Overarching Perspectives: Main Themes

Fundamentally, we find that many cybersecurity organizations “miss the forest for the trees” with respect to implementing security frameworks such as NIST CSF. In particular, most organizations have not historically performed risk assessments with even order of magnitude accuracy to be able to make the correct foundational decisions around their approach to cybersecurity and framework adoption. For example, decisions such as determining which Implementation Tier or Framework Profile is appropriate require appropriate insight informed by an understanding of the risk that a poor cybersecurity posture presents to the business. Today, cyber risk assessments are mostly subjective, and typically result in an underestimation of the level of cyber risk. As a result, we have underinvestment or mis-directed investment in appropriate people, process, and technology. To counter this, we strongly recommend that NIST CSF 2.0 more strongly highlight the importance of initial data-driven, quantified risk assessments such that organizations may be better placed to leverage the framework for better outcomes.

While implementation focus for many practitioners has been extent and coverage of the NIST CSF Categories and Subcategories across Functions, we find that the “organizational mindset” as aligned to Implementation Tiers (1 to 4) is more closely correlated to improved cybersecurity posture and cyber-related outcomes. For example, whether an organization is Adaptive, e.g., “The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators” vs. Repeatable, e.g., “risk management practices are formally approved and expressed as policy” is typically more important in practice than implementing the next incremental Category or Subcategory of the framework. We recommend that NIST CSF 2.0 more strongly highlight the value of adopting more advanced Implementation Tiers when making the necessary cost/benefit tradeoffs.

In particular, given the dynamic nature of enterprise environments and the current threat landscape, also recommend that NIST CSF 2.0 increasingly highlight the importance of velocity (speed in an appropriate direction) with respect to learning, adaptation, and taking corrective action. For example, identifying and categorizing an enterprise’s assets once a month simply does not work when the mean-time-to-weaponize newly found vulnerabilities is less than 15 days.

Overarching Perspectives: Implementation Tiers

The current NIST CSF 1.1 Implementation Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). Based on the variety of challenges, organizational processes, and levels of investment that we see at enterprise organizations of all

sizes, we recommend that NIST CSF 2.0 incorporate the following practical progression with respect to Implementation Tier design regarding proactive cybersecurity processes:

1. Having visibility - This includes the ability to eliminate inventory blind spots and know what is being secured. Organizations initially struggle to get a good grip on fundamental visibility. Organizations should be able to answer simple questions like “how much coverage and confidence do we have in asset inventory?”. The answer to this should be quantitative, e.g., 98% coverage at 95% confidence, and not qualitative.
    a. While there is a growing need and interest for the continuous and unified asset inventory, software inventory often is overlooked.
    b. Up to date and unified software inventory is key to identifying, and remediating vulnerabilities with high velocity. Teams often spend weeks and months to investigate and identify the appropriate vulnerabilities and fixes. This leads to very high and often unacceptable time to mitigate or remediate critical vulnerabilities.
    c. Visibility today means fortnightly and monthly scans for most organizations. Having a continuous view of vulnerability is critical to achieving a better viewpoint of risk aiding in swifter decisions. Today most organizations have more incoming vulnerabilities in the time allocated for scans and remediations as compared to the planned remediations.
2. Having consolidated viewpoints - Organizations are too often using dozens of different tools, resulting in information remaining siloed and not shared in a manner that is useful for effective reporting or decision making.
3. Having qualitative security views - Knowing what weaknesses lurk where. Given the volume of the vulnerabilities that can affect assets of all types, organizations need to have a standardized approach to auditing, documenting, and bookkeeping everything that affects their broader cybersecurity posture.
    a. Automated way to do this is critical given the proliferation of assets, 3rd party software, open-source software and the new vulnerabilities that arrive.
4. Having quantitative security views - Given the volume of vulnerabilities and the acknowledgement that it is impossible to address them all in a timely manner, quantifying the risk stemming from each vulnerability and prioritization on this basis is key for organizations to manage cyber risk efficiently.
5. Having all of the above assessed continuously - This concept was already incorporated in one of the maturity levels in CSF 1.1 (Tier 4: Adaptive) and should continue to be so. We recommend being more prescriptive on the time granularity required, which might be near real-time or within a few hours, as opposed to fortnightly, monthly, or quarterly.
6. Being able to make risk-informed decisions - This aligns with the newly proposed “Govern” category of items. In order to effectively set policies based on the risk reduction that is feasible from various programs, based on the risk transfer and risk appetite that is acceptable for the enterprise, to identify changing patterns of risk and corresponding response needed in security programs, a continuous risk assessment and quantification mechanism that is explainable and traceable, that can simulate “what if” scenarios are critical.

