Response to Final Draft NIST Cybersecurity Framework 2.0

01 November 2023

Presented by: Graeme Payne, Head of US Advisory Services
Contact: [redacted]

U.S. Corporate Headquarters
Kudelski Security
[redacted]

Kudelski Security is a leading cybersecurity company. We partner with our clients to enhance their cyber confidence, threat immunity and data protection through our comprehensive consulting, technology engagements, managed security services, and ability to innovate to create new capabilities.

With offices and labs in Switzerland, London, Spain, Germany, France, and the United States, we leverage a rich history of engineering and innovation to develop real solutions to our clients' toughest cybersecurity challenges.

Kudelski Security has been utilizing the National Institute of Standards and Technology's ("NIST") Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (commonly referred to as the Cybersecurity Framework ("CSF") as a reference framework for the delivery of our advisory services and managed detection and response services. We have conducted an extensive number of assessments leveraging the NIST CSF framework and use it to help build and mature cybersecurity programs.

In response to the *NIST Public Draft: The NIST Cybersecurity Framework 2.0* and *Discussion Draft: The NIST Cybersecurity Framework 2.0 Core with Implementation Examples* both released on August 8, 2023, Kudelski Security offers the following feedback. Our comments are based on our practical and applied experience of utilizing the NIST CSF v1.1 framework.

1. FEEDBACK ON NIST PUBLIC DRAFT: THE NIST CYBERSECURITY FRAMEWORK 2.0

1.1 Does the draft revision address organizations' current and anticipated future cybersecurity challenges, is aligned with leading practices and guidance resources, and reflects comments received so far?

NIST's structure of providing the CSF 2.0 Core and separate "Implementation Examples" is a logical approach and consistent with a typical organization's governance structure. The "Core" is like a policy document, which is typically updated on a less frequent basis, while the "Implementation Examples" are like the procedures or guideline documents that are not formally authorized and can be updated more frequently to address ongoing changes to the industries' threat landscape.

The addition of guidance for "Governance" is a logical addition, like what the CMMC/AB has attempted to prescribe in the CMMC framework. In Kudelski Security's assessments leveraging NIST CSF 1.1, we added the concept of Governance, so the formal addition in this version is welcome.

Another positive outcome is the way CSF 2.0 explains the Tiers. With a more straightforward explanation of how the tiers can be leveraged, the use of tiers can be more actionable. In the past, we have observed many organizations only partially adopted CSF 1.1. The categories and subcategories were generally adopted but most organizations we worked with did not adopt the

tier model. We feel with this updated guidance, we can better support the full CSF implementation.

1.2 How to present the modification from CSF 1.1 to CSF 2.0 to support the transition

Appendix C of the document presents Functions, Categories, and Subcategories of the Framework Core. We believe this presentation which shows categories and subcategories that have been combined, dropped, or moved provides a good mapping to help in transitioning from CSF v1.1 to CSF v2.0.

Retaining the number reference for subcategories from CSF v1.1 also provides traceability but over time may be confusing as certain subcategories will not be used. For example, DE.AE will have six subcategories (DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08) with DE.AE-01 and DE.AE-05 being “not used”. We believe this is better than renumbering the subcategories in CSF 2.0 which would be more confusing and require additional mappings.

We would recommend the unused subcategory numbers be “retired” and any future new subcategories would be added to the number sequence rather than using an “unused” subcategory.

1.3 Improvements for the draft document

One of the objectives of the CSF 2.0 Core was to provide more guidance around cybersecurity measurement and assessment. The guidance related to the development of current state and target profiles is sound and will be helpful in the development of organizational and industry-specific profiles.

The Framework Tier guidance has been improved from CSF v1.1 but remains lacking in providing a clear description of how Framework Tiers can be used to assess the maturity of an organization’s cybersecurity program. More specifically the Tier concept is not aligned with the Functions, Categories, and Subcategories. This view was expressed by several respondents in comments on the CSF 2.0 Concept Paper.

Organizations want to be able to benchmark their security program capabilities against the CSF framework. Without a common framework security consulting and advisory firms have developed their own proprietary models often based on the CMMI process maturity framework.

We encourage NIST to develop specific guidance to help provide for common assessments against CSF 2.0.

2. FEEDBACK ON DISCUSSION DRAFT: THE NIST CYBERSECURITY FRAMEWORK 2.0 CORE WITH IMPLEMENTATION EXAMPLES

2.1 Concrete Improvements to the Examples

The following table provides our feedback on specific improvements that can be made to the Examples. The table below notes the page reference of the category/sub-category to which the feedback applies. For feedback on existing examples, the Example Reference is provided. Where there is no Example Reference, the feedback represents additional examples that could be added.

Page No.	Category	Subcategory	Example Reference	Feedback on Implementation Examples
2	GV.OC	GV.OC-02	Ex1	Clarify: Expectations from the Board of Directors should be sought as well
3	GV.OC	GV.OC-04	Ex3	Recovery time objectives are only one piece of resilience objectives. Consider expanding or updating the example to include business continuity, disaster recovery, or contingency processing objectives.
4	GV.RM	GV.RM-01	Ex2	The example could be expanded to include other areas of risk management, such as measurable objectives for the risk register.
4	GV.RM	GV.RM-03		Identify longer-term and emerging technology and cybersecurity risks
4 **14** **15** **24**	GV.RM ID.AM ID.AM PR.DS	GV.RM-04 ID.AM-05 ID.AM-07 PR.DS-02	Ex1 Ex3 Ex2	A definition of classification of data should be included within this document, with informative references. There is a lot of confusion around the classification of data, and how to develop policies, standards, and processes.
5	GV.RM	GV.RM-05	Ex1	Include the Board of Directors
5	GV.RM	GV.RM-06		Perform risk assessments when new infrastructure or technology is introduced to identify cybersecurity risks
6	GV.SC	GV.SC-02		The terms “roles” and “responsibilities” should be clarified. Often these terms get mixed up with job descriptions.
8	GV.SC	GV.SC-05		Specify in contracts the requirement to notify when a security breach of the supplier’s systems occurs or is identified
8	GV.SC	GV.SC-05		Contractually require suppliers to securely dispose of retained data or otherwise verify that data is no longer accessible

Page No.	Category	Subcategory	Example Reference	Feedback on Implementation Examples
10	GV.RR			Strengthen the wording to say Board of Directors. This is often confusing, as some have interpreted the past CSF to not include the Board of Directors
10	GV.RR	GV.RR-01		Establish a process for reporting on cybersecurity risks including escalation procedures
11	GV.RR	GV.RR-02		Define and communicate the role and responsibilities of users and employees in identifying and reporting potential cybersecurity risks
11	GV.RR	GV.RR-02		The roles and responsibilities of suppliers and other third parties for identifying and reporting cybersecurity risks are identified and incorporated into relevant agreements
11	GV.RR	GV.RR-04	Ex2	Change to: Embed cybersecurity knowledge requirements or incentives in hiring, training, and retention discussions
12	GV.PO			This section references Policies, Processes, and Procedures, however, it only alludes to a risk management policy. What about other policies? In addition, it appears to use the term policy broadly, and does not reference the need for standards that should be between policies and procedures.
14	ID.AM	ID.AM-02		Monitor the use of software to ensure compliance with usage restrictions (e.g., deployment restrictions)
14	ID.AM	ID.AM-03		Data flows between applications (both business and operating) should be maintained.
15	ID.AM	ID.AM-08		Identify legacy systems (e.g., those no longer supported by vendor) that could increase the organization's risk profile
15	ID.AM	ID.AM-09		Implement secure disposal methods for removal of systems when they reach the end of the lifecycle
16	ID.RA	ID.RA-01		Utilize secure posture management solutions to provide ongoing identification of vulnerabilities and misconfigurations
18	ID.RA	ID.RA-08		Utilize Information Sharing and Analysis Centers (ISAC) and other cybersecurity data sharing entities for information on vulnerabilities

Page No.	Category	Subcategory	Example Reference	Feedback on Implementation Examples
19	ID.IM	ID.IM-03		Conduct incident postmortem reviews and adjust processes based on lessons learned
21	PR.AA	PR.AA-02		Maintain an inventory of service accounts
21	PR.AA	PR.AA-03		Enforce strong authentication for privileged access roles (e.g., one-time passwords)
21	PR.AA	PR.AA-04		Utilize secure password vaults for specialized roles and identities
21	PR.AA	PR.AA-04		Utilize approved identity providers to validate user identities based on required level of identity assurance
22	PR.AA	PR.AA-05		Utilize access roles or groups to manage common access to systems
22	PR.AA	PR.AA-05		Utilize human resource changes (e.g., joiner, mover, leaver) to automate changes in access permissions
22	PR.AA	PR.AA-06		Periodically review physical access permissions.
22	PR.AA	PR.AA-06		Log access to sensitive areas (e.g., data center, human resources)
23	PR.AT	PR.AT-01	Ex4	Test users' cybersecurity awareness (e.g., require minimum scores in user awareness tests)
23	PR.AT	PR.AT-01		Provide a hotline for users to report security incidents or suspicious activity
23	PR.AT	PR.AT-01		Train users on acceptable data handling practices, including sanctioned storage locations, privacy, and retention requirements, and when and how to apply encryption to data.
24	PR.DS	PR.DS-01	Ex4 & 5	Provide examples of removable media (e.g., USB drives, tape, external hard drives).
24	PR.DS	PR.DS-02		Provide users with real-time warnings of possible data handling violations
25	PR.DS	PR.DS-09		Periodically identify and remove aged or stale data
25	PR.DS	PR.DS-10		Utilize tokenization or masking techniques to protect sensitive data from observability
25	PR.DS	PR.DS-11	Ex 2	Change to: Test backups and restores for all types of data sources at regular intervals based on its criticality
25	PR.DS	PR.DS-11		Use data replication services to ensure continuous availability of critical data
28	PR.PS	PR.PS-05		Restrict access to open-source software libraries

Page No.	Category	Subcategory	Example Reference	Feedback on Implementation Examples
28	PR.PS	PR.PS-05		Scan code contained in software repositories for vulnerabilities
28	PR.PS	PR.PS-05		Maintain check-out/check-in controls over shared software libraries
28	PR.PS	PR.PS-05		Validate code composition software bill of materials (SBOM) prior to deployment into production environments
28	PR.PS	PR.PS-06		Create and maintain software bill of materials (SBOM) for organization-developed software
30	DE.CM	DE.CM-02		Monitor remote installations containing sensitive industrial control systems
30	DE.CM	DE.CM-03	Ex1	Use behavior analytics to detect anomalous user activity (e.g., policy violations, use of unsanctioned data stores) to mitigate insider threats
31	DE.CM	DE.CM-09		Identify critical systems that are not being monitored and develop plans to implement monitoring or compensating controls (e.g., network isolation)
32	DE.AE	DE.AE-04	Ex2	Change to: Employ a framework to estimate impact and scope (e.g., using downtime impact, asset valuation, and public perception / brand impact)
32	DE.AE	DE.AE-06		Create and maintain automated response playbooks for defined incidents
33	RS.MA			Metrics and measures of incident management should be added.
34	RS.MA	RS.MA-02		Assess the potential financial impact of an incident to determine escalation and disclosure requirements
34	RS.MA	RS.MA-04		Escalate potentially material incidents to internal stakeholders (e.g., legal, Board of Directors) for disclosure to appropriate authorities
35	RS.AN	RS.AN-03		Conduct interviews and analysis to validate incident's attributed to insider threat
35	RS.AN	RS.AN-08		Costs and impacts of the incident are tracked and monitored
36	RS.CO	RS.CO-02		Notify senior management and other internal stakeholders in accordance with organizations incident communication protocols
39	RC.CO	RC.CO-04		Update regulatory filings and notifications

2.2 Whether the Examples are written at an appropriate level of specificity and helpful for a diverse range of organizations

We believe the implementation examples are written at the appropriate level of specificity to be able to be used as a tool to help implement CSF 2.0.

As we discussed above, we believe there is opportunity to develop additional guidance related to assessment and measurement of an organization's security capabilities against the NIST CSF Framework. One approach to this guidance would be to align specific Implementation Examples with different levels of capability maturity.

As an example, for NIST CSF 2.0 **PR-DS-11: Backups of data are created, protected, maintained, and tested** the following Implementation Examples could be mapped to the applicable Tier levels.

TIER 1 – PARTIAL	TIER 2 – RISK INFORMED	TIER 3 – REPEATABLE	TIER 4 – ADAPTIVE
• Backups are conducted on an ad-hoc basis across the organization (e.g., manually with little or no maintenance or testing).	• A documented backup policy or standard exists • Continuously back up critical data in near-real-time and back up other data frequently at agreed-upon schedules. • Securely store some backups offline and offsite so that an incident or disaster will not damage them	• Documented backup policies, standards and procedures exist and are consistently implemented. • Continuously back up critical data in near-real-time and back up other data frequently at agreed-upon schedules. • Test backups and restores for all types of data sources based on data criticality.	• Documented backup policies, standards and procedures exist and are consistently implemented. • Continuously back up critical data in near-real-time and back up other data frequently at agreed-upon schedules. • Test backups and restores for all types of data sources based on data criticality. • Backup/restore procedures are integrated with other security processes (e.g., DR, incident response and security monitoring). • Automated tools monitor the backup process and send alerts on status of backup jobs.

TIER 1 – PARTIAL	TIER 2 – RISK INFORMED	TIER 3 – REPEATABLE	TIER 4 – ADAPTIVE
			• Metrics and measures are generated to report on the effectiveness of the process. • Automated backup tools sense when backup issues arise and automatically correct. • Backup and restore processes and tools are continuously tested and evaluated. • Processes and tools are updated when changes occur in the business, technology, or threat environment.

For the initial deployment of NIST CSF 2.0 we recommend that the current Implementation Examples be used (with appropriate updates based on feedback). NIST should then work on developing additional guidance to build out Implementation Examples for each Tier level as shown in the Example above.

2.3 What other types of Examples would be most beneficial to Framework users?

We have included some specific recommendations in Section 2.1 above.

2.4 What existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks)?

There are a broad range of open frameworks and standards that could be used as sources of implementation guidance. NIST should consider among others the following:

- NIST Standards and Guidelines, including NIST SP 800-53, NIST SP 800-171, NIST 1800 series. NIST 800-82

- NICE Framework
- ISO 27000 series, ISO 28000, ISO 29147
- COBIT
- CIS Controls
- PCI-DSS
- Cloud Security Alliance Cloud Control Matrix
- CMMC
- Cyber Essentials
- ISA/IEC 62443
- ENISA National Capabilities Assessment Framework
- ETSI Critical Security Controls for Effective Cyber Defence
- ISF Standard of Good Practice for Information Security
- IoT Cybersecurity Alliance
- IoTSF Security Compliance Framework
- MITRE ATT&CK
- NCSC Cyber Assessment Framework

2.5 How often Examples should be updated?

We believe an annual update to the examples would be an appropriate timeframe.

2.6 Whether and how to accept Examples developed by the community?

We believe the cybersecurity community should be able to recommend Implementation Examples and Informative References to NIST for consideration and inclusion in the NIST Cybersecurity and Privacy Reference Tool (“CPRT”).

We believe NIST should review the submissions for applicability and relevance before incorporating them into the CPRT. A set of evaluation criteria could be developed to assist in this review. For example, the criteria for evaluation of Implementation Examples might include:

- Does the example represent a common practice?
- Is the example relevant to the category and subcategory?

- Is the example applicable across a range of organizations (e.g., government, private sector, not-for-profit organizations)?
- Is the example not specific to an industry sector? (Industry specific examples should be included in community profiles)
- Is the example not reliant on a specific technology vendor solution? (Classes of technology should be considered rather than specific vendor solutions)