CYBER RISK INSTITUTE

November 1, 2023

To: National Institute of Standards and Technology
From: The Cyber Risk Institute
Subject: CRI Response to Proposed Changes to Public Draft Cybersecurity Framework 2.0

To Whom It May Concern:

The Cyber Risk Institute (CRI)[1] appreciates the opportunity to provide comments to the National Institute of Technology's (NIST) discussion draft of the Cybersecurity Framework (CSF) 2.0. We appreciate NIST's efforts to continuously improve and adapt the framework to address emerging threats and challenges, as well as advances in cyber risk management and associated practices. CRI particularly appreciates NIST's addition and refinement of the CSF's new "Govern" function and further addressing developments in technology and risk management.

In light of an ever-evolving cybersecurity landscape, we believe it is imperative that NIST further refine the Govern function to align with best practices, recognize the increasing significance of supply chain risk by elevating it to its own distinct function, and continue enhancing the clarity of category and subcategory statements within the core framework.

Addition and Refinement of the Govern Function Is Commended

We commend NIST on the addition and further refinement of the Govern function within the CSF. This evolution and organization should assist organizations in identifying the necessary steps for implementing integral cybersecurity risk management capabilities. By instilling principles of good governance, organizations can enhance their cybersecurity posture. Further, it underscores the important role that boards and senior leadership play in overseeing and managing cyber risk.

We also believe NIST could go further to suggest certain best practices that are proven-effective like the Three Lines of Defense risk management model that is currently largely used within the financial sector. This could help other sectors instill a structured and comprehensive approach to managing cyber risk that would amplify the positive enhancements in the new "Govern-Roles, Responsibilities, and Authorities" (GV.RR) category. We were pleased to see that NIST included enterprise risk management as a subcategory and independent audit in the implementation examples; however, independent audit is a

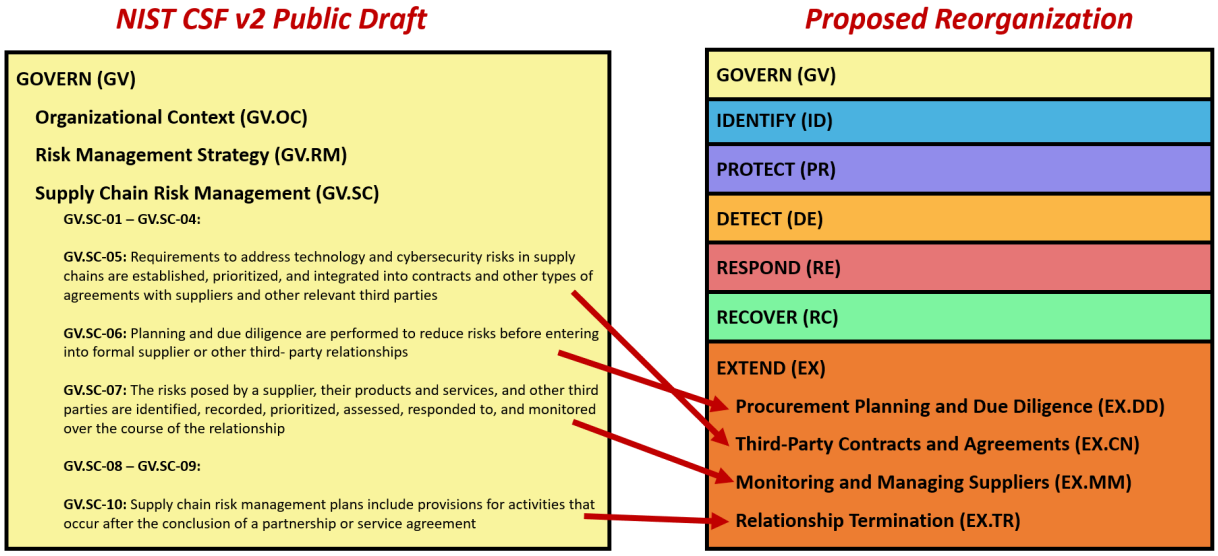
[1] CRI is a not-for-profit association of financial institutions representing the broad diversity of the financial services sector—from global institutions to community banks to cryptocurrency exchanges, etc. CRI's mission is to provide a flexible framework, called the CRI Profile, based on leading practices to help the financial sector better manage cyber risk. The Profile is derived from the NIST Cybersecurity Framework (CSF), but extended to include additional functions, control principles (called diagnostic statements), and regulatory references specific to the financial services sector. This extension of the NIST CSF is a testament to the CSF's usefulness and broad applicability to the private sector. It is from NIST, in fact, that the Profile derives its name—it is a "Framework Profile" based on guidance provided in the CSF.

