Compliance checklist

To review compliance regulations and standards, read the 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: it's crucial to follow the GDPR because it's a legal requirement when handling personal data of individuals from the European Union, no matter where your company is located. By complying with the GDPR, you ensure the protection of individual rights, implement robust data security measures, and reduce the risk of facing substantial fines and damage to your reputation. It's also a way to build trust with your customers and partners, showing them that you prioritize responsible data handling practices and take data privacy seriously.

☑ **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: It's crucial to follow PCI DSS because it ensures the protection of cardholder data, preventing data breaches and securing transactions. Complying with PCI DSS is a legal and contractual requirement imposed by payment card networks and financial institutions, which helps your company avoid penalties and maintain business relationships with payment processors. By adhering to these standards, your company demonstrates a commitment to data security, instilling trust and confidence in your customers.

☐ **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

☑ **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 follow System and Organization Controls (SOC) for these reasons: SOC compliance provides assurance to clients and partners about your security practices, meets client requirements for vendor risk management, and helps mitigate security risks by identifying and addressing potential weaknesses in your systems and processes