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.

- ☑ **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.

- ☑ **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.

- ☐ **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.

☑ **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 is subject to critical compliance mandates such as GDPR, PCI DSS, and SOC 1 / SOC 2 due to its operational scope involving the handling of customer data—potentially from EU citizens—the processing of payment card transactions, and the oversight of sensitive internal systems like accounting, inventory, and security infrastructure. Adhering to these standards is not merely procedural but a strategic imperative to uphold data stewardship, fortify information assurance, and reinforce stakeholder trust. Noncompliance could precipitate substantial regulatory penalties, reputational erosion, and operational disruption, undermining both the company's resilience and its capacity for sustainable growth in an increasingly risk-aware digital ecosystem.