

# 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:**

## ☒ **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: Botium Toys conducts business worldwide including the EU. As an organization that hosts data center services and potentially handles customer data, it is important to adhere to the standards outlined under the GDPR. This will help keep customer data safe and provide a template if a breach were to occur.**

## ☒ **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: As an e-commerce and commercial business Botium handles Payment data on a regular basis. Compliance with the PCI DSS is mandatory to ensure the safety of customer and vendor payment information.**

☐ **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: Assets listed by the IT manager include, remote workstations, desktops/laptops, vendor access management, data center hosting, and more. This along with the amount of users possibly interacting with data increase the risk of fraud and breaches. With a stated intention of increasing the size of the team, Implementing SOC1 or SOC2 would be a good idea to counter the risk.**