# Compliance checklist

To review compliance regulations and standards, read the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/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 does not have to comply with this regulation since it is not directly in the business of generation, transmitting or distributing electricity or any other critical infrastructure for that matter.*

**\_\_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:** *Since the Botium Toys sells merchandise to people beyond the US, there is a high chance that some of their customers are from Europe. The GDPR applies to any organization doing business with any resident of the EU …including Botium. Hence, Botium must prove their compliance with the GDPR as it regards customer’s PII and financial data.*

**\_\_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:** *Botium would have to show compliance with this regulation since it offers electronic payment methods from consumers. Electronic payment typically retains consumer data such as name, address, card numbers, etc.*

**\_\_\_\_\_ 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:** *Botium does not have to show compliance for this regulation since it does not collect patient’s health data.*

**\_\_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:** *Botium would have to show compliance with this control framework as it employs procedures, standards and policies that should safeguard financial data as well as safety of company, vendors’, and client’s data. Should there be vulnerabilities that are exploited by threat actors, it will cause financial and reputation damage to all parties and might cost the organization some regulatory fines.*