# 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:** **N/A**

* **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:** As part of the expanding market for Botium Toys, it is strongly recommended to comply with General Data Protection Regulation (GDPR) due to the possible dealings and transactions with international clients that are part of the European Union (E.U.) and its neighbouring countries that are within this scope. This is also to ensure that the privacy, data protection, and security of each potential client would be prioritised for any possible incident, breach, or threat that would also benefit the company's business continuity.

* **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:** Nationwide and International-based transactions from current or future clients that uses or will use electronic form of payment from their bank accounts such as Electronic Fund Transfer at Point of Sale (EFTPOS) or any form of online payment should adhere with such regulations not just for seamless transaction but to implement security and privacy in all aspects. This will also strengthen and improve business reputation to organisations, clients, and external stakeholders.

* **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:** Financial compliance must have its own security measures most specifically with Botium Toys aiming to cater the online market abroad. Having structured policies and procedures regarding financial compliance is deemed necessary given the variation of laws, regulation and/or legislation of each country involved and to restrict any chances of paying hefty fines and any fraudulent activities. This should be applicable to all aspects of financial transactions. E.g., Invoicing, reimbursement, accounts payable and receivable, and many more.