Specific Perspectives on the NIST Cybersecurity Framework 2.0 Concept Paper

Section 1: CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications

Point of view:

1.2. Scope the CSF to ensure it benefits organizations regardless of sector, type, or size

- It is important to ensure that smaller organizations with limited cybersecurity resources and time can effectively use the CSF. So, it would be beneficial to provide more specific guidance on implementation. For example, predefined profiles with baseline functions, categories, and subcategories that an organization can customize to their specific needs and risk profile would be helpful. Additionally, it would be helpful to consider if it is feasible to map to technologies where applicable. Organizations can use the profiles to inform their buying decisions for security tools and services.

Section 2: CSF 2.0 will remain a framework, providing context and connections to existing standards and resources

Point of view:

2.2. Relate the CSF clearly to other NIST frameworks

- Keeping other NIST cybersecurity and privacy-related frameworks separate is a good direction. This keeps CSF's focus clear and concise. However, it would be helpful to have references/mappings from CSF to the other frameworks where applicable and it is kept current as per section 2.4.

2.4. Use updatable, online Informative References

- Having the Informative Reference mappings consolidated online in one place and updated periodically will be very helpful to ensure users have the most current information for implementation. Perhaps consider allowing users to directly request mapping additions through the CPRT application.

2.6. Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices

- It makes sense for CSF to continue to be technology and vendor neutral as the technology landscape changes over time. However, it would be helpful to have mappings from CSF to specific technologies that are important for modern enterprise cybersecurity architectures. Part of the problem in cybersecurity is that customers are pulled in so many different directions by different frameworks and analyst market acronyms. Some convergence and alignment in these will provide a huge service, especially to smaller and less mature organizations.
- Noting that "CSF 2.0 will expand consideration of outcomes in the CSF Respond and Recover Functions", it is critical to highlight the fundamental importance of proactive

cybersecurity hygiene as represented by the Identify and Protect functions. Organizations that proportionally over-focus on reactive cybersecurity response vs. proactive hygiene face being overwhelmed by the increased volume of successful attacks on their highly exposed environments. An ounce of prevention is worth a pound of cure.

Section 3: CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

Point of view:

3.1. Add implementation examples for CSF Subcategories

- It would be beneficial to have the notational implementation examples as a column in the CSF core for better ease of usage. One of the challenges we see organizations facing is building a unified cybersecurity risk model to understand all the cybersecurity risks more easily they face, prioritizing risk mitigation, and their impact on the business. While the CSF Identify function has an asset management category, perhaps it would be helpful to include the need for unified asset management across the organization and that the types of assets are more varied today when considering applications deployed in cloud environments.

3.3. Improve the CSF website to highlight implementation resources

- The proposed greater emphasis on published success stories should be beneficial. In particular, it is desirable that these success stories highlight outcomes that result in tangible and quantified risk reduction.

Section 4: CSF 2.0 will emphasize the importance of cybersecurity governance

Point of view:

- A dedicated 'Govern' function will give impetus to uplevelling the cybersecurity conversations in the organizations (at exec/board levels) at par with broader enterprise risks (financial, legal, reputational risks etc.)
- It will help organizations better be able to align cybersecurity activities with their overall business objectives.
- The core idea behind 'Govern' function can further be enriched by including a mention of organizations adopting cyber risk quantification (CRQ) as one of the key mechanisms to measure and manage cybersecurity risks. It will help provide a singular language (in monetary terms) to express overall organizational risks. This can help ensure that everyone is on the same page when it comes to understanding the potential impact of cyber threats and the need for effective cybersecurity governance.
- Govern function boundaries include 'determination of priorities and risk tolerances of the organization.' CRQ can also help organizations in prioritizing and defining the acceptable levels of risk and provide a consistent approach to managing risk across the enterprise.

