FORRESTER®

Forrester Response to NIST Cybersecurity Framework 2.0 RFC

03 November 2023

Forrester Research, Inc.

[redacted]

Taylor Hawkins | Account Manager II – NIST

[redacted]

Table of Contents

Feedback on NIST Cybersecurity Framework

Overview

In summary, the NIST CSF 2.0 represents a substantial enhancement compared to its initial iteration, effectively tackling numerous challenges encountered by practitioners. The significance of this framework to the industry and professionals cannot be overstated. It is for this reason that we are providing constructive feedback on select aspects of the framework. Our intention is to contribute to the clarification of the CSF's objectives, its implementation in achieving these objectives, and to support NIST's ongoing efforts in a manner that offers clarity to practitioners and aligns with models they commonly utilize.

Distinguish between Framework Tiers and Capability Maturity Models

We strongly advise clarifying the Framework Tiers to distinguish them from cybersecurity capability maturity models. As former federal employees who have implemented the NIST CSF and as industry advisors working with the public and private sector, we notice that practitioners overwhelmingly conflate Framework Tiers with measures of cybersecurity capability maturity. This problem is more than semantical. In practice, many organizations develop multi-year roadmaps and allocate resources to projects because they believe it will move them to a higher Tier – but when they begin the process of tracking their improvements, they find that they do not have a way of measuring capability maturity at all. The result is vague reports to leadership promising improvement while security teams implement control projects that diverge from CSF best practices (and their related NIST SP 800-53 control).

While this was briefly addressed in the original CSF, we believe that *Section 3.3 – Using Framework Tiers to Characterize Cybersecurity Risk Management Outcomes* should encompass not only the definition of what Framework Tiers *are* but also explicitly outline what they are *not*. The Tiers' title language uses similar terms as capability maturity models with specific reference to cybersecurity outcomes – but practitioners confuse this with capability maturity models for the categories and subcategories in the CSF. We recommend specifying that Framework Tiers are not a measure of category-level maturity and noting that users can/should incorporate capability maturity models as a way of assessing capability at this level. NIST's OLIR Program includes informative references to such models today, including the C2M2 model, to further substantiate the difference while giving the reader additional references to consider.

Bridge the Risk Management Gap between Govern and Identify

To further enhance the relationship between risk management strategy (Govern) and practice (Identify), we recommend NIST address two key gaps noted below. The goal is to improve how readers consume the information via direct reference while specifying implied or assumed activities.

ID.RA (Risk Assessment) – Add a subcategory for assets

We recommend adding a subcategory to ID.RA to specify that the asset inventory (and control status of those assets) from the preceding ID.AM category is shared/maintained with an organization's risk management system. This makes it clear to operators that asset inventories are essential to effective risk management. In practice, many organizations manage their asset inventories in different systems, which are disconnected from a risk management system and the teams that conduct risk assessments beyond a business impact analysis. To bridge this gap, we believe it is important to connect ID.RA with ID.AM directly to show the interconnected relationship.

This addresses a simultaneous challenge in industry where organizations confuse vulnerability or threat assessments with risk assessments. Without the risk assessment being directly routed within the context of the assets, an organization cannot fully assess the likelihood or impact of a loss event occurring (as noted in NIST SP 800-30, *Guide for Conducting Risk Assessments*).

ID.IM (Improvement) – Add a subcategory for Continuous Control Monitoring

We recommend adding a subcategory to ID.IM to specify that organizational and system-level security controls are regularly evaluated for effectiveness. The CSF 2.0 does not reference control monitoring or effectiveness in its current state. We believe this is a significant area for improvement that will help organizations mature their existing risk management programs. The concept of control assessment is implied in ID.RA, but not stated. Likewise, DE.CM addresses continuous monitoring – but it is focused on technical monitoring capabilities across assets, rather than control monitoring. There is a missing link between technical monitoring in the Detect category vs the control monitoring needed at a program-level in Identify.

