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:** This is a toy company and has no impact to a power grid. This is not relevant

**\_\_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:** This regulation applies if Botium Toys processes personal data of people located within the EU, even if the company is based outside of the EU. They have a requirement to protect the personal data and privacy of EU citizens.

**\_\_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:** The toy company will be processing payment transactions for each customer that buys something. The toy company is responsible for the payment data and has an obligation to ensure the data is processed, transmitted, and stored correctly.

**\_\_\_\_\_ 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:** This is not relevant to a toy company. They don't have patients and will not be working with health information

**\_\_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: The SOC 1 and SOC 2 reports are relevant to Botium Toys because they have users data stored under their control. They also are handling financial data so they need to be able to verify compliance and regulate risk. SOC 1 focuses on the controls relevant to user entities financial reporting. SOC 2 focuses on controls related to security, availability, integrity, confidentiality, and privacy regarding financial data. These reports can be essential for building trust and demonstracting the company's commitment to security and compliance.**