CYBER RISK
INSTITUTE

June 15, 2023

To: National Institute of Standards and Technology
From: The Cyber Risk Institute
Subject: CRI Response to Proposed Changes to the CSF v2.0 Core

The Cyber Risk Institute (CRI)[1] appreciates the opportunity to provide comments to the National Institute for Standards and Technology's (NIST) Discussion Draft of the Cybersecurity Framework Core 2.0. CRI commends the continued efforts of NIST to ensure that the next version of the CSF is forward-looking, clear, addresses developments in technology and risk, and improves alignment with national and international cybersecurity standards and practices. NIST's efforts deserve much praise, as most of the proposed changes constitute marked improvement. Notably, the addition of the "Govern" function is an important upgrade.

To further advance the NIST CSF's utility, longevity, and international acceptance, CRI offers a few additional, important refinements for consideration. While CRI recognizes that the financial services sector is more highly regulated compared to other sectors, CRI and its members feel strongly that the comments below help ensure that the CSF remains aligned with the U.S. Government's national security priorities and other global authorities' cybersecurity related expectations. Moreover, these recommendations can be applied across all sectors as cybersecurity continues to be a significant focus for all industries.

Consider Creating a New Supply Chain Risk Management Function

We appreciate NIST's continued focus on how the CSF should best address supply chain risk, or third-party risk management as commonly referred to in the financial services sector. Although we appreciate that NIST enhanced the CSF's existing Supply Chain Risk Management Category, the proposed structure distributes many important third-party risk management elements throughout the Core. CRI members strongly believe that the NIST CSF would be more useful today and in the future if NIST elevated Supply

[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.

Chain Risk Management to its own Function (perhaps called "Extend"[2]) through a simple reorganization of what is already contained in the last published version of the NIST CSF in addition to the recent draft Core update. We believe that reorganizing these key elements into a single Function will assist with better (1) alignment with existing standards and regulations, (2) focus on risks, (3) visibility to Boards, (4) practical implementation by users, and (5) ensuring the CSF's longevity through "future-proofing." Specifically, we propose consolidating the lifecycle management of suppliers (from planning and due diligence to relationship termination). See Appendix I for the components to be reorganized. See Appendix II for how they can be more fully described.

(1) Alignment

The number of standards, guidance documents, best practices, and regulatory issuances related to supply chain risk management is not only growing but accelerating. Additionally, the scope, coverage, and focus of these standards is converging very cleanly in the need to extend organizational policy and practices into a third-party ecosystem supporting and "extending" the organization. The NIST CSF is used to align and map to many other related documents and, as such, NIST should reflect the large body of standards work focused specifically on supplier management and ecosystem extension.

Not only does this align with national and international standards and practices, it supports U.S. government's priorities in addressing the challenge of understanding our supply chains and managing the risks associated with an increasingly interconnected world.

Supply chain or third-party risk management has been a priority for financial regulators and standards-setting bodies, globally. For example, ISO 27002 has a separate category for "supplier relationships." Likewise, recent supervisory and regulatory operational resilience principles and rulemaking[3] are driving financial institutions to increase the level of understanding of the potential impacts that a third-party may have on their resilience and the third-party's ability to rapidly recover from material operational events. These expectations often require additional visibility of and testing with critical third-party providers and as a result, several new and updated third-party risk management frameworks currently exist. Given this global evolution in supply chain risk management focus, a separate Supply Chain Risk

[2] CRI understands that it is important for NIST to maintain consistency with respect to labeling Functions. CRI offers a few suggestions to address "supply chain risk management," including "Extend," "Entrust," "Connect," "Oversee," or "Link."

[3] To address concerns over effective resilience practices in the wake of increased use of third-parties within the financial services sector, a number of recent papers, principles and rules have been established globally by standard setting bodies and regulators including, but not limited to:

- The Bank of England's *Policy on Outsourcing and Third Party Risk Management for Financial Market Infrastructures* - https://www.bankofengland.co.uk/paper/2023/policy-on-outsourcing-and-third-party-risk-management-for-fmis;
- The International Organization of Securities Commission's *Principles on Outsourcing* - https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf;
- European Union's *Digital Operational Resilience Act* - https://www.digital-operational-resilience-act.com/DORA_Articles.html;
- The Board, FDIC and OCC's *Proposed Interagency Guidance on Third-Party Relationships: Risk Management* https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management.

