# 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:** The company uses employee equipment, internet, data centers, and badge readers, all of which use power from the U.S. and North American power grid, and if any of which were to be compromised it would negatively affect the power grid, breaking compliance of the FERC-NERC

* **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:** The company, though small, does have a growing online presence that has reached customers abroad, which may include E.U. citizens. A compromise would endanger the safety of the data and privacy of E.U. citizens, violating compliance of the GDPR

* **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:** Utilizing management of systems, software, and services in regards to accounting, in addition to data and storage, the company may contain customer credit card information. An incident in which this information is stolen would result in a violation of PCI DSS.

* **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:** Being an online business, the company’s data centers will contain user information. An incident leaking personally identifiable information customers would result in violation of HIPAA

* **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:** Being an online business, the Botium Toys’ data centers will contain user information. An incident leaking personally identifiable information customers would result in violation of SOC1 and SOC2.