NIST Cybersecurity Framework AI Assignment

Justin T Wilson

CSYE 200T

In a one page summary, what are the differences between the 1.1 edition and the 2.0 edition of the NIST cybersecurity framework?

NIST CSF 1.1 vs. 2.0: Key Differences

1. **Expanded Scope and Integration**:
    a. **CSF 1.1**: Primarily focused on U.S. critical infrastructure.
    b. **CSF 2.0**: Broadened to a global audience, integrating with other frameworks like the NIST Privacy Framework and Secure Software Development Framework.
2. **New Functions and Categories**:
    a. **CSF 1.1**: Five core functions: Identify, Protect, Detect, Respond, Recover.
    b. **CSF 2.0**: Added a new function called **GOVERN**, emphasizing governance and risk management.
3. **Enhanced Guidance and Practical Examples**:
    a. **CSF 1.1**: Provided general guidelines.
    b. **CSF 2.0**: Introduced **Implementation Examples** to help organizations apply the framework effectively.
4. **Continuous Improvement and Feedback**:
    a. **CSF 1.1**: Emphasized regular assessments.
    b. **CSF 2.0**: Added an **Improvement Category** within the Identify function to stress ongoing cybersecurity efforts.
5. **Refined Categories and Subcategories**:
    a. **CSF 1.1**: Categories like Identity Management, Access Control, and Data Security.

Commented [WJ1]: The internet has grown and more people and entities around the world are interacting and becoming vulnerable and affected by the other frameworks so it was necessary to grow.

Commented [WJ2]: The Govern function encompasses all of the original 5 core functions. Adding it engrains risk management into the whole framework before and during the other functions, minimizing risk.

Commented [WJ3]: Having examples instead of only general guidelines makes the using framework easier and more applicable.

Commented [WJ4]: Instead of assessing issues after the fact, Identifying and "Improving" in real time, you can continue to keep up with changes in cybersecurity threats and vulnerabilities.

Commented [WJ5]: Expanding the categories and breaking up certain categories into separate categories leads to more specific and covered instances.

b. **CSF 2.0**: Refined and expanded categories, such as separating Identity Management and Access Control into distinct categories.

6. **Supply Chain Risk Management**:
    a. **CSF 1.1**: Limited focus on supply chain risk.
    b. **CSF 2.0**: Enhanced supply chain risk management guidelines, including a new subcategory for supply chain security practices.
7. **Organizational Profiles and Tiers**:
    a. **CSF 1.1**: Provided a basic structure for organizational profiles and tiers.
    b. **CSF 2.0**: Expanded on these concepts, offering more detailed descriptions of current and target cybersecurity postures.

Commented [WJ6]: The supply chain is important and has vulnerabilities, the expansion was necessary to maintain supply chain security.

Commented [WJ7]: As cybersecurity postures evolved, a more robust set of tiers and profiles were needed to cover more scenarios and better prioritizations.