Management Function would enable a more holistic cybersecurity framework for financial services organizations to develop their cybersecurity programs and risk management practices.

(2) Focus

Managing suppliers, and the products and services they offer, should be a unified and holistic activity within an organization in order to be effective. Without a singular lifecycle view of potentially long-term and critical relationships with suppliers, decisions made early in a relationship may have severe negative consequences later. For example, inadequate and uninformed due diligence prior to establishing a contract could have consequential implications upon the failure of a supplier. Further, a focused treatment of supplier management in the CSF would promote harmonization (and avoid fragmentation) of the treatment of this topic in the implementation of the *National Cybersecurity Strategy* and future policy, legislative, and regulatory development. NIST should provide organizations with holistic guidance in managing the entire supplier lifecycle.

(3) Visibility

The NIST CSF is used by CRI members to effectively communicate key cybersecurity risks to the Board and executive management through its high-level Functions. Because the CSF is the structure by which organizations crystallize cyber risks, it is critical for the CSF's Functions to reflect the key risks Boards should be considering. In today's environment, Boards and executive management should have specific focus on the lifecycle management of the organization's suppliers and external ecosystem. A separate Supply Chain Function (potentially known as "Extend"), like for "Govern," would provide the necessary visibility to receive adequate attention by senior leaders.

(4) Practical Implementation

Likewise, creating a separate Supply Chain Function ("Extend") would facilitate organizations' management of its third-party relationships and help decrease complexity. A separate function would also help to increase the level of understanding of the potential impacts that a third-party may have on resilience by clearly highlighting important risk management elements.

It is important for organizations that the CSF adequately reflects their organizational needs and effectively shapes their focus, emphasis, and priorities. Because the CSF is often used by organizations to implement cyber risk management programs, the CSF should provide a consolidated approach to supplier lifecycle management. For users of the CSF, having a separate Supply Chain Function would make the NIST CSF more user friendly. The CSF Core changes include many supply chain elements embedded throughout the other Functions, which introduces additional complexity with respect to implementation of third-party risk management.

Irrespective of whether NIST creates a separate function for supply risk management, CRI recommends that NIST create an easier way to identify all content related to supply chain risk management (e.g., tagging or a table) to enable organizations to quickly reference the NIST CSF for guidance.

(5) Future-Proofing

CRI recognizes that the financial services sector is more mature and highly regulated when compared to other sectors, and our view is that supply chain risk management will become an undeniable focus area for regulators across all sectors. In fact, supply chain risk management is already a key focus across the

U.S. Government - per the Cybersecurity and Infrastructure Security Agency (CISA), *"If vulnerabilities in the ICT supply chain—composed of hardware, software, and managed services from third-party vendors, suppliers, service providers, and contractors—are exploited, the consequences can affect all users of that technology or service.*[4]*"* Securing global supply chains is also a strategic objective in the recent *National Cybersecurity Strategy* released by the White House in March 2023.

Supply chain risk management is not simply a regulatory matter, it has become fundamental to sound cybersecurity hygiene practices and will continue to be so in the future. For the CSF to remain useful in the years to come, it is imperative that it not only includes and highlights the key areas of today but also of tomorrow as well.

Recognize the Three Lines of Defense Model as a Subcategory of the Roles and Responsibilities Category

CRI applauds NIST for including the Govern function in NIST CSF v2.0. As previously stated, elevating governance to its own function indicates to boards and senior leadership that they play a critical role in cybersecurity. CRI appreciates accepting previous recommendations for subcategories of the Govern function. We still recommend that NIST consider including subcategories for independent risk management, independent audit, and/or independent assessment.

