# Botium Boys Compliance checklist

# **\_\_\_\_\_ The Federal Energy Regulatory Commission - North American Electric**

**Reliability Corporation (FERC-NERC)**

The rule is relevant to entities in activities related to electricity, particularly those connected to the U.S and north American power grid. Such organizations are obligated to proactively ready themselves for, mitigate and report any potential security breaches that could have adverse impact on the power grid. Legal compliance mandates that these organizations adhere to the Critical Infrastructure Protection Reliability Standards (CIP) as defined by the Federal Energy Regulatory Commission (FERC)

**Explanation:** NA

**\_\_X\_\_ 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:** Botium Toys needs to adhere to GDPR because they conduct business and collect personal information from people worldwide, including the E.U.

**\_\_X\_\_ 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 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 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:** NA

**\_\_X\_\_ 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:** Botium Toys needs to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.