Botium Toys - Compliance checklist

To review compliance regulations and standards, read the controls, frameworks, and compliance document.

- ☐ **The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

  The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

  Explanation:

- ☑ **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:
  This regulation applies if Botium Toys processes personal data of individuals located within the European Union, even if the company is based outside the EU. GDPR requires businesses to protect the personal data and privacy of EU citizens and comply with data processing and storage rules.

☑ **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:
Botium Toys needs to adhere to the PCI DSS if it processes, stores, or transmits credit card information. This standard aims to ensure the secure handling of cardholder data and protect against potential data breaches and fraud.

☐ **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:

☑ **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:

SOC 1 and SOC 2 reports may be relevant to Botium Toys depending on the company's operations and its relationships with third-party vendors. SOC 1 focuses on the controls relevant to user entities' internal control over financial reporting, while SOC 2 focuses on controls related to security, availability, processing integrity, confidentiality, and privacy. These reports can be essential for building trust and demonstrating the company's commitment to security and compliance.