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:

Not applicable as Botium Toys is not involved with the U.S. or North American power grid.

✓ **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: As Botium Toys conducts business in the EU, it is imperative to comply with GDPR. This regulation protects the processing of EU citizens' data and mandates notification within 72 hours of a data breach. Adherence is crucial for customer privacy and avoiding substantial fines.

✓ **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: Since Botium Toys accepts online payments, complying with PCI DSS is essential. This standard ensures that credit card information is processed, stored, and transmitted securely, minimizing the risk of 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:

Not relevant as Botium Toys does not deal with patient health information.

- ✓ **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 reports are vital for assessing Botium Toys' user access policies and financial compliance. They cover important aspects like confidentiality, privacy, integrity, availability, security, and overall data safety. Compliance helps in mitigating risks related to fraud and maintaining data integrity.