Compliance Checklist

Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC) The FERC-NERC standards are relevant for companies involved in electricity production or connected to the power grid in the U.S. and North America. These organizations must prepare for, reduce, and report any security incidents that could impact the grid. Compliance with the Critical Infrastructure Protection Reliability Standards (CIP) as set by FERC is legally required.

Explanation: NA

General Data Protection Regulation (GDPR) The GDPR is a regulation from the European Union (EU) that safeguards the data processing and privacy rights of EU citizens, regardless of where the data processing occurs. In the event of a data breach involving EU citizens, they must be notified within 72 hours.

Explanation: Botium Toys must comply with GDPR as they operate globally and collect personal data, including from EU residents.

Payment Card Industry Data Security Standard (PCI DSS) PCI DSS is an international standard designed to ensure that organizations handling credit card data do so securely, whether they store, process, accept, or transmit such information.

Explanation: Botium Toys needs to follow PCI DSS because they manage credit card data both in-store and online.

The Health Insurance Portability and Accountability Act (HIPAA) HIPAA is a U.S. federal law established in 1996 to protect patient health information. It requires that patient information not be shared without consent, and mandates that patients be informed in case of a data breach.

Explanation: NA

System and Organization Controls (SOC Type 1, SOC Type 2) SOC 1 and SOC 2 reports focus on the policies related to user access within an organization at various levels. These reports assess financial compliance, risk levels, and cover aspects such as confidentiality, privacy, integrity, availability, security, and overall data safety. Failures in these controls can lead to fraud.

Explanation: Botium Toys should implement and enforce appropriate user access policies for both internal and external (third-party vendor) personnel to mitigate risks and ensure data protection.