SAP America, Inc.
[redacted]
info@sap.com

Via Electronic Mail

November 6, 2023

Laurie Locascio
Director
National Institute of Standards and Technology
[redacted]

RE: SAP Response to the Discussion Draft of the NIST Cybersecurity Framework Core 2.0 with Implementation Examples

Director Locascio:

SAP appreciates the opportunity to submit comments in response to the *discussion draft of the NIST Cybersecurity Framework (CSF) 2.0 with core implementation examples*. Overall, SAP is pleased with the agency's continued engagement and collaboration with the public and private sectors in the enhancement of this framework.

SAP is the world's largest enterprise software provider. Since our establishment over 50 years ago, we are helping companies of all sizes and in all sectors run at their best. We operate in over 150 countries and have over 110,000 team members worldwide. Our core mission is to help the world run better and improve people's lives. SAP customers generate 87% of total global commerce (or $46 trillion annually), and 99 out of the 100 largest companies in the world run SAP software.

We believe SAP is uniquely suited to provide NIST with insights into the opportunities and challenges associated with the implementation of the NIST CSF 2.0. Due to the diversity of the customer baseline and the increasingly complex regulatory environment, SAP decided to implement the NIST CSF 2.0 and make it a key priority and strategic goal.

We share the agency's concerns about the evolving cyber threat landscape as well as its impacts on individuals and organizations. SAP supports the development of swift and constructive frameworks by NIST to strengthen baseline cybersecurity, but we encourage NIST to examine existing international frameworks and standards to avoid duplication and foster harmonization.

In closing, SAP encourages NIST to continue engagement and gaining feedback as the agency finalizes the CSF 2.0 by conducting workshops, industry roundtables, or leveraging conferences and forums such as SAP SAPPHIRE - the world's largest cloud and business technology event - to engage with thousands of companies regarding the adoption of the framework. We hope that SAP's recommendations support the advancement of positive change that leads to a more secure nation. Thank you again for the opportunity to engage in the development of this framework. We look forward to collaborating more with NIST. For any questions, please contact Ms. Vanessa Barber in SAP Global Security and Compliance (SGSC) at Vanessa.Barber@sap.com.

Respectfully Submitted,

Daniel Fryer
Head of Security Policy, Standards & Frameworks
Enclosure

PUBLIC

NIST Cyber Security Framework (CSF) Draft Version 2.0 (Core) Feedback

Copyright

Original document

The original version of this document shall be stored in the Corporate Portal.

Organization of documents

All hard copies of documents represent a copy of the corresponding original document. Only the original is kept up to date. The maintenance and archiving of documents are governed:

Author(s)

Vanessa Barber
Chief Information Security Compliance Expert
SAP, Global Risk, Compliance and Security

History

Version	Status	Date	Change Description
1.0	Final	11/03/2023	Published

INTRODUCTION

We appreciate the opportunity to provide feedback on NIST's Discussion Draft of the Cybersecurity Framework (CSF) 2.0 Core (hereafter NIST CSF 2.0). SAP has made it a strategic priority to align to the NIST Cybersecurity Framework and will continue to invest in the NIST CSF 2.0.

Due to the diversity of the customer baseline and the increasingly complex regulatory environment, SAP decided to implement the NIST CSF 2.0 and make it a key priority and strategic goal. Below are key reasons for this decision:

- The Framework is outcome-driven and does not mandate how an organization must achieve those outcomes. SAP can therefore enhance already existing cybersecurity activities and has the option to align already existing certifications and attestations to the informative references. This allows for a one framework view of all risks and security controls independent of source.

- The Framework is aligned to Special Publications from the NIST organization that offers a key set of implementation options originally based on the need for secure critical infrastructure.

- The Framework provides a common terminology and methodology for managing cybersecurity risk to communicate with stakeholders inside and outside of the company.

- The Framework leverages the simplified language of cybersecurity risk with target profiles and implementation plans which can be leveraged in prioritizing cybersecurity improvement activities and enabling investment decisions to address gaps.

- The Framework helps guide key decision points about risk management activities through the various levels of an organization from senior executives to business and process level, to implementation and operations.

