# 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:** N/A

**\_\_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 an E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident.

**Explanation: Botium Toys will have to adhere to the GDPR because their online market is selling toys in countries part of the E.U. where customer data would be stored on databases belonging to the company. And these databases would need to be fortified physically and technically.**

**\_\_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 Toys will have to adhere to the PCI DSS, because first and foremost they’re a business and generally all businesses would have some sort of transaction/ sales. And these sales could be through credit cards, and in this case since Botium Toys also sells their products online they would be storing, accepting, processing and transmitting credit card infromation.**

**\_\_X\_\_ 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**

**\_\_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 Toys will need to conduct SOC1 and SOC2 reports because even if this is a small organization there will still be a hierarchy within it from the associate level to the executive level which all have some sort of user access. Also the company would be handling internal financial information, such as payroll for employees and accounting records regarding invoices or accounts receivable. And identifying the organization’s security posture regarding confidentiality, privacy, integrity, availability, security, and overall data safety can also benefit the evidently growing organization.**