/l regulations and guidelines. This is the main reason in which Botium Toys received a risk score of 8/10 when it comes to their internal security controls. They do not have the necessary concept of least permission that would allow them for adequate protection of their data.

Due to this, I suggest that Botium Toys adhere to the NIST CSF framework in order to realign their security controls in compliance with US and international regulations and standards. This will ensure that they are able to protect their organizations data, as well as

identify and manage the security risks that they currently suffer from.

Control Assessment:

Administrative Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Least Privilege	Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs	x	High
Disaster recovery plans	Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration	x	High
Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	x	High
Access control policies	Preventative; increase confidentiality and integrity of data	x	High

Administrative Controls			
Account management policies	Preventative; reduce attack surface and limit overall impact from disgruntled/former employees	x	Medium
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain	x	High

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Firewall	Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network	N/A	N/A
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	x	High
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	x	High
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	x	High
Password management	Corrective; password recovery, reset, lock out notifications	x	Medium

system			
Antivirus (AV) software	Corrective; detect and quarantine known threats	x	Medium
Manual monitoring, maintenance, and intervention	Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities	x	High

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats		Low
Adequate lighting	Deterrent; limit “hiding” places to deter threats	x	Low
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	x	Medium
Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	x	Medium
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	x	Low

Locks	Preventative; physical and digital assets are more secure	Already Implemented	High
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; detect fire in the toy store's physical location to prevent damage to inventory, servers, etc.	x	low

Compliance Checklist:

☐ **General Data Protection Regulation (GDPR)**

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

Explanation: Botium Toys does not currently protect users data in a satisfactory way, and is starting to gain some customers from the E.U. They need to adhere in the future to do worldwide business

☐ **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: No, Botium Toys does not currently have the proper security measures in place to protect credit card data during transactions, such as encryption. They also currently have many legacy systems in place that does not fit current standards.

☑ **The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a federal law established in 1996 to protect U.S. patients' health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

Explanation: N/A

☐ **System and Organizations Controls (SOC type 1, SOC type 2)**

The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Explanation: This organization has not performed any SOC audits, as they are currently trying to build up an IT department big enough to focus on my cyber policy.

Stakeholder Recommendations:

It is recommended that Botium Toys upgrades online security protocols for multiple reasons. The first being to comply with various national and international rules and regulations to ensure compliance that will not lead to a fine, or lead to a loss in user data. In order to do this, the IT department will focus on adhering to the NIST CST framework to ensure proper handling of PII and company assets. In addition to this, focus will be placed on complying with the PCI DSS to ensure the secure handling of customer credit card information, and to ensure compliance to avoid security breaches and fines. Integration of IDS and anti-virus software will also be installed to the system to protect our devices and servers, along with secure encryption to ensure the security and integrity of our data. Furthermore, physical security will be implemented at our physical location. This will include CCTV cameras along with state of the art locks to help protect theft of our assets.