

Botium Toys: Audit

Analyze the audit scope, goals, and risk assessment

What are the biggest risks to the organization?

The two biggest risks are that Botium Toys does not know which assets would be lost in a potential breach and that the organization is not fully compliant with regulations regarding protecting customer data.

Which controls are most essential to implement immediately versus in the future?

The most essential controls to implement immediately are the controls required to be compliant with U.S. regulations. Other controls to implement immediately would be related to business continuity such as having data backup systems in place and ensuring that internal applications have secure default states. Improving network controls will also be necessary to focus on as more global customers begin to use the service. Overall, admin and technology controls are likely the types of controls to focus on immediately.

Future controls to implement depend on how quickly Botium Toys wants to enter the E.U. markets. Becoming compliant with E.U. regulations could be held off until the organization is ready, otherwise these controls would also need to be implemented immediately. Sufficient physical controls such as badge readers and surveillance cameras are already in place, according to the risk assessment, so these can likely be improved on in the future.

Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?

- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Information Security Modernization Act (FISMA)
- General Data Protection Regulation (GDPR for E.U.)