# 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:**

Botium Toys must comply with these regulations because they operate in the electricity sector and the North American power grid. They have a legal obligation to prepare for, mitigate, and report any security incident that could negatively impact the power grid.

* **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:**

It is crucial for Botium Toys to comply with GDPR if they operate in or with EU citizens, as it protects personal data and privacy rights of EU citizens, with strict notification requirements in case of security breaches.

* **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:**

Botium Toys needs to comply with PCI DSS if they handle credit card information, ensuring that card data is handled securely to protect against fraud and meet international security standards.

* **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:**

If Botium Toys handles patient health information in the United States, they must comply with HIPAA to protect patient information privacy and notify about security breaches as required by federal law.

* **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:**

Meeting SOC type 1 and SOC type 2 standards not only helps Botium Toys meet regulatory and compliance expectations, but also strengthens its security and risk management posture, thereby protecting the financial and data interests of the company and its stakeholders.