# 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:**

* **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: Botium Toys needs to adhere to GDPR if they process data of European Union (EU) citizens, regardless of whether the processing occurs within or outside the EU. The reasons are:**

**Data Protection: GDPR ensures the protection of personal data and privacy rights of EU citizens. Botium Toys must implement measures to secure this data and ensure it is processed lawfully and fairly.**

**Transparency and Consent: GDPR mandates that individuals must give informed consent for their data to be processed. This requires Botium Toys to be transparent about data processing practices and to obtain explicit consent when necessary.**

**Breach Notification: In case of a data breach that risks individuals' rights and freedoms, Botium Toys must notify affected individuals within 72 hours. This ensures that individuals are informed promptly about potential risks to their data.**

**Accountability: GDPR requires organizations to be accountable for data processing activities. This includes appointing a Data Protection Officer (DPO) and implementing measures to demonstrate compliance.**

* **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: Payment Card Industry Data Security Standard (PCI DSS):**

**Botium Toys needs to adhere to PCI DSS if they store, accept, process, or transmit credit card information. The reasons are:**

**Credit Card Data Protection: PCI DSS ensures that credit card data is handled securely throughout the entire payment process, reducing the risk of data breaches and fraud.**

**Customer Trust: Compliance with PCI DSS demonstrates to customers that Botium Toys takes their financial data security seriously, enhancing customer trust and reputation.**

**Avoiding Fines and Legal Consequences: Non-compliance with PCI DSS can result in hefty fines and legal consequences. Adhering to the standard helps Botium Toys avoid financial penalties and legal disputes.**

* **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:**

* **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 needs to consider SOC type 1 and SOC type 2 reports to assess their user access policies, financial compliance, and overall data safety. The reasons are:**

**Risk Management: SOC reports help Botium Toys identify and manage risks associated with user access, financial processes, and data security. This enables the organization to prevent potential issues and vulnerabilities.**

**Data Integrity and Availability: SOC reports evaluate the integrity and availability of data, ensuring that systems and controls are in place to prevent unauthorized access and data loss.**

**Trust and Transparency: SOC reports provide customers, vendors, and stakeholders with a level of assurance that Botium Toys is operating with proper controls and security measures in place.**

**Financial Compliance: SOC type 1 and SOC type 2 reports assess financial compliance, helping Botium Toys meet industry and regulatory requirements related to financial data integrity.**

**In summary, applying these compliance regulations (GDPR, PCI DSS, SOC type 1, SOC type 2) helps Botium Toys protect customer data, enhance trust, avoid legal consequences, and demonstrate accountability in their operations.**