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: Botium Toys are required to adhere to this compliance law as breaches can cause damage to assets and in turn may cause damage to power grid also. In case of negligence and not reporting any expected issue to FERC - NERC , fines can be imposed.

☑ **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: In order to adhere to GDPR , Botium Toys customer’s PII and SPII should be critically handled and should not be exposed to outside vendors. Therefore, proper protection methods need to be implemented.

☑ **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: Botium Toys customers credit card information is not properly encrypted. So, assessments need to be done to comply with this law.

☑ **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: As a major element in CRF, PII and SPII of Botium Toys customers need to be protected. So, compliance with this law is also on our to do list.

☐ **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: No need to check mark this as Botium Toys are already complying with SOC's user access policies.