Compliance checklist

☐ **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: NA

☑ **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: Non-compliance with GDPR can lead to severe consequences, including significant fines and reputational damage. Therefore, it is crucial for Botium Toys to implement appropriate security measures, data protection practices, and processes to ensure compliance with GDPR requirements. By doing so, the company demonstrates its commitment to safeguarding the privacy and rights of its E.U. customers, which ultimately fosters trust and confidence in the company's handling of 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: PCI DSS is an international standard that plays a crucial role in ensuring the security and confidentiality of credit card information. By adhering to this standard, Botium Toys can create a secure environment for handling credit card data, protect its customers, and demonstrate their commitment to data security and compliance.

☐ **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: NA

☑ **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: By obtaining these reports, organizations can demonstrate their commitment to security and compliance, instilling confidence in their clients and stakeholders that their data is handled with utmost care and integrity.