**Sprint Four: Regulatory Compliance**

**Group Members Responsible:**

**What does it mean the differences between a cybersecurity secure program being in regulatory compliance?**

**Regulations**: Regulations are specific rules and guidelines established by regulatory authorities or industry bodies. ***Being "in regulations" means that the cybersecurity secure program aligns with the specific regulations relevant to the organization's industry or operations.*** This entails meeting the additional requirements beyond the basic legal obligations. Regulations are typically more specific and detailed than laws, and they often focus on a particular industry, sector, or specific aspect of a broader law. In the cybersecurity realm, regulations outline specific requirements and standards that organizations must follow to ensure the security and privacy of data. These regulations may be issued by governmental bodies or industry-specific regulatory agencies.

*Example*: The General Data Protection Regulation (GDPR) in the European Union is a regulation that governs the privacy and protection of personal data for individuals residing in EU member states. It sets specific requirements for organizations to handle personal data, including cybersecurity measures, breach notification obligations, and data subject rights.

**Compliance**: Compliance refers to the act of adhering to all applicable legal requirements, regulations, and standards. ***A cybersecurity secure program is considered "in compliance" when it fulfills all the necessary obligations, both legal and regulatory.*** Compliance demonstrates that the program meets the required standards and best practices. Compliance programs are designed to mitigate risks, promote good governance, and ensure adherence to legal and regulatory obligations.

*Example*: An organization being in compliance with the Payment Card Industry Data Security Standard (PCI DSS) means that it has implemented the necessary technical and operational security measures to protect cardholder data as required by the standard. Compliance with PCI DSS is essential for organizations that handle payment card information.

**Compliance: Depending on what regulation and/or cybersecurity framework you’re working on, the research and writing should answer most the following questions (with APA Cited References):**

* **What federal regulations does a cybersecurity secure program for a non-profit organization have to adhere to?**
* **What state regulations does a cybersecurity secure program for a non-profit have to adhere to?**
* **Why does the cybersecurity program have to adhere to this specific federal or state regulation? (For example, it’s because they take online payments.)**
* **What industry-specific regulations are applicable to the non-profit organization?**
* **What does the cybersecurity secure program have to contain or offer to satisfy or adhere to (regulation being discussed)?**
* **Are there any California, Georgia or New Jersey state regulations applicable to a cybersecurity secure program for an NPO (as TKH operates in CA, GA and NJ)?**
* **Which cybersecurity frameworks would keep a secure program in regulatory compliance? How?**
* **What is CIS and how is it used as a security control tool? How does CIS satisfy compliance?**
* **What are the data breach notification requirements? (What are the legal obligations and timelines for reporting data breaches or security incidents to affected individuals, regulatory authorities, or other relevant parties?)**
* **Relate it back to legal compliance:** 
  + **What federal laws are being followed when a cybersecurity secure program is following [insert federal regulation here]?**
  + **What federal laws are being followed when a cybersecurity secure program is following [insert state regulation here]?**
    - For example, breach notification for personal information breaches is in alliance with the New York SHIELD Act

**Preliminary Research**

**Regulatory Considerations:**

1. **What sensitive data that TKH possesses is covered by specific regulations?** Identify the types of data assets involved, such as personally identifiable information (PII), financial information, health records, or student records. *Determine if the organization falls under specific regulatory frameworks like HIPAA (Health Insurance Portability and Accountability Act) for healthcare data or FERPA (Family Educational Rights and Privacy Act) for student records.*
2. **Are there any specific data privacy laws applicable to the non-profit organization?** Determine if the organization operates in states or countries with data privacy laws beyond federal requirements. For instance, in addition to federal laws like HIPAA or GDPR (General Data Protection Regulation), consider state-specific laws like the California Consumer Privacy Act (CCPA) if the non-profit organization handles data of California residents.
3. **How does the non-profit organization handle consent and opt-outs?** Evaluate if the organization has processes in place to obtain consent from individuals for data collection, use, and sharing. Ensure compliance with regulations requiring explicit consent, opt-out mechanisms, or specific notices to individuals.
4. **Are there any contractual obligations with stakeholders?** Review contracts with vendors, partners, or service providers to ensure compliance with regulatory requirements and data protection clauses. Consider any data protection agreements or clauses required to safeguard data when engaging with third parties.
5. **New York State Department of Financial Services (DFS) Cybersecurity Regulation (23 NYCRR 500):** Although primarily focused on financial institutions, this regulation may apply to non-profit organizations that are regulated by the DFS or act as service providers to covered entities. It sets forth comprehensive cybersecurity requirements, including risk assessments, data encryption, incident response plans, and third-party vendor management.