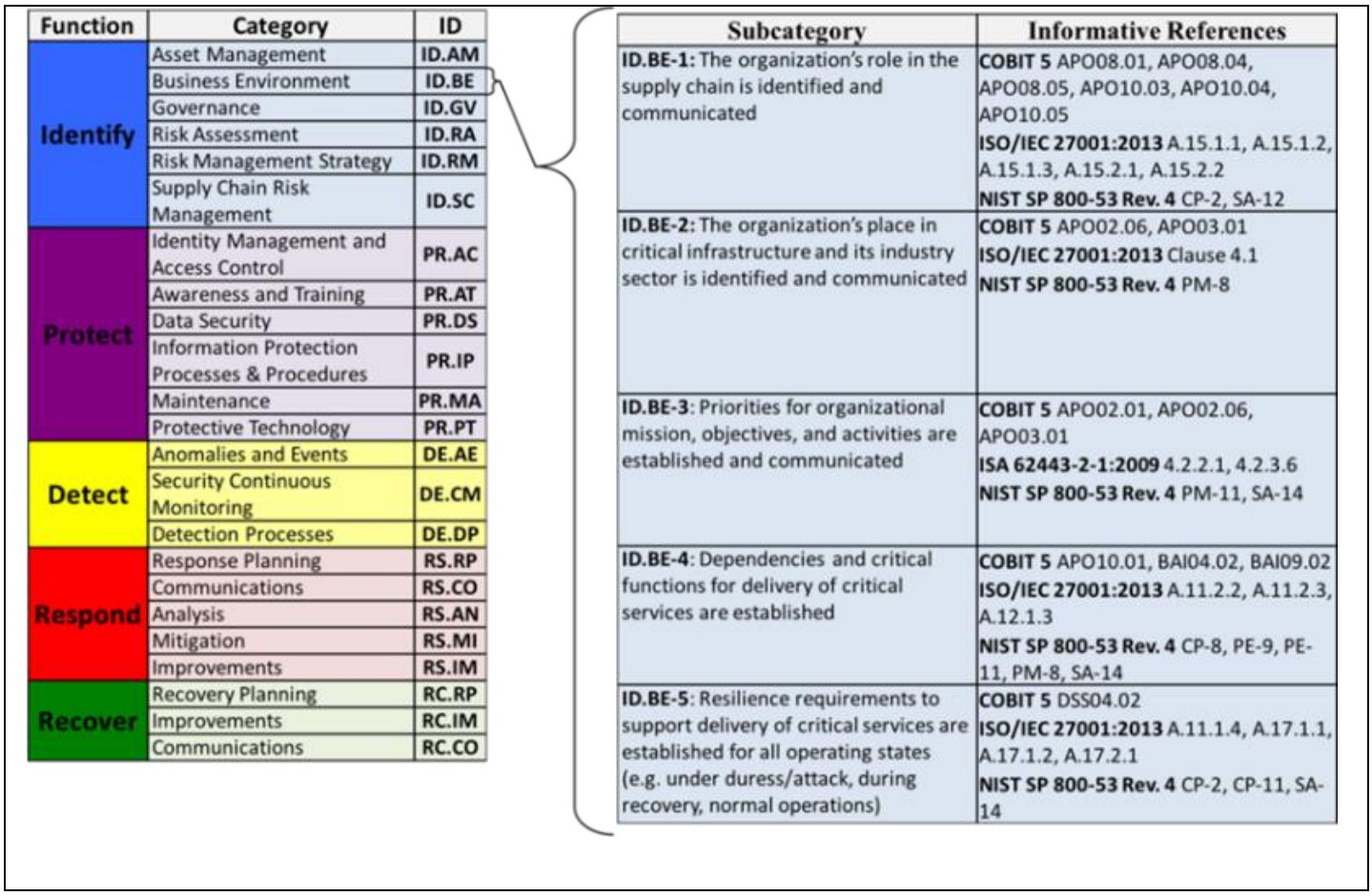
1. PURPOSE

TOPIC	OBSERVATION	RECOMMENDATION
1.1 Clarifying the Purpose	• NIST CSF 2.0 is not a compliance framework. With the understanding that the implementation examples and the informative references are vital to assist organizations needing guidance, it is important to note that there is a lot of misunderstanding about the NIST CSF 2.0 Core being a compliance framework. • This detracts from the point that the that the NIST CSF Core 2.0 should act as a useful starting point for reducing cybersecurity risk. In other words, it was not intended to provide organizations with a checklist of actions necessary to meet desired cybersecurity outcomes.	• NIST may consider re-emphasizing that the NIST CSF 2.0 provides a high-level structure for managing risks. • NIST may also emphasize that the NIST CSF 2.0 is a good starting point for small to medium businesses and for companies such as SAP the NIST CSF 2.0 provides the ability to align multiple compliance frameworks under one umbrella to manage cyber risk. The NIST CSF is therefore scalable.