Based on our research, we find that continuous control monitoring is a fundamental capability for governance, risk, and compliance teams to determine and communicate the effectiveness and value of security control investments. While DE.CM focuses on asset monitoring, the control monitoring side that typically resides in an organization's risk management function is missing. Continuous monitoring at a program-level is achieved when asset-level monitoring (operations-focused) is combined with control effectiveness monitoring (oversight-focused). When combined, cybersecurity programs can address immediate operational detection needs while evaluating control performance to plan for long-term maturity. We believe this is key to shifting organizations from *reactive* to *proactive* risk management.

Section 5 (Next Steps) – Add a reference to NIST 800-160 series for risk-based secure systems engineering

We recommend citing the NIST SP 800-160 volumes as a reference in Section 5. The 800-160 volumes connect to the NIST SP 800-53 controls and the NIST Risk Management Framework. They should also be connected to the NIST CSF 2.0 to achieve a full view of how engineering teams fit into the overall CSF as an organization implements it. This is especially important for critical infrastructure organizations as it reinforces the collaborative relationship needed between security and engineering teams, which are often independent in practice.

Add a Function-Specific Process and Policy Category for Each Function

We recommend adding a Process and Policy category to each function. DE.DP was an example of this – it makes more sense to have the policy outlined in the category than it does to put it in one consolidated category like Govern or Identify. Otherwise, it will be confusing and challenging for security professionals to find related recommendations to various functions. Further, consolidating under GV.PO will be challenging to manage, as in its current state it does not directly reflect the need for processes to support Identify, Protect, Detect, Respond, and Recover functions.

For example – as a detection engineer, it's ideal to go to one place – Detect – to find everything one needs to know about detection, instead of going to detection for only certain parts. Ultimately, this is about aligning to the reader.

Bring in Additional Links to Zero Trust

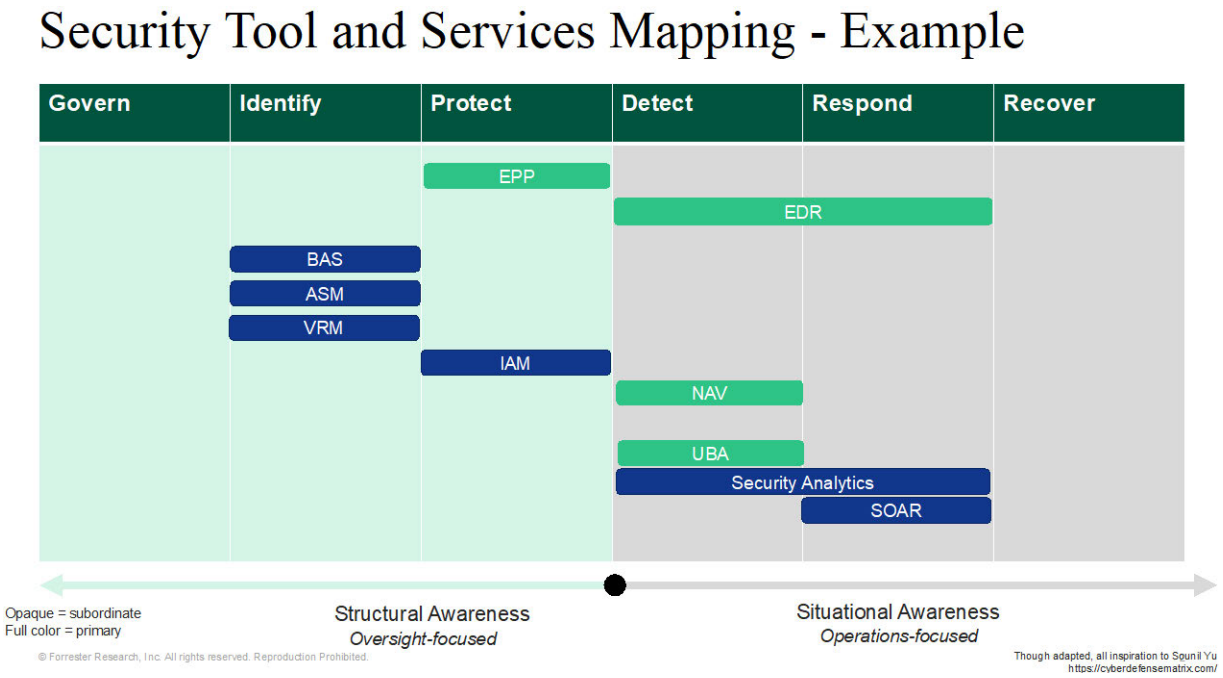
One of the top requests we receive when it comes to frameworks is how they align to Zero Trust (ZT). We highly recommend more closely aligning the pillars of ZT to the NIST CSF within this document to better tie together the different recommendations NIST and Cybersecurity and Infrastructure Security Agency (CISA) have. While referencing ZT and related works is useful, clear alignment and delineation in the document helps clarify in more depth how the frameworks can work together – which is one of the most challenging parts for practitioners.