References:

New York State Senate. (n.d.). General Business Law Article 39-F. Retrieved from<https://www.nysenate.gov/legislation/laws/GBS/39-F>

U.S. Department of Health & Human Services. (n.d.). Health Information Privacy. Retrieved from<https://www.hhs.gov/hipaa/index.html>

U.S. Department of Education. (n.d.). Family Educational Rights and Privacy Act (FERPA). Retrieved from<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

New York Codes, Rules, and Regulations. (n.d.). Title 23 - Department of Financial Services. Retrieved from<https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I4b5a5f30ebe011e6a9ed9f4b4f51db02&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)>

**What federal regulatory bodies and compliance regulations govern cyber secure programs to protect confidential data assets in a non-profit organization that is designed to help students develop skills in technology?**

In the United States, several federal regulatory bodies and compliance regulations govern cyber secure programs to protect confidential data assets in non-profit organizations focused on helping students develop technology skills. The following are key regulatory bodies and regulations to consider:

1. Federal Trade Commission (FTC): The FTC is responsible for enforcing consumer protection laws and regulations, including those related to data security and privacy. Non-profit organizations that collect, store, or process personal information need to comply with FTC regulations to ensure the privacy and security of individuals' data.
2. Children's Online Privacy Protection Act (COPPA): COPPA is enforced by the FTC and focuses on protecting the privacy of children under 13 years old. Non-profit organizations that provide online services or collect personal information from children must comply with COPPA regulations.
3. Federal Communications Commission (FCC): The FCC oversees regulations related to communication networks and services. While primarily focused on telecommunications, the FCC may have relevant regulations regarding cybersecurity and data protection for non-profit organizations operating in the technology education space.
4. Family Educational Rights and Privacy Act (FERPA): FERPA is enforced by the U.S. Department of Education and governs the privacy and security of student education records. Non-profit organizations involved in education that receive federal funding must comply with FERPA regulations.
5. National Institute of Standards and Technology (NIST): NIST provides guidance and standards on cybersecurity and data protection. While not a regulatory body, NIST's frameworks, such as the NIST Cybersecurity Framework and NIST Special Publications, offer best practices and guidelines that non-profit organizations can adopt voluntarily to enhance their cybersecurity programs.

These regulatory bodies and compliance regulations ensure the protection of confidential data assets and privacy in non-profit organizations that focus on technology education for students.

APA Citation:

Federal Trade Commission. (n.d.). Protecting Kids' Privacy Online. Retrieved from<https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy>

U.S. Department of Education. (n.d.). Family Educational Rights and Privacy Act (FERPA). Retrieved from<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

**What FTC regulations govern cybersecurity secure program within a non-profit organization?**

The Federal Trade Commission (FTC) is responsible for enforcing various regulations related to cybersecurity and data protection in non-profit organizations, particularly concerning consumer privacy and security. While there isn't a specific set of FTC regulations exclusively for non-profit organizations, the FTC has general regulations and guidelines that apply to all entities, including non-profits. Here are some key regulations and guidelines enforced by the FTC:

1. Section 5 of the Federal Trade Commission Act: Section 5 prohibits unfair or deceptive practices in commerce, including deceptive or misleading claims related to cybersecurity measures. Non-profit organizations, like all businesses, must ensure they do not engage in deceptive practices regarding their cybersecurity practices.
2. Safeguards Rule (part of the Gramm-Leach-Bliley Act): The Safeguards Rule requires financial institutions, including certain non-profit organizations that handle financial information, to develop a written information security program to protect the confidentiality and security of consumer information.
3. Red Flags Rule: The Red Flags Rule requires financial institutions and creditors, including some non-profit organizations, to develop and implement identity theft prevention programs to identify and mitigate the risk of identity theft.
4. Health Breach Notification Rule: While primarily enforced under HIPAA (Health Insurance Portability and Accountability Act), the FTC has jurisdiction over non-profit organizations that are not covered entities but handle personal health information. Such organizations must comply with the Health Breach Notification Rule, which requires them to notify individuals and the FTC in the event of a breach of unsecured personal health information.

