# Compliance checklist

**\_\_\_\_\_ 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:** FERC-NERC regulations apply to entities in the energy sector, particularly, those involved in the generation, transmission, and distribution of electric power.

**\_\_\_\_\_ 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 an E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident.

**Explanation:** Botium Toys is expanding its online market to Europe. GDPR governs the protection, processing, and transfer of personal data of individuals within the European Union. Compliance with GDPR ensures that Botium Toys handles personal data of EU residents in a lawful and secure manner, respecting their privacy rights.

**\_\_\_\_\_ 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 processes payment card transactions, they need to comply with PCI DSS. This standard ensures the secure handling of credit cardholder data and establishes guidelines for maintaining a secure payment environment. Compliance with PCI DSS helps protect customer payment card information and reduces 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:** Botium Toys is not in the healthcare business, hence HIPAA compliance may not be necessary.

**\_\_\_\_\_ 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 may need to undergo SOC Type 1 and SOC Type 2 audits to demonstrate their adherence to security, availability, processing, integrity, confidentiality, and privacy controls. These reports are often requested by customers and business partners to assess the effectiveness of an organization’s internal controls.