# 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:**

**__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:** As Botium Toys are moving their business to European market, they must adhere GDPR because Botium Toys will be handling E.U. citizens PII, such as their: Name, age, gender, address, debit card/credit card information.

**_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 operations involves selling toys mainly from their online platform but also selling them from their store. These transactions may involve payment by card or cash. As Botium Toys deal with credit card information physically and online, hence, they must comply with PCI DSS

**___ 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:**

**___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:** In risk assessment it was identified that there is inadequate management of assets. One of the assets identified was the data. Therefore to mitigate this risk, Botium Toys must establish and enforce appropriate user access for its employees to ensure data safety.