Cloud Security Alliance
709 Dupont Street Bellingham, WA 98225
March 8, 2023

NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

CSA Response:

1. **Do the proposed changes reflect the current cybersecurity landscape (standards, risks, and technologies)?**

   The proposed changes should improve the framework's usability, clarify its underlying principles, and account for changes in the cybersecurity landscape since the framework's original release in 2014.

   The proposed changes include a shift towards a more outcomes-based approach, increased focus on supply chain risk management, and expanded guidance on identity and access management.

   Overall, the changes proposed in the NIST Cybersecurity Framework 2.0 Concept Paper are getting much closer to ensuring that the framework remains relevant and effective in addressing current and future cybersecurity challenges. However, the effectiveness of these changes will ultimately depend on how they are implemented and adopted by organizations.

2. **Are the proposed changes sufficient and appropriate? Are there other elements that should be considered under each area?**

   The proposed changes to the Risk Management category include greater emphasis on supply chain risk management, increased guidance on third-party risk management, and a focus on identifying and prioritizing risks. Emphasis on the Shared Responsibility Model Report should be considered, emphasized, and considered mandatory.

   An SSRM outlines the respective security responsibilities of the cloud service provider (CSP) and the customer in a cloud computing environment. The advantages of the shared responsibility model include

   Clarity of responsibility: The shared responsibility model provides a clear delineation of security responsibilities between the CSP and the customer. This helps to reduce confusion and ensure that each party understands their respective responsibilities.

Better security posture: Help to improve the overall security posture of a cloud environment. By clearly defining security responsibilities, all parties can focus on their respective areas of expertise to implement appropriate security measures.

Improved compliance: The shared responsibility model can help to improve compliance with security and privacy regulations.

Cost savings: Help to reduce costs by allowing the parties to manage security measures that are specific to the provider while the customer can focus on security measures specific to their application.

Increased flexibility: The shared responsibility model allows for greater flexibility in terms of the specific security measures that are implemented.

Risk management: The shared responsibility model allows for better risk management by identifying potential security risks and assigning responsibility for their management.

CSA has formed a subgroup to the Cloud Control Matrix (CCM) and a mechanism to evaluate the SSRM and author a guidance document on SSRM. This group is made up of many industry experts as well as CSA analysts. While this subgroup concentrates on the Cloud Control Matrix that addresses controls specific to the cloud sector, we would happily engage with NIST to collaborate on supporting similar guidance activities regarding the CSF 2.0.

A mechanism for validating compliance.

The paper does mention that 2.0 may include examples of how organizations have used the CSF to assess and communicate their cybersecurity capabilities. However, still no real mention of a formal third-party or “independent review”. Communicating how you do something or a self-attestation does not add any value unless there are some checks and balances in place.

Having said that, if the CSF is positioned to be a company’s cyber security business strategy, that is a board governance function, similar to the overall business strategy. It would be appropriate to validate the results, not the plan, just as we validate a company’s business strategy through its audited financials.

Independent verification (could be 2nd or third-party provides):

Objectivity: Provides an objective assessment of an organization's security controls. This helps reduce bias and ensure that the assessment is conducted in a fair and impartial manner.

Credibility: This is a big one as it can increase the credibility of an organization's security controls. This is because the report is issued by an independent organization that is recognized for its expertise in the field. Interpretation and consistency thereof are always a concern.

Compliance: It can help show the all-important “due diligence” and “standard of care” showing that an organization has taken proper care and proper steps to claim they comply with applicable industry standards and regulations. We must be mindful that some regulations and standards require organizations to undergo some sort of independent evaluation or even certification as a way to demonstrate compliance with security and privacy requirements.

Risk management: It can help organizations manage security risks better by validating that nothing was missed and validating the current process.

Competitive advantage: It can provide organizations with a competitive advantage. Independent verification can demonstrate to customers, partners, and other stakeholders that an organization takes security seriously and has implemented effective security controls.

Efficiency: It can help organizations to more efficiently assess the effectiveness of their security controls. By leveraging the expertise of an independent organization, organizations can avoid the need to conduct assessments themselves, which can be time-consuming and resource-intensive.

Validation should be strongly encouraged but we support the open stance that flexibility should be maintained.

3. **Do the proposed changes support different use cases in various sectors, types, and sizes of organizations (and with varied capabilities, resources, and technologies)?**

   It does propose to provide and include updated and expanded guidance on Framework implementation as well as use cases and so on, suggesting to document implementation examples to provide additional guidance for specific sectors, threats, or use cases.

   As we deduced from the workshop sessions the cloud is the elephant in the room for 2.0. With the huge upsurge in cloud adoption, as we have never seen before, it is critical to document good best practices and possibly even form a think tank that users can join to discuss and debate interpretation issues.

   CSA can offer its services to coordinate such a think tank if NIST would like to engage.

4. **Are there additional changes not covered here that should be considered?**

   We did not detect anything immediately other than what has been mentioned above.

5. **For those using CSF 1.1, would the proposed changes affect the continued adoption of the Framework, and how so?**

   The proposed changes to the Cybersecurity Framework (CSF) 1.1 could potentially have a positive and negative effect on the continued adoption of the Framework in a number of ways, so transition guidance (not to be confused with implementation) along with some sort with expected timelines may be in order. Some of the ways in which the proposed changes could impact adoption include:

   Compatibility with existing implementations: The proposed changes to the CSF 1.1 may make it more difficult for organizations to adopt the updated version of the Framework, as they may need to make significant changes to their existing implementation.

   Complexity: The proposed changes to the CSF 1.1 may increase the complexity of the Framework. This could make it more difficult for organizations to understand and implement the Framework, thus slowing adoption.

   Increased cost: The proposed changes to the CSF 1.1 may increase the cost of implementing the Framework. This could make it more difficult for small and medium-sized organizations to adopt the Framework, as they may not have the resources to implement the updated version.

   Improved effectiveness: On the other hand, the proposed changes to CSF 1.1 should also improve the effectiveness of the Framework. By addressing weaknesses in the existing version of the Framework and incorporating new cybersecurity best practices, the updated version could provide better guidance for organizations looking to improve their cybersecurity posture, thus making a case for updating.

   It will ultimately depend on how the changes are implemented and how well they are received by organizations that use the Framework.

6. **For those not using the Framework, would the proposed changes affect the potential use of the Framework?**

   The proposed changes to the CSF 1.1 could impact the potential use of the Framework for organizations that are not currently using it. While the changes could make the Framework more relevant and provide improved guidance, they could also increase complexity and require additional resources to implement. It will ultimately depend on the specific needs and resources of each organization to determine whether the Framework is a good fit for their cybersecurity program.