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: N/A

- ☑ **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: The company's failure to implement comprehensive data protection policies is a primary reason for non-compliance. GDPR requires organizations to have clear and documented policies for data handling, storage, and security. Without such policies, there is a higher risk of mishandling and unauthorized access to sensitive data, which could lead to data breaches and potential legal liabilities.

☑ **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: Non-compliance with PCI DSS results from critical gaps in their payment card data security practices. Lack of proper encryption, data segmentation, and secure network architecture leaves cardholder data vulnerable to unauthorized access. The absence of regular security testing and vulnerability assessments further increases the risk of data breaches, potentially leading to severe financial penalties and loss of card payment privileges.

☐ **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: N/A

☑ **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: Non-compliance with SOC Type 1 and SOC Type 2 can be attributed to their lack of comprehensive security controls and risk management practices. SOC Type 1 certification evaluates the design and implementation of an organization's controls at a specific point in time, while SOC Type 2 assesses the effectiveness of these controls over a period. The company's absence of documented and tested controls, such as access controls, encryption, monitoring, and incident response plans, prevents them from demonstrating the necessary level of security and compliance required for these certifications.