Controls assessment

Administrative Controls				
Control name	**Control type and explanation**	**Needs to be implemented (X)**	**Needs to be corrected**	**Priority**
Password policies	Preventative: establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques		X	High
Disaster recovery plans	Corrective: Provides business continuity, by having plan of action in case of event	X		High
Least privilege	Preventative: Providing the least amount of access required to perform everyday tasks, reducing the potential damage of a breach.	X		High
Access Control Policies	Preventative: Managing account lifecycle, reduces attack surface, limits overall impact from distinguished former employees and default account usage.	X		High
Separation of duties	Preventative; Reducing the risk of overall impact of malicious insider or compromised accounts.	X		Medium

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Intrusion detection systems (IDS)	Detective; To detect and prevent anomalous traffic that matches a signature or rule.	X	High
Backups	Corrective; Helps restoring the systems and data after even	X	High
Password management	Preventative; Reduce password fatigue, improve security, reduce breaches	X	High
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (i.e., anomalous traffic) quickly	X	High
Encryption	Deterrent; makes confidential information/data more secure (i.e., website payment transactions)	X	High/ Medium

Risk description

Currently, there is inadequate management of assets. Poor password control and access control. The lack of encryption and partially implemented controls raises the risk of threat actors. Additionally, proper controls are not in place and the organization is not compliant with U.S. and international compliance 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.
The organization will need to dedicate resources to managing assets. Additionally, they will need to 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 control and adherence to necessary compliance regulations and standards and multiple .

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 are 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. Some practices and controls are not fully implemented, which causes risk of threats and possible fines.

Recommendations

The password policies should be updated, and stronger passwords should be implemented. MFI should be implemented for users. Creating an employee hierarchy with least privilege control is crucial for users' safety, and safe work process. Creating backups and disaster recovery plans is crucial for recovering after an event. A schedule for the legacy systems, and plan of action should be created in case of event.