Doing so is important because organizations are increasingly adopting, or being encouraged or required to adopt, these functions, which are consistent with the Three Lines of Defense Model (3LoD)[5]. The 3LoD outlines essential roles and duties for an organization's risk management framework, including:

- First Line of Defense (1LoD): The first line of defense lies with the business and process owners. Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. This consists of identifying and assessing controls and mitigating risks.
- Second Line of Defense (2LoD): The second line supports management to help ensure risk and controls are effectively managed. Management establishes these functions to ensure the first line of defense is properly designed, in place, and operating as intended.
- Third Line of Defense (3LoD): The third line of defense provides assurance to senior management and the board that the first- and second-lines' efforts are consistent with expectations. The main difference between this third line of defense and the first two lines is its high level of organizational independence and objectivity.

[4] CISA also notes that they are committed to working with government and industry partners to ensure that supply chain risk management is an integrated component of security and resilience planning for the Nation's infrastructure - https://www.cisa.gov/information-and-communications-technology-supply-chain-risk-management

[5] Three Lines of Defense Model definitions from Institute of Internal Auditors - https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

The 3LoD is a regulatory expectation across the financial services sector to ensure sufficient independence. However, the concept of 3LoD is applicable to any organization and can be leveraged by other sectors, particularly as other sectors are beginning to see increased scrutiny from regulatory agencies.

Finally, we have included additional, detailed suggestions and changes as Appendix III.

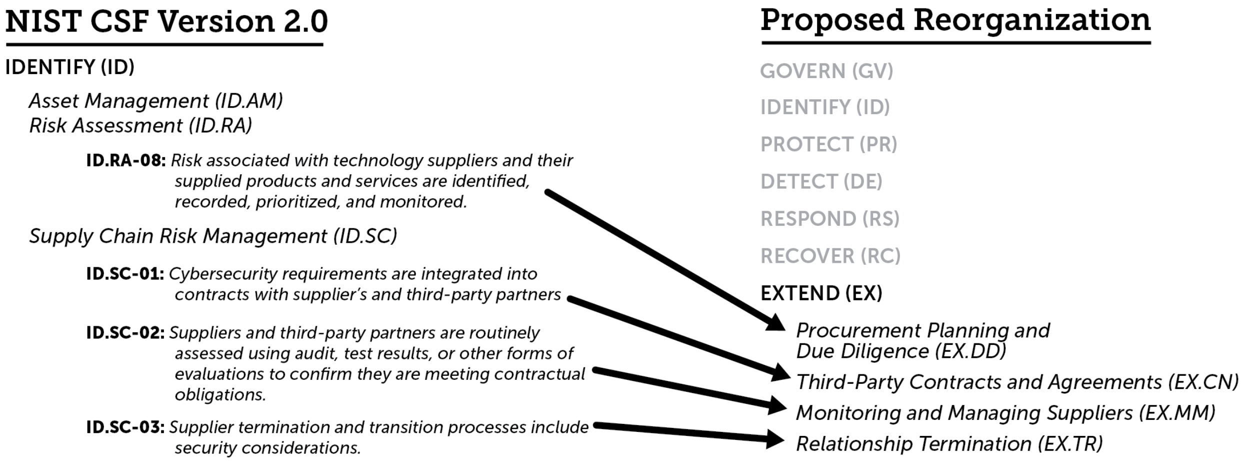
Thank you for the opportunity to respond to the NIST CSF v2.0 discussion draft. We recognize the tremendous effort to understand all viewpoints and balance competing priorities. Our 51 organizations represent all sections of the financial sector and believe strongly that supply chain risk management will remain a top-of-mind consideration for the foreseeable future. Without a supply chain function, the CSF risks not keeping pace with the ever-evolving cybersecurity landscape that practitioners are busy facing every day.

Thank you,

/S/

Josh Magri
President
Cyber Risk Institute (CRI)

Appendix I: Proposed Reorganization of Supply Chain/Third-Party Related Components into a 7th Third-Party Function called "Extend"



NIST CSF Version 2.0

IDENTIFY (ID)

Asset Management (ID.AM)
Risk Assessment (ID.RA)

ID.RA-08: *Risk associated with technology suppliers and their supplied products and services are identified, recorded, prioritized, and monitored.*

Supply Chain Risk Management (ID.SC)

ID.SC-01: *Cybersecurity requirements are integrated into contracts with supplier's and third-party partners*

ID.SC-02: *Suppliers and third-party partners are routinely assessed using audit, test results, or other forms of evaluations to confirm they are meeting contractual obligations.*

