Compliance Checklist

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

The FERC-NERC regulation pertains to organizations involved in the electricity sector and the U.S. and North American power grid. They must be prepared to address and report security incidents that could impact the power grid. These organizations are legally obligated to follow the Critical Infrastructure Protection Reliability Standards (CIP) outlined by the FERC.

Explanation: NA

☑ **General Data Protection Regulation (GDPR)**

GDPR, or the General Data Protection Regulation, is an E.U. data regulation designed to safeguard the processing of data belonging to E.U. citizens and uphold their right to privacy within and outside the E.U. In the event of a data breach impacting an E.U. citizen, prompt notification within 72 hours of the incident is mandatory.

Explanation: Botium Toys must follow GDPR because they conduct business and collect personal information from people worldwide, especially the E.U.

☑ **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS, the Payment Card Industry Data Security Standard, is a global security framework established to guarantee that organizations handling, accepting, processing, and transmitting credit card data maintain a secure operational environment.

Explanation: Botium Toys must follow PCI DSS because they store, accept, process, and transmit credit card information in person and online.

☐ **The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA, or the Health Insurance Portability and Accountability Act, is a federal statute enacted in 1996 to safeguard the health information of U.S. patients. It strictly prohibits

the sharing of patient information without their explicit consent. Organizations are legally mandated to notify patients in the event of a data breach.

Explanation: NA

☑ **System and Organizations Controls (SOC type 1, SOC type 2)**

SOC1 and SOC2 reports are comprehensive evaluations that delve into an organization's user access policies across various organizational tiers. These reports serve as critical tools for gauging an organization's financial compliance and risk posture. They encompass an array of factors including confidentiality, privacy, integrity, availability, security, and overall data protection. Failures in control within these domains can potentially result in fraudulent activities.

Explanation: Botium Toys needs to establish and enforce user access for internal and external personnel to mitigate risk and ensure data safety.