These regulations, while not exclusive to non-profit organizations, apply to all entities engaged in commerce, including non-profits. Non-profit organizations should ensure they have appropriate cybersecurity measures in place, adhere to industry best practices, and avoid engaging in deceptive practices related to cybersecurity.

APA Citation:

Federal Trade Commission. (n.d.). Protecting Personal Information: A Guide for Business. Retrieved from<https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>

**How do I use NIST 800-171 and ISO 27001 to ensure the secure program is legally and regulatory compliant for a medium non profit organization?**

To ensure that your secure program for a medium non-profit organization is legally and regulatory compliant, you can leverage NIST 800-171 and ISO/IEC 27001 as follows:

1. NIST 800-171: NIST 800-171 focuses on protecting Controlled Unclassified Information (CUI) in non-federal systems. It provides security requirements and guidelines that can be tailored to suit the organization's specific needs. By implementing the controls outlined in NIST 800-171, you can address the protection of sensitive information and comply with relevant regulations.

For example, one control in NIST 800-171 is "Access Control (AC)." To satisfy this control, you can implement strong authentication mechanisms, such as multi-factor authentication, to control access to sensitive data and systems. This ensures that only authorized individuals can access the information, in compliance with regulations that require strong access controls.

1. ISO/IEC 27001: ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a systematic approach to managing information security risks and ensures the implementation of appropriate security controls. Compliance with ISO/IEC 27001 demonstrates a commitment to maintaining a robust security program.

For example, one control in ISO/IEC 27001 is "Information Security Incident Management (A.16.1.5)." To satisfy this control, you can establish an incident response plan that outlines the procedures for detecting, responding to, and mitigating security incidents. This ensures compliance with regulations that require organizations to have a well-defined incident response capability.

By integrating NIST 800-171 and ISO/IEC 27001, you can achieve legal and regulatory compliance across multiple frameworks. These frameworks address various aspects of cybersecurity and provide a comprehensive set of controls and practices to enhance your secure program.

The use of NIST 800-171 and ISO/IEC 27001 can satisfy several cybersecurity frameworks, including:

1. Federal Acquisition Regulation (FAR) Clause 52.204-21: This clause requires organizations doing business with the U.S. federal government to implement specified security controls. By following NIST 800-171, you can meet the requirements outlined in this clause.
2. General Data Protection Regulation (GDPR): The GDPR outlines data protection requirements for organizations handling personal data of European Union citizens. Adhering to ISO/IEC 27001 can demonstrate compliance with GDPR's security and privacy requirements.
3. Payment Card Industry Data Security Standard (PCI DSS): PCI DSS applies to organizations that handle payment card data. By implementing relevant controls from NIST 800-171 and ISO/IEC 27001, you can address several PCI DSS requirements related to data protection and secure systems.

References:

National Institute of Standards and Technology. (2020). Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements.

**What New York State department of education regulations govern cybersecurity secure program within a non-profit organization?**

The New York State Department of Education (NYSED) has several regulations and guidelines related to cybersecurity within non-profit organizations, particularly those involved in educational activities. While NYSED does not have specific regulations solely dedicated to cybersecurity, they provide guidance and requirements regarding student data privacy and protection. Here are a few relevant regulations:

1. New York State Education Law § 2-d: This law focuses on the privacy and security of student data. It outlines requirements for educational agencies, including non-profit organizations, regarding the collection, storage, and use of student data. It mandates the adoption of policies and practices to ensure data privacy, security, and appropriate data sharing.
2. New York State Education Department Data Privacy and Security Policy: NYSED has developed a Data Privacy and Security Policy to provide guidelines and best practices for educational agencies, including non-profit organizations. This policy emphasizes the protection of student data, data governance, and data sharing agreements.

References:

New York State Education Department. (n.d.). Data Privacy and Security Policy. Retrieved from<http://www.nysed.gov/data-privacy-and-security/data-privacy-and-security-policy>

New York State Education Department. (n.d.). Education Law Article 2-D. Retrieved from<http://www.counsel.nysed.gov/portal/sites/default/files/reports-and-materials/SAM_Education_Law_Article_2-D.pdf>

New York State Education Department. (n.d.). Data Privacy and Security Policy. Retrieved from<http://www.nysed.gov/data-privacy-and-security/data-privacy-and-security-policy>