ID.SC-03: *Supplier termination and transition processes include security considerations.*

Proposed Reorganization

GOVERN (GV)

IDENTIFY (ID)

PROTECT (PR)

DETECT (DE)

RESPOND (RS)

RECOVER (RC)

EXTEND (EX)

Procurement Planning and Due Diligence (EX.DD)
Third-Party Contracts and Agreements (EX.CN)
Monitoring and Managing Suppliers (EX.MM)
Relationship Termination (EX.TR)

Appendix II: Detailed Description of the Third-Party Function, Categories and Subcategories

EXTEND (EX): Extend organizational risk management policy and practices over the lifecycle of third-party relationships, products, and services

Procurement Planning and Due Diligence (EX.DD): Planning and due diligence are performed to reduce risks before entering into a formal third-party relationship

EX.DD-01: Planning is performed for procurements and agreements that involve elevated risk to the organization

EX.DD-02: The organization performs thorough due diligence on prospective third parties, consistent with procurement planning and commensurate with the level of risk, criticality, and complexity of each third-party relationship

EX.DD-03: The organization assesses the suitability of the technology and cybersecurity capabilities and risk management practices of prospective third parties

EX.DD-04: Third-party products and services are assessed relative to business, risk management, and cybersecurity requirements

Third-Party Contracts and Agreements (EX.CN): Contracts establish baselines protections to manage risk over the life of the third-party relationship

EX.CN-01: Contracts clearly specify the rights and responsibilities of each party and establish requirements to address the anticipated risks posed by a third party over the life of the relationship

EX.CN-02: Expected cybersecurity practices for critical third parties that meet the risk management objectives of the organization are identified, documented, and agreed

Monitoring and Managing Suppliers (EX.MM): The risks posed by a third-party are monitored and managed over the course of the relationship

EX.MM-01: Critical suppliers and third parties are monitored to confirm that they continue to satisfy their obligations as required; reviews of audits, test results, or other assessments of third parties are conducted

EX.MM-02: Inter-dependent and coordinated cybersecurity risk management practices with third parties are managed to ensure ongoing effectiveness

Relationship Termination (EX.TR): Relationship termination is anticipated, planned for, and executed safely

EX.TR-01: The organization anticipates and plans for the termination of critical relationships under both normal and adverse circumstances

EX.TR-02: Relationship terminations and the return or destruction of assets are performed in a controlled and safe manner

APPENDIX III: Detailed Feedback on NIST CSF v2 Discussion Draft

Govern Function

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

2. ***Risk Management Strategy*** (**GV.RM**):

   The RM category talks to RM strategy, but only addresses RM processes in -07, where RM processes are "reviewed and adjusted." RM processes should be more explicitly addressed as they are a superset of risk assessment processes (ID.RA). Consider changing -01 to "risk management objectives and processes are established…". Also consider adding "and processes" to GV.RM-02 to define a supply chain risk program (not just a strategy). Perhaps consider changing the category to "Risk Management Strategy and Processes".

3. ***Risk Management Strategy*** (**GV.RM**):

   Consider adding a 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 projects. There are separate cyber risk management activities associated with these areas that aren't addressed elsewhere in the draft.

4. **GV.RR-03**: *Roles and responsibilities for customers, partners, and other third-party stakeholders are established and communicated*; and, **GV.RR-04**: *Roles and responsibilities for suppliers are established, documented in contractual language, and communicated*:

   There is some overlap between the reference to partners and other third-party stakeholders in -03 and suppliers specifically in -04. Consider deleting -04, and modifying ID.SC-03 to "Cybersecurity roles, responsibilities, and requirements are established and integrated into contracts with suppliers and third-party partners".

5. **GV.RR-05**: *Lines of communication across the organization are established for cybersecurity risks, including supply chain risks*:

   Consider: "Lines of communications and decision authorities across the organization…". Although "authorities" is mentioned under -06, the implication there seems to be related specifically to decisions around resourcing. Suggest tying decision-making to communications (two of the core elements of governance) as it more broadly addresses things like incident response decisions, etc.

6. **GV.RR-07**: *Cybersecurity is included in human resources practices (e.g., training, deprovisioning, personnel screening)*:

   Training is covered under PR.AT. Perhaps reference "hiring/retention", "changes in role", and/or "accountability and incentives" in this subcategory.

7. **GV.PO-02**: *The same policies used internally are applied to suppliers*:

   As currently worded, this proposed outcome appears untenable. For polices to be "applied," there needs to be some enforcement mechanism (i.e., policies without some means of enforcement or penalties are suggestions, not policies). The only enforcement mechanism for suppliers would be a contract. If a supplier is required to follow all of its customer organizations' (presumably, relevant) security policies by contract, they would likely be forced into the untenable position of being required to adhere to conflicting or inconsistent policies. Additionally, smaller suppliers might be unwilling or unable to comply with the more rigorous security policies of much larger and more mature customer organizations. Consider modifying to something similar to: "The security policy used to manage a supplier is commensurate with the risk to the organization of the supplier, its products, and its services."

Identify Function

8. **ID.AM-01**: *Inventories of physical devices managed by the organization are maintained*:

   Consider "physical and virtual devices…". There's a lot of confusion about how virtual devices should be addressed in inventories. Consider things allocated an IP address here, to include virtual devices, or explicitly include virtual devices under ID.AM-02 (software inventory).

9. **ID.AM-05**: *Assets are prioritized based on classification, criticality, resources, and organizational value*:

   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.

10. **ID-AM-07**: *Sensitive data and corresponding metadata are inventoried and tracked*:

    The word "tracked" is ambiguous in this context. What does tracking encompass beyond just inventorying? Should the outcome be tied more clearly to information privacy management expectations, or is it referring to possible Detect function monitoring of data?

11. **ID-RA.01**: *Vulnerabilities in first-party and third-party assets are identified, validated, and recorded*:

    Consider replacing "first-party" with "organizational" to be consistent with the category description and the rest of the document.

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

    While change management includes aspects of risk assessment, it includes many other activities designed to manage the potential risks; i.e., it is not inherently or primarily a risk assessment activity. Recommend moving it to PR.PS, just after configuration management.

13. **ID.RA-08**: *Risks associated with technology suppliers and their supplied products and services are identified, recorded, prioritized, and monitored*:

    As recommended above, the components of this outcome dealing with individual supplier, product and service due diligence should be moved to the ID.SC category (with the other supplier lifecycle management activities). If retained, this subcategory should focus on aggregate-level supply chain risk assessment.

14. **ID.RA-10**: *Exceptions to security measures are reviewed, tracked, and compensated for*:

    Consider "… are reviewed, risk-assessed, approved at appropriate levels, and tracked to closure". All too often security exceptions are accepted by people who don't/shouldn't have the authority to do so.

15. **ID.SC-04**: *Suppliers and third-party partners are routinely assessed using audit, test results, or other forms of evaluations to confirm they are meeting their contractual obligations*:

    Minor language point: "assessment" and "evaluation" are slightly different activities and have slightly different objectives. The words shouldn't be used interchangeably in the text.

16. **Improvements (ID.IM)**: *Improvements to organizational cybersecurity risk management processes and activities are identified*:

    Recommend including here or in the Govern function something more explicit about measurement, metrics, reporting, trending, benchmarking, KPIs, KRIs, etc.

17. **Improvements (ID.IM)**: *Improvements to organizational cybersecurity risk management processes and activities are identified*:

    All three subcategories "identify" improvements, but there is no call to consider, prioritize and implement improvements. Consider a Govern function activity relating risk management, improvements, and resource allocation.

<u>Protect Function</u>

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

    Strongly consider adding subcategories for privileged access management and service account management. These topics are too critical to be treated generically with other access types.

19. **PR.AA-04**: *Federated assertions are generated, protected, conveyed, and verified*:

    This subcategory seems a bit narrow in focus. Consider something a bit broader along the lines of: "Access credential and authorization mechanisms for internal systems and across security perimeters are designed to maintain security, integrity, and authenticity."

20. **PR.AT-01**: *Awareness and training are provided for users so they possess the knowledge and skills to perform relevant tasks*:

    Consider "undeleting" RS.CO-1 (into RS). Understanding roles and sequence of recovery is a critical special case for awareness and training.

21. **PR.DS-07**: *The development and testing environments are separate from the production environment (deleted)*:

    Consider "undeleting" segregating production and non-production environments or, better yet, address network environment segregation (esp. IT and OT networks, and internal versus external networks) more broadly. The concept of segregation is too important to just assume. See also PR.IR-02.

22. **PR.PS-02:** *Software is patched, updated, replaced, and removed commensurate with risk*:

    The subcategory conflates two different activities and objectives. Software patching is a more or less continuous process to address vulnerabilities. Updating, replacing, and removing software may also address vulnerabilities, but is a more controlled, planned, and managed effort more commonly pursued to provide new business capabilities and/or maintain vendor support. The latter might better be addressed as a part of a broader "application lifecycle management" activity. The two efforts are generally performed by different organizational units.

23. **PR.PS-04**: *Log records are generated for cybersecurity events 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, and log security requirements. This is a separate, but critical, part of log management that's distinct from generating the logs. Consider "system events" as "cybersecurity events" tends to imply only generating logs when a cyber event actually occurs (i.e., not just continuous "cybersecurity-relevant" events).

24. **PR.PS-06:** *Backups of platform software are conducted, protected, maintained, and tested*:

    This specific instance of backup type could be assumed to be included under PR.DS-11. If retained, however, consider "platform software and configuration files…"

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

    Consider addressing accurate and resilient time services. This is critical to logging, event analysis, forensics, transaction processing, etc.

26. **PR.IR-01**: *Response and recovery plans (e.g., incident response plan, business continuity plan, disaster recovery plan, contingency plan) are communicated and maintained*:

    ID.IM-02 is inadequate to cover recovery plan testing. This is a complete endeavor and set of activities in and of itself.

27. **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 really, really need to be explicitly referenced (could be in a parenthetical to this subcategory statement). These are fundamental security concepts. Periodic network device (e.g., firewall) configuration review should also be addressed.

28. **PR.IR-05**: *Adequate resource capacity (e.g., storage, power, network bandwidth, computing) to ensure availability is maintained*:

    Consider "Resource capacity is managed, and adequate capacity…"

Detect Function

29. **DE.CM-03:** *Personnel activity and technology usage are monitored to find adverse cybersecurity events*:

    In PR.AT, "personnel" is expanded to include "third parties." Is that the intent here?

30. **DE.AE-08**: *Adverse cybersecurity events are categorized and potential incidents are escalated for triage*:

    Triage typically includes categorization and prioritization, at least in a medical context: "the sorting of sick or injured patients according to their need for emergency medical attention." Incidents should be escalated for "potential response", not "triage". This subcategory should be rationalized with subcategories RS.MA-02 and RS.MA-03.

    Also, consider "categorized and summarized…" to capture the concept of a standard incident report.

31. **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, end-point, OT, and data.

Respond Function

32. **RS.MA-02**: *Incident reports are triaged and validated*; and **RS.MA-03**: *Incidents are categorized and prioritized*:

    See DE.AE-08. These subcategories should be deleted, combined, or otherwise disambiguated from DE.AE-08.

33. **RS.MA-04**: *Incidents are escalated or elevated as needed*; and **RS.MA-05**: *Criteria for initiating incident recovery defined and applied*:

    These subcategories are somewhat duplicative and could be combined.

34. **RS.AN-09**: *Incident status is tracked and validated*:

    This subcategory seems more appropriate under Incident Management (RS.MA).

35. **RS.CO-03**: *Information is shared with designated internal and external stakeholders, as required by law, regulation, or policy*:

    Consider "<u>Authorized</u> information is shared…"

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

    "Eradicated" seems a poor word choice. One cannot completely "eradicate" all records, logs, documentation, or lessons learned about incidents. Suggest 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.

    <u>Recover Function</u>

37. **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 done 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.

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

    The objective of this subcategory is unclear. Is the objective here to establish new operational norms or to verify that operations have returned to some defined state of pre-existing operational norm?

39. **RC.CO-01:** *Public relations are managed*; and **RC.CO-02:** *Reputation is repaired after an incident*:

    These activities would not appear to be within the scope of a cybersecurity or technology function.