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) documents.

**\_\_\_\_\_ The Federal Energy Regulatory Commission - North American Electric**

**Reliability Corporation (FERC-NERC)**

The FERC-NERC regulation applies to organizations that work with electricity or are involved with the U.S. and North American power grids. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. They are also legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

**Explanation:** Botium Toys is unlikely to need to adhere to this regulation as it is not an organization that works with electricity or is involved with the U.S. and North American 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 an E.U. citizen’s data is compromised, they must be informed within 72 hours of the incident.

**Explanation:** Botium Toys needs to adhere to GDPR if it handles the personal data of European Union (EU) citizens, regardless of whether It is based in the EU or not. GDPR protects the processing of EU citizens' data and their right to privacy both inside and outside the EU. Adhering to GDPR ensures that Botium Toys processes personal data lawfully, fairly, and transparently and protects the rights of the data subjects, including the right to access, correct, and delete their personal data.

**\_\_✓\_ 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 must adhere to PCI DSS if it stores, processes, or transmits credit card information. PCI DSS is an international security standard designed to ensure that organizations handle credit card data securely and protect it from unauthorized access, use, or disclosure. Adhering to PCI DSS helps Botium Toys prevent credit card fraud and protect its customers' financial information.

**\_\_\_\_\_ 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 Toys is unlikely to need to adhere to HIPAA unless they handle protected health information (PHI) of US patients, which is unlikely given that Botium Toys is a toy company. HIPAA is a US federal law that sets national standards for protecting PHI, including its use, disclosure, and security requirements. Adhering to HIPAA ensures that PHI is handled and protected appropriately and helps prevent unauthorized access or disclosure of patients' sensitive health information.

**\_\_✓\_ System and Organizations Controls (SOC type 1, SOC type 2)**

The SOC1 and SOC2 are reports focusing on an organization's user access policies at different organizational levels. They are used to assess an organization’s financial compliance and risk levels. They also cover confidentiality, privacy, integrity, availability, security, and data safety. Control failures in these areas can lead to fraud.

**Explanation:** Botium Toys may need to adhere to SOC type 1 or SOC type 2 if they handle financial information, such as payroll or accounting records. SOC type 1 and SOC type 2 are reports that evaluate the effectiveness of an organization's controls related to financial reporting and data security. Adhering to SOC type 1 or SOC type 2 helps ensure that Botium Toys' financial data is accurate, complete, and secure and has appropriate controls to prevent fraud or errors.