Topic 1 Discussion 2

Briefly examine a law, regulation, and a standard that organizations use to align with government requirements around cybersecurity best practices within their industry.

Hello Class,

Law: Children’s Online Privacy Protection Act (COPPA)

COPPA is a U.S. federal law that protects the privacy of children under 13 years old by requiring parental consent before collecting personal information from them. Organizations must provide clear privacy policies, obtain verifiable parental consent, and ensure the security of children’s data, thereby promoting responsible data handling practices.

Regulation: Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a U.S. government program that standardizes the security assessment, authorization, and continuous monitoring for cloud services used by federal agencies. Cloud service providers must meet specific security requirements outlined in the FedRAMP Security Assessment Framework. This includes implementing a robust set of security controls based on NIST SP 800-53, ensuring that government data is adequately protected when stored or processed in the cloud.

Standard: International Organization for Standardization (ISO) 27001

ISO/IEC 27001 is an internationally recognized standard for managing information security. It provides a systematic approach to managing sensitive company information. Organizations seeking certification must establish, implement, maintain, and continually improve an Information Security Management System (ISMS). This involves assessing and mitigating risks to protect data confidentiality, integrity, and availability, thereby aligning with global best practices

References:

Federal Register :: Request Access. (2013, January 17). Unblock.federalregister.gov. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

FedRAMP. (n.d.). Program Basics | FedRAMP.gov. Www.fedramp.gov. https://www.fedramp.gov/program-basics/

ISO/IEC 27001 Standard: Information Security Management. (n.d.). Www.nsf.org. https://www.nsf.org/management-systems/iso-iec-27001

What is FedRAMP and How Does it Work? | Synopsys. (n.d.). Www.synopsys.com. https://www.synopsys.com/glossary/what-is-fedramp.html