NIST CSF 2.0 Core with Implementation Examples – Schellman Feedback

Schellman is providing feedback to NIST on the following areas of requested input:

Concrete Improvements to the Examples

Note: Content in red font in the table below added by Schellman.

#	Example	Improvement
01.	**GV.OC-01** **Ex1**: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) with senior leadership, risk owners, and other stakeholders to provide a basis for identifying risks that may impede that mission
02.	**GV.OC-05** **Ex2:** Identify and document external dependencies that are potential points of failure for the organization's critical capabilities and services	Identify, document, and communicate with internal cybersecurity risk management personnel, the external dependencies that are potential points of failure for the organization's critical capabilities and services Further, providing a risk ranking/prioritization of the dependencies will allow for a more detailed response plan
03.	**GV.RM-01** **Ex3:** Senior leaders agree about cybersecurity objectives and use them for measuring and managing risk and performance	Senior leaders agree about cybersecurity objectives and use them for measuring (quantitatively and qualitatively) and managing risk and performance Further, the cybersecurity objectives are documented and reviewed on an organization defined cadence (e.g., annually)
04.	**GV.RM-05** New Example	Determine how the organization will reassess and communicate with internal stakeholders regarding changes in risks posed by suppliers and other third parties
05.	**GV.RM-06** **Ex1:** Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas	Establish criteria for using a quantitative approach (e.g., Monte-Carlo scenarios, FAIR model, etc.) to cybersecurity risk analysis, and specify probability and exposure formulas
06.	**GV.RM-06** **Ex3:** Establish criteria for risk prioritization at the appropriate levels within the enterprise	Establish criteria for risk prioritization and ownership at the appropriate levels within the enterprise

#	Example	Improvement
07.	**GV.RM-07** New Example	Apply the same quantitative approach to cybersecurity risk management for positive risk evaluation and factor as a component of product or service pricing considerations (risk premium)
08.	**GV.SC-02** New Example	Provide cybersecurity training to suppliers, customers, and partners when interacting with critical organization systems that align with the risk ranking/prioritization developed and defined internally.
09.	**GV.SC-05** New Example	Include a “right to audit” in contracts with suppliers or other relevant third parties supporting or providing critical systems, assets, or services
10.	**GV.RR-01** New Example	Senior leadership, risk owners, and other stakeholders is required to complete cybersecurity and risk management training
11.	**GV.RR-02** New Example	Enforcement of cybersecurity responsibilities includes disciplinary actions for failure to perform assigned cybersecurity responsibilities up to and including termination
12.	**ID.AM-07** **Ex1:** Maintain a list of the designated data types of interest (e.g., personally identifiable information, protected health information, financial account numbers, organization intellectual property)	Maintain a list of the designated data types of interest (e.g., personally identifiable information, protected health information, cardholder data, customer managed data, financial account numbers, organization intellectual property) and identify if the data is permitted to cross international borders. Further, formally review this list on a Quarterly basis.
13.	**ID.AM-08** New Example	Assign end of life systems to a designated system owner who is responsible for ensuring system vulnerabilities and other cybersecurity considerations are addressed and logs are maintained for actions taken.
14.	**PR.DS-11** **Ex4:** Enforce geolocation restrictions for data backup storage	Enforce geolocation restrictions and geographical separation for data backup storage
15.	**PR.PS-01** New Example	Perform monitoring for drift from the organization’s approved hardened baseline configuration
16.	**PR.PS-04** New Example	Configure log storage access security architecture and settings to ensure nonrepudiation of logged data (i.e., no access for users responsible for managing the logged system (separation of responsibilities), and read-only access for auditors)

#	Example	Improvement
17.	**PR.IR-01** **Ex3:** Implement zero trust architectures to restrict network access to each resource to the minimum necessary	Implement zero trust architectures to restrict network access to each resource to the minimum permissions necessary (i.e., fine-grained permissions, need to know permissions)
18.	**DE.AE-04** **Ex2:** A person creates their own estimates of impact and scope	A person creates their own qualitative (for rapid assessment, less complex) or quantitative (when less time sensitive, more complex) estimates of impact and scope
19.	**RS.MA-02** **Ex2:** Apply criteria to estimate the severity of an incident	Apply criteria to estimate the severity of an incident and identify which incident playbook to use

Whether the Examples are Written at an Appropriate Level of Specificity and Helpful for a Diverse Range of Organizations

The examples are generally written at an appropriate level of specificity; however, they do not seem to address an enterprise wide NIST CSF assessment supporting the oversight of several hundred systems and multiple business units with diverse reporting lines. In an enterprise-wide assessment the implementation examples should also help answer with respect to each subcategory: How does the organization identify key cybersecurity functions, measure those functions, monitor the effectiveness of the functions, and adjust strategies in light of the performance of the organization's cybersecurity functions?

What Other Types of Examples Would Be Most Beneficial to Framework Users

Framework users would also benefit from:

- Defining foundational examples (or where to start)
- Examples specific to the Profiles found in Internal Reports that overlay their requirements on top of the NIST CSF (e.g.IR 8183, IR 8374, IR 8441, IR 8473, etc.)
- Refreshed mappings to industry best practice standards (i.e., ISO 27001:2022, SOC 2, etc.)
- Additional implementation guidance on how to meet the Cybersecurity Disclosure Rule

What Existing Sources of Implementation Guidance Might Be Readily Adopted as Sources of Examples (Such as the NICE Framework Tasks)

No recommendations.

How Often Examples Should Be Updated

Examples should be updated every one to two years.

Whether and how to Accept Examples Developed by the Community

Examples developed by the community should be accepted. If possible, the example could be denoted as Community Developed, until there has been time to fully validate the applicability of the example. Further,

an up or down vote system open to the community could allow for a free market of feedback such that Framework users could make a decision for themselves about whether the Example was particularly useful.