Clarify Functions with Oversight vs Operations Wrapper

The work to shift subcategories like DE.CM-08, which align more to Identify than Detection, will be a huge improvement to the CSF. It will clarify control and process capabilities and the differentiation between detection and response to attacks versus finding misconfigurations or vulnerabilities. In order to ensure clarity, we suggest taking this a step further and differentiating capabilities between structural (oversight) and situational (operations).

- **Structural (oversight)** – Structural functions help provide visibility into (identify) and establish prevention (protect) for the enterprise infrastructure. This is often owned by the security engineering team, who is responsible for oversight, while IT operations is responsible for implementation.
- **Situational (operations)** – Situational functions help find (detect), remove (respond), and revert (recover) attacker activity that compromises enterprise infrastructure.

This helps clarify left of boom and right of boom, which is incredibly beneficial for understanding control functions, the processes that fit within them, and the teams responsible for them. See the figure below for an example of this.



Forrester

Forrester Research, Inc. is an American-Owned, publicly traded (NASDAQ: FORR) independent research and advisory firm that provides industry-leading research, advisory, and consulting services that have guided government and commercial clients to be their very best since 1983. Our unique blend of capabilities has given global consumer business and technology leaders a clear vision to see "what's now" and "what's next." Providing leaders like you a clear, guided path through the challenges of today and the ability to see over the horizon for tomorrow's successes and challenges.

Since its inception, Forrester has stood for uncompromising personalized service to our clients, acting as your partner through change. We accelerate your organization toward its objectives through technology adoption, increased efficiency, and effectiveness while creating vastly improved constituent and employee

experiences. Through our partnership, you can leverage all of Forrester's research and subject matter expertise in an integrated fashion within your teams and projects.

Our proven approach has assisted more than 60% of the Fortune 500 and 14 of 15 Executive Branch Departments to lower costs and increase their effectiveness. Forrester's banner product, Forrester Decisions, is so effective that in a 2023 Total Economic Impact (TEI) survey of our major clients, they cited an average of 259% Return on Investment over three (3) years. Furthermore, organization initiatives that leveraged Forrester data and know-how were 26% more likely to succeed than without our support.

So, what can Forrester mean to the National Institute of Standards and Technology (NIST)? It means having a true teammate in your endeavors, experts by your side when needed, and actionable guidance for some of your most challenging situations backed by real-life experience and research. It means having a steady, omnipresent support mechanism to help you make the right moves at the right time with the experts who actually do the research and have done the tasks. Forrester simplifies your service offering by bundling valuable certifications and industry-leading event attendance with unmetered research and advisory services for a holistic service that addresses your specific priorities with curated and focused content. In short, Forrester is your force and experience multiplier enabling your team to transcend its most challenging objectives.

Conclusion

Forrester appreciates the opportunity to offer feedback on the CSG 2.0 Public Draft. Should NIST desire more details regarding Forrester and our capabilities, please do not hesitate to contact the point of contact on the cover– or contact us here.