Security Audit of Botium Toys

Biggest Risks to Organisation:

- Inadequate management of assets within the organisation
- Proper controls are currently not in place
- Botium Toys may not be compliant with U.S. and international regulations and guidelines which could lead to penalties if a breach occurs
- Current risk score after assessing is 8/10, due to the lack of controls and adherence to compliance regulations and standards

Due to the high risk rating after conducting a risk assessment of Botium Toys' current security posture, it is of utmost importance that proper controls are put in place and that Botium Toys are compliant with regulatory standards to improve the security posture of the organisation and to avoid any penalties if attacks are successful.

Essential Controls to be implemented immediately

- Dedicate resources to management of assets
- Determine the impact of the loss of existing assets and determine which assets would be lost
- Implement the concept of least permissions when it comes to user credential management
- Firewall, IDS, backups, encryption etc. More of this is covered in the controls assessment.

Botium Toys need to ensure that they are compliant with regulatory standards that are in place to ensure that the data of customers and vendors is protected, and by following regulations this can help improve the organisation's security posture and can avoid the organisation from experiencing data breaches which could potentially lead to fines / legal action. By following the NIST CSF framework and its controls and best practices mentioned, this can help Botium Toys are aligned with regulatory standards expected for an organisation's security posture. Botium Toys need to ensure that they are compliant with the PCI DSS as they sell products online, and that they follow the GDPR as they may sell products to European customers.

Analysis of Audit Results

Scope: To perform an audit of all assets within the organisation alongside the internal processes and procedures, and determine what needs to be improved.
Goals: To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

- Establish a better process for their systems to ensure they are compliant
- Fortify system controls

- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

All controls are to be implemented immediately. Controls assessment provides the exact controls that are to be implemented to improve security posture. Botium Toys need to ensure that they are compliant with the GDPR, PCI DSS, and System and Organizations Controls.