- In general, key issues with developing effective cybersecurity governance include cybersecurity risk data is spread across multiple siloed tools, data gathering, and processes are manual, mapping to business impact is difficult, budget for security initiatives, and the lack of resources. It would be helpful if the current subcategories being proposed for moving to this new function are more general to include all organizations' infrastructure (e.g., ID.BE and ID.RM) and perhaps through Informative References or technology mappings indicate that automation and moving towards a more unified risk model will greatly simplify the implementation of a governance program.

Section 5: CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (C-SCRM)

Point of view:

- The last update to NIST happened in 2018 and post that software supply chain vulnerabilities and resultant attacks like SolarWinds, Log4j, Spring4Shell have had significant impact. Supply chain security is among the top-of-the-mind concerns of most organizations. The expanded coverage on protecting the supply chain in the upcoming version CSF is a welcome move.
- The upcoming version of the framework could emphasize on inclusion of the Software Bill of Materials (SBOM) under the 'Identify' pillar. Our work with Fortune 100 companies at the onset of Log4j revealed that most organizations struggled with their lack of ability to produce a software bill of materials (SBOM) on demand for the in-use application packages and applications. Without an accurate SBOM, identifying the instances where this vulnerability exists may take months.
- An area that NIST CSF 2.0 could emphasize is the need for real-time visibility into the Software Bill of Materials (SBOM). Currently, many organizations lack an up-to-date software inventory view, which can result in a lag between the actual state of the network and the view of the organization's software assets. By prioritizing real-time SBOM visibility, NIST CSF 2.0 can help organizations better identify and mitigate software vulnerabilities, as well as third-party vendor risks.
- To effectively manage cybersecurity supply chain risk, the importance of addressing both software component vulnerabilities and third-party vendor risks needs to be sufficiently covered. For example, a software component vulnerability risk could be the discovery of a vulnerability in a widely used software library per examples such as OpenSSL, Log4J, etc. Meanwhile, a third-party vendor risk could be a breach of a cloud service provider. Given that these two broader types of supply chain risks need different handling and on-ground processes, NIST could simplify and lay separate emphasis on both software and third-party sections in the upcoming CSF 2.0 update. (Rather than calling it under one broad category)

Section 6: CSF 2.0 will advance understanding of cybersecurity measurement and assessment

Point of view:

- Current Implementation tier model of NIST CSF (v1.1) talks about the implementation tiers as Partial, Risk Informed, Repeatable, Adaptive, in an order that mirrors overall maturity. CSF v2.0 proposed updates include the desire for the CSF to clearly explain how organizations can use the Implementation Tiers, and how they relate to measurement. One of the factors in determining implementation tiers is an 'Integrated Risk Management Program' that is measured via the awareness of cybersecurity risk at the organizational level. This factor does not seem to include the maturity of the organization's unified risk model (siloed visibility to unified visibility) as one of the criteria. This is something that could be explicitly stated.
- It would be beneficial to articulate and include reporting requirements of data. Building the right metrics, trend lines of data and reporting mechanisms for easy explainability and actionability will enhance the framework's usability

Specific Perspectives on the NIST CSF 1.1 Elements for Update in NIST CSF 2.0

- Asset Management (ID.AM): given the nature of asset and software inventory data that is increasingly siloed and distributed across numerous technologies and data sources of different types, at different frequencies and level of fidelity, it is important to recognize that building and maintaining an up-to-date and accurate asset inventory requires collection, normalization and correlation of asset data in a parallel manner as described in (DE.AE-3): "Event data are collected and correlated".
- Likewise, given the nature of vulnerability assessment and scanning capabilities, typically distributed across multiple technologies, and detecting vulnerability assessment data at different frequencies and levels of fidelity, processes such as (ID.RA-1): "Asset vulnerabilities are identified and documented" should be modified to refer to collection, normalization, and correlation of vulnerability data.