# 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:**

**\_\_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:** In order to conduct business outside the US, the company must adhere to the GDPR regulations for the protection of user data of citizens of the E.U. The lack of a security framework that includes controls for mitigating the risk of loss of assets such as PII, as well as corrective measures to be followed in the case of a security incident could result in fines due to non-compliance of the GDPR.

**\_\_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:** In order to reduce fraudulent transactions, the company must implement a framework that contains the necessary controls to ensure the secure handling of payment information which includes credit card information, PII, and SPII. Failure to meet the standards of PCI DSS may mean loss of confidence in the company resulting in reduced revenue.

**\_\_\_\_\_ 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:** The company needs to implement policies to minimize the amount of access to assets based on controlling least privilege. This limits the amount of risk to by limiting access to assets to internal threat actors such as disgruntled employees. This minimizes financial loss due to sabotage of systems or loss of intellectual property.