

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:

☒ **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:

☒ **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:

☐ **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:

☒ **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 will need to adhere to the GDPR as their online presence continues to grow across multiple countries. GDPR will allow the company to establish regulations / policies to adhere to the European Union (E.U.) general data regulation for its citizens from Europe who access the company site.

As the company handles payments online, they will also need to adapt to PCI DSS, an international security standard to protect user data when storing, accepting, processing, and transmitting credit card information.

Additionally, the company will need to adhere to FERC-NERC regulation applied to organizations that work with electricity since they are manufacturers of toys using electricity in doing so. This will also help provide backup and disruption to the electricity grid.

Lastly, the company should implement the SOC1 and SOC2 are a series of reports to ensure confidentiality, privacy, integrity, availability, security, and overall data safety to prevent fraud from occurring and adding an additional layer of security for all employees and users.