critical role within the governance of cybersecurity programs. As noted in our previous response to NIST, we still recommend that NIST consider including independent audit as its own subcategory.[2]

Elevating Supply Chain Risk Management Remains Important

We applaud NIST's efforts to consolidate supply chain risk management considerations in the Govern function category (GV.SC). This change will enhance visibility of supply chain risks and provide a firm foundational roadmap to address supply chain risks as part of an organization's cybersecurity program. However, while this consolidation has undeniable improvements, the dynamic and intricate nature of supply chain threats and attacks in our current threat landscape necessitates an even more focused spotlight.

Additionally, the new CSF content consolidates both supply chain governance and operational activities, which does not entirely reflect the way organizations manage these functions. In our June submission, we suggested that such a function be named "Extend," and offered pertinent categories and subcategories. We, again, make this recommendation (and incorporate that submission by reference). Please see the following graphic for more detail.



We strongly urge NIST to elevate supply chain risk management to a distinct function. This elevation is critical to ensure futureproofing and global relevancy of the framework, as was expressed by non-US participants at the NIST workshops on September 19th and 20th, 2023. Governments and supervisors around the world have highlighted the importance of understanding supply chain risks, including those related to organizations' third, fourth, and "nth" parties, because of the heightened risks that these

[2] CRI, *CRI Response to Proposed Changes to the CSF v2.0 Core,* (Washington, D.C.: June 15, 2023). NIST website accessed October 20, 2023: https://www.nist.gov/document/cyber-risk-institute-06152023-discussion-draftredacted.

relationships pose. Indeed, elevating supply chain to its own function ensures alignment with emerging policies like the G7's *"Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector"*[3] and the Bank of England's "*Supervisory Statement – SS2/21: Outsourcing and Third Party Risk Management."*[4]

As NIST aims to position the CSF for future use, CRI encourages NIST to carefully consider the increasing dependence on third parties for business operations and the concurrent focus of regulators that are driving organizations to increase their understanding of third parties impact on their own resilience. While this may be a current focus for the financial services sector, most critical infrastructure sectors are dependent on third parties to enable their operations and will likely remain so in the future. To effectively future proof the CSF, CRI still recommends a separate function, which would streamline and simplify the ability to find relevant supply chain risk management considerations and outcomes. As a result, organizations of all sizes and in all sectors would be better positioned to appropriately manage these challenges should NIST elevate supply chain to its own function.

Recommended Revisions to Category and Subcategory Statements

The Cyber Risk Institute and its members have identified specific areas in the category and subcategory organization and statements that can benefit from increased clarity and alignment with evolving standards and regulatory developments. Consistent, uniform language improves comprehension and allows organizations to understand what of their existing practices align to CSF considerations. Please see the attached Appendix I for a detailed summary of recommendations.

In conclusion, the NIST Cybersecurity Framework continues to be an essential tool for organizations to navigate a complex, intricate cybersecurity threat landscape. We appreciate the opportunity to provide feedback and are confident with these suggested enhancements, the CSF will be better equipped to guide organizations towards more secure outcomes.

Thank you for your consideration to our feedback. We value NIST's commitment to obtaining and considering various viewpoints to ensure the CSF remains useful and relevant for the wide array of its users.

Sincerely,

/s/
Josh Magri
CRI CEO & President

---

[3] G-7, *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*, October 24, 2018. https://home.treasury.gov/system/files/216/G-7-FUNDAMENTAL-ELEMENTS-FOR-THIRD-PARTY-CYBER-RISK-MANAGEMENT-IN-THE-FINANCIAL-SECTOR.pdf.

[4]Bank of England's Prudential Regulatory Authority, *Supervisory Statement – SS2/21: Outsourcing and Third Party Risk Management,* March 31, 2022. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

Appendix I: Detailed Feedback on CSF's Categories and Subcategories

CRI has identified specific areas in the category and subcategory organization and statements that can benefit from increased clarity and alignment with evolving standards and regulatory developments. We have organized these comments by function below.

Govern Function

1. **GV.OC-04:** *Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated*; and **GV.OC-05:** *Critical outcomes, capabilities, and services that the organization depends on are determined and communicated*:

   The wording of these two subcategories is so general and similar that ambiguities arise in what "stakeholders expect" and what the "organization relies on." For example, stakeholders expect their online services to always be available, but the organization also relies on continuous availability of system services. The subcategories appear to be trying to target a) the identification of critical organizational products and services, and b) the dependencies (systems, resources, suppliers, other services, etc.) necessary to deliver the critical services (i.e., the primary subjects of Business Impact Analysis (BIA)). Perhaps the subcategory statements could more clearly distinguish between the two outcomes. By way of demonstration, Implementation Examples 1 and 2 for GV.OC-04 would appear to be equally valid for GV.OC-05. The challenge appears to be that GV.OC-04 includes dependencies for internal stakeholders, which are also covered by GV.OC-05.

2. ***Consider Adding a Risk Management Strategy*** (**GV.RM**):

   Consider adding a risk management (RM) subcategory along the lines of: *"The risks of technology assimilation and implementations are managed"* to address the management of risks associated with technology innovation and technology implementation projects. There are separate cyber risk management activities associated with these activities that aren't addressed elsewhere in the draft core—e.g., project lifecycle-related cyber risk management activities.

3. **GV.SC-05:** *Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties*; and **GV.SC-06:** *Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships:*

   Consider moving GV.SC-06 before GV.SC-05 as due diligence activities are generally performed before contracts are established.

4. **GV.SC-10:** *Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement:*

   Relationship termination planning should address certain activities and circumstances that occur prior to the conclusion of a partnership, not just after the conclusion of the partnership.

Consider "…include provisions that anticipate and address the risks of the termination of a partnership or service agreement."

5. **GV.RR-05**: *Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties*:

   Consider: *"Lines of communications and decision authorities across the organization…".* Suggest tying appropriate decision-making authority level to communications (two of the core elements of governance) as it more broadly addresses things like incident response decisions, third-party risk decisions, etc. Appropriate decision authority is not otherwise addressed in the core.

6. **GV.OV-01:** *Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction***; GV.OV-02:** *The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks*; and **GV.OV-03:** *Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction:*

   There appears to be considerable overlap in these three statements in that all three call for review ("outcomes are reviewed", "strategy is reviewed" and "performance is measured and reviewed") and all three call for adjustment of strategy ("adjust strategy and direction", "strategy is reviewed and adjusted" and "adjust strategic direction"). Consider combining or better disambiguating these three statements.

   It would also seem that Oversight (GV.OV) should in some way describe the role and cyber risk management outcomes expected of organizational leadership (as is referenced in GV.RR-01). Consider moving GV.RM-02 (establishment of risk appetite and tolerance) and GV.RM-04 (strategic direction in appropriate response options) under Oversight (GV.OV) as these are generally the responsibility of organizational leadership.

   As noted above, independent audit or independent review (whether internal or external) also play a critical role in governance and should be included in Oversight (GV.OV) or elsewhere in the Govern function.

Identify Function

7. **ID.AM-01**: *Inventories of hardware managed by the organization are maintained*:

   Consider *"hardware and virtual devices…".* Organizations often experience confusion about how virtual devices should be addressed in inventories. Consider any device (hardware or virtual) that is allocated an IP address here, to include virtual devices, or explicitly include virtual devices under ID.AM-02 (software inventory).

8. **ID.AM-05**: *Assets are prioritized based on classification, criticality, resources, and impact on the mission*:

   Consider *"Assets and services are prioritized…".* A critical aspect of BIAs is prioritizing the business processes and associated technology services. The assets supporting those processes and services can then be prioritized.

9. **ID.RA-07**: *Changes and exceptions are managed, assessed for risk impact, recorded, and tracked*:

   Change management and exception management should not be combined into a single subcategory. These are largely unrelated activities and are generally performed by different staff in even moderately-sized organizations.

   While change management includes aspects of risk assessment, it includes many other activities designed to actually manage the associated risks (i.e., change management is not inherently or primarily a risk assessment activity). Consider moving change management to PR.PS, just after configuration management. Exception management seems appropriately placed under ID.RA (another reason why they should be separate).

10. **ID.IM-04:** *Cybersecurity plans that affect operations are communicated, maintained, and improved*:

    It is unclear what *"cybersecurity plans that affect operations"* are—this phrase is too generic. The Implementation Examples seem to primarily reference incident response plans and vulnerability management plans. Both of these risk management activities (not really program improvement activities) are significant cyber program components and really deserve their own subcategories. Consider splitting into separate subcategories and moving under the Protect function.

Protect Function

11. **Identity Management, Authentication and Access Control (PR.AA)**: *Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access*:

    Consider adding a subcategory for privileged access management and service account management. These are significant targeted vulnerability areas and are too critical to be treated generically with other access types, similar to the way PR.AT-02 addresses "Individuals in specialized roles" separately from generic user training.

12. **PR.PS-04**: *Log records are generated and made available for continuous monitoring*:

    Recommend "undeleting" PR.PT-1 and providing a discrete mention of "determining" what events need to be logged, the content of log records, log security requirements, and the scope of assets for which logs should be collected. This is a separate, but critical, part of log management that's distinct from generating logs.

13. **Platform Security (PR.PS)**:

    Consider addressing accurate and resilient time services. This is critical to logging, event analysis, forensics, transaction processing, etc. and does not appear to have a clear subcategory home.
    Encryption standards and key management also do not appear to have a clear home. Although certificate management is referenced in the Implementation Examples for credential management, encryption, key, and certificate management warrant their own subcategory.

14. **PR.IR-02**: *The organization's networks and environments are protected from unauthorized logical access and usage*:

    Network segregation, access isolation, and defense-in-depth should be explicitly referenced as fundamental outcomes in a manner similar to "least privilege and segregation of duties" in PR.AA-05.

Detect Function

15. **DE.CM-09**: *Computing hardware and software and their data are monitored to find adverse cybersecurity events*:

    This subcategory appears too broad, especially in combining data with hardware and software. Suggest a more discrete treatment of these monitoring topics: perhaps something like at the level of compute, OT, and data; hardware, software, and data; or simply compute and data.

Respond Function

16. **RS.MA-02:** *Incident reports are triaged and validated*; **RS.MA-03:** *Incidents are categorized and prioritized*; and **RS.MA-04:** *Incidents are escalated or elevated as needed*:

    Consider combining these related activities into a single subcategory, such as: "*Incidents are triaged, categorized, prioritized, and escalated as warranted*."

17. **RS.CO-03**: *Information is shared with designated internal and external stakeholders*:

    Consider "Authorized information is shared…" to imply and emphasize a controlled process for information sharing.

18. **RS.MI-02**: *Incidents are eradicated*:

    Consider selecting a different word for "eradicated" when referring only to incidents. Although "Containment Eradication & Recovery" is a defined incident response phase in NIST SP 800-61, eradication in that context is described as specifically related to the artifacts of an attack. For incidents to be eradicated, one cannot completely "eradicate" all records, logs, documentation, or lessons learned about incidents. Suggest qualifying eradication to attack artifacts or deleting

this subcategory. Consider changing RS.MI-01: *Incidents are Contained*, to "Incidents are contained and mitigated" or change "eradicated" to "mitigated" in this subcategory.

Recover Function

19. **RC.RP-03:** *The integrity of backups and other restoration assets is verified before using them for restoration*; and **RC.RP-05:** *The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed*:

    These activities are normally performed together, and the subcategories could be combined. Alternatively, RC.RP-03 could be deleted by assuming the verification of the restored assets would encompass verification of the backups and other restoration assets.

20. **RC.RP-04:** *Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms*:

    The language in this subcategory statement is unclear. Is the objective to establish new operational norms (based on critical mission functions and cybersecurity risk management) or to verify that operations have returned to some defined state of pre-incident operational norm?