2. MAPPINGS & INFORMATIVE REFERENCES

TOPIC	OBSERVATION	RECOMMENDATION
2.1 Depictions of Mappings	• Despite the emphasis on governance, there is a lot of misunderstanding among the consulting and compliance communities which causes intense discussions about mappings of security controls. The introduction of the implementation examples may further exacerbate this misunderstanding and lead to mappings from implementation examples to and from informative references which may/may not add value and might further complicate any understanding of the NIST CSF 2.0. • An illustrative example is Figure 1 below. It awakens multiple suppositions that the informative references are either check-box security controls, are equal to, or that all are required to be compliant. This misunderstanding may also be further endorsed by implementation examples, which may awaken the impression that if the examples are implemented then the organization is compliant.	• To facilitate a better understanding of the framework, NIST may consider specifically showing the relationship between the risk and the informative reference (security control). • A more generic image which might make the intent clearer is depicted in Figure 2. This shows the relationship between framework elements with a more simplistic view of the relationship within the NIST CSF 2.0 and additional guidance. • Specifically, Figure 2 below provides a simplified view of the relationship between risks, implementation examples, and informative references that may address the issue with the current depiction in Figure 2.
2.2 Identification of dependencies when updating informative references	• Although there are relationships shown in the Informative references there is no clear taxonomy of the dependencies.	• While understanding that the NIST Special Publication SP 800-55, Performance Measurement Guide for Information Security and the NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations may have been prepared by other responsible parties than the NIST CSF 2.0 owners, the usage might be simplified by identifying core dependencies and then scheduling updates by determining the criticality of the documentation. The publications are currently not synchronized. • This would improve consistency across information references for readers/users of the NIST CSF 2.0.

Comparing Mappings (Current vs. Proposed)



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 1. Illustration showing the relationship between Function, Category, Subcategory, and Information Reference.

Function	Category	ID	Sub-Category	Reference	Risk	Implementation Example	Informative Reference
Identify	Asset Management	ID.AM	ID.AM-1: Inventories of hardware managed by the organization are maintained	ID.AM-1	Risk Example: Failure to manage an IT hardware asset register may result in security risks due to unauthorized access, data breaches, and loss of confidential information. Without a complete and up-to-date record of IT hardware, it may be difficult to identify vulnerable endpoints or to track device usage. …	Ex1: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices. Ex2: Constantly monitor networks to detect new hardware and automatically update inventories.	**CIS** CSC 1 **COBIT 5** BAI09.01, AI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
			ID.AM-2: Inventories of software, services, and systems managed by the organization are maintained	ID.AM-2	Risk Example: Failure to manage an IT software asset register can result in legal and financial risks due to non-compliance with licensing agreements. Without an accurate and comprehensive record of software assets, it may be difficult to track licenses, determine usage rights, or identify duplicate software installations. …	Ex1: Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services. Ex2: Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes. Ex3: Maintain an inventory of the organization's systems.	**CIS** CSC 2 **COBIT 5** BAI09.01, AI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
			ID.AM-3: Representations of the organization's authorized network communication and internal and external network data flows are maintained (formerly ID.AM-03, DE.AE-01)	…	…	…	…
			…		…	…	..
	Risk Assessment	ID.RA					
	Improvement	ID.IM					

Figure 2. Simplified view of the relationship between risks, implementation examples and informative references.

3. FUNCTIONS

TOPIC	OBSERVATION	RECOMMENDATION
3.1 Overall Framework Balance	• Although the balance of the Functions and Categories has been improved there is still room for consideration for better balance.	• The new Governance function may be overloaded and/or needs operation outcomes defined in the other 5 categories. See more specific feedback in 3.3. • The Detect and Recover Functions are underbalanced with only 2 Categories. • Detect could be part of the Identify Function.
3.2 Respond & Recover functions	• The "Respond" function is reminiscent of a process more than any of the other functions. This serves it well as repositories. It helps create a flow that does not exist within any of the other functions. • The "Recover" function includes "Incident Mitigation", but the tabular form suggests a break.	• The solution might be to portray the "Respond" function and the "Recover" function as follows: o Recover function: The "Recover" function is comparatively short but is a run on from the "Respond" function from NIST CSF v1.1. o The title for "Recover", RC.RP Category references the execution of a plan which has not been mentioned in a category title before. o This could be solved by changing the title to "*Incident Recovery Execution*", or "*Incident Recovery*" or to avoid the re-use of the function title maybe "*Post incident re-build*".

TOPIC	OBSERVATION	RECOMMENDATION
3.3 Addition of the Govern function	• SAP supports the addition of a new Govern Function in the NIST CSF 2.0 Core. This new Function reflects the importance that governance plays in organizations' cybersecurity risk management practices and recognizes that profound changes are evolving in the cybersecurity arena. This includes but is not limited to the explosive increase in the number of cyber threats, the security risks related to accelerated global connectivity, and advances in technology such as Artificial Intelligence. To-date there has been reliance on information technologies and industrial control systems which have made cybersecurity a major source of enterprise risk (including business interruption, breach of privacy, and financial losses). • The Govern Function is an attempt to address these changes, by elevating the importance of governance. It also helps the simplification in messaging and communication with the core business by ensuring that cyber risk as a consideration for senior leadership, on par with legal, financial, and other sources of enterprise risk.	• **Improvement Category.** Elevating the Improvement Category from the Identify Function to the Govern Function would allow for the Improvement Category to be applied to all the other Functions and Categories. • Improvements are organizational cybersecurity risk management processes, procedures, and activities which are identified across all Framework Functions. As the draft also updates the implementation tiers definition and now includes factors like cybersecurity risk governance, cybersecurity risk management, and third-party cybersecurity risks, this also underscores a shift to a more holistic approach which might be better placed on the Govern Function. • Breaking the improvement into strategy and assessment would allow for the assessment portion to remain under the Identify Function. • There is also an opportunity to divide meaning of continuous (monitoring) and continual (audits) into the Govern Function and the Identify Function respectively. This would also align with ISO terminology and be semantically correct. • **Supply Chain Risk Management.** At a broad level, risk management is covered by introducing the Govern function GOVERN for the risk strategy under the category GV.RM. Risk Assessment is covered in the ID.RA category. • We understand that the NIST explicitly decided against adding a seventh function focused on Supply Chain Risk Management, CSF 2.0 provides additional details on third- party risk, integrates supply chain guidance into the new governance function, and provides that cybersecurity risk in supply chains should be considered as an organization performs all framework functions (not just governance). With the wording "Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle" we believe you might agree that inherently Supply Chain Risk Management is part of Risk Management. It is a type of risk. Elevating it to its own category might be in reaction to ongoing discussions about risk levels relating to this subject. A solution might be to divide the categories into RM and RA depending on the intent (strategy or assessment).

4. IMPLEMENTATION EXAMPLES

TOPIC	OBSERVATION	RECOMMENDATION
4.1 Implementation Examples	• A notable facet of the draft NIST CSF 2.0 is the comprehensive guidance it offers for implementation for smaller companies. • This iteration provides a wealth of "Implementation Examples" offering practical insights into how the NIST CSF 2.0 categories can be achieved via action-oriented examples (e.g., “Assign data classifications to designated data types through tags or labels”).	• Like the informative references, it would be beneficial NOT to show implementation examples in a tabular form but rather in a dynamic form using a tool which aligns them with profiles and security controls which can be selected wherever the fit is appropriate.

5. PROFILE TEMPLATES

TOPIC	OBSERVATION	RECOMMENDATION
5.1 Profile Template	• A target profile is helpful to envision a desired future-state cybersecurity posture.	• The provision of a profile template for use in applying the framework and tailoring to suit specific organizational needs offers practical direction and serves as a valuable resource for organizations seeking to translate theory into effective action by implementing cybersecurity practices and capabilities.
5.2 Cloud-Specific Profile Example	• The relationship between the NIST CSF 2.0 and cloud security is of increasing interest for many stakeholders. Organizations are evolving from cloud use cases where an organization manages and secured its own cloud infrastructure to cloud environments where third-party companies take legal and operational responsibility for managing the cloud. • The NIST CSF 2.0 facilitates some degree of oversight in cloud-hosted environments through its expanded governance and supply chain risk management provisions. In addition, NIST's updated framework is designed to allow its broad outcomes to be leveraged by organizations using cloud services and other technologies. Still, the many discussions around the subject of the NIST CSF not being cloud specific shows the need for further guidance on the use of profiles.	• It might be beneficial to create a profile sample not only for small, medium, and large businesses but also to create cloud specific profile examples for public use. • This approach would allow for the NIST CSF 2.0 to remain a CORE but offer opportunities to create profiles for deployment models such as public, private, hybrid (among others) and to standardize more clearly the carve-in/carve-out of security controls for the cloud service providers and cloud service user, which could also provide input for contract standardization.

6. TRANSITION PERIOD

TOPIC	OBSERVATION	RECOMMENDATION
6.1 Transition Period	• Guidance needed for a Transition period from the NIST CSF 1.1 to the NIST CSF 2.0.	We recommend that NIST provides the following: • Set a transition period from the NIST CSF 1.1 to the NIST CSF 2.0 (the International Accreditation Forum, Inc. recommends a maximum of 3 years for larger organizations to transition for ISO certifications). This would help to set expectations and allow for a transition period to self-assess Tier Level Implementations to the 2.0 in a pragmatic, staged form). • Provide transition documentation with key milestones and organizational communication messages during the transition.