NIST CSF Team,

I'm grateful for the opportunity to provide my input on the NIST Discussion Draft of the Cybersecurity Framework Core 2.0. And I also appreciate the efforts NIST dedicates toward enhancing alignment with both national and international cybersecurity standards and practices.

After reviewing the CFT 2.0, I noticed that the incorporated "Govern" function introduces a framework for structuring cybersecurity strategies that align directly with business objectives. Additionally, there is an enhanced focus on supply chain risk, which is rooted in the critical role that supply chains play in today's interconnected business environment. Ultimately, the underlying principles and best practices described play a substantial role in the overall cybersecurity readiness of both organizations and nations.

It is my pleasure to submit the following recommendations for consideration:

Section
Location
Suggestion

Govern

GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood

Wording changes to add clarity in identifying and defining stakeholders and expectations.

Proposed change: Internal and external stakeholders are identified, and their needs and expectations regarding cybersecurity risk management are defined.

Govern

GV.RM: The organization’s priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)

Assumptions should not be defined, rather expectations should be.

Proposed change: The organization’s priorities, constraints, risk tolerance and appetite statements, and expectations are established, communicated, and used to support operational risk decisions.

Govern

GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions

> The term positive risks does not need to be defined, it creates a detraction of importance with other strategic opportunities .

Govern

GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

> Due diligence is vague, consider defining the expectations for this.

Govern

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

> Consider expanding plans to include all stages of partnership not just after events.

Govern

GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced (formerly ID.AM-06, ID.GV-02, DE.DP-01)

> Should include roles and responsibilities being continuously reviewed against the organization’s focus.

Govern

GV.RR-03: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies

> Stating “adequate” resources is unnecessary when adequate is not defined.

Identify

ID.AM-01 / ID.AM-02

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

ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained

> Consider being inclusive of all assets managed outside the organization, