

**Recommendations (mitigation plan):**

The internal audit aims to align Botium Toys' current business practices with industry standards and best practices set by the NIST and CSF. Its purpose is to offer mitigation recommendations for vulnerabilities identified as "high risk" and to develop an overall strategy to enhance the organization's security posture. The audit team has documented their findings, these are the remediation plans and efforts, to be communicated effectively with stakeholders.

**Risk description:**

Currently, there is not adequate management of assets. Additionally, proper controls are not in place and the organization may not be compliant with U.S. and international compliance regulations and standards. The organization will need to dedicate resources to managing assets.

**Additional comments:**

The likelihood of a lost asset or fines from governing bodies is high because the organization does not have all of the necessary controls in place and is not adhering to required regulations and standards related to keeping PII data private.

**Admin Controls:**

Password policies, Preventative; establish password strength rules to improve security/reduce the likelihood of account compromise through brute force or dictionary attack techniques. Priority high.

**Technical Controls:**

Install an Intrusion Detection System (IDS). this allows the IT team to identify possible intrusions (i.e., anomalous traffic) quickly. Employee data encryption, this makes confidential information/data more secure (i.e., website payment transactions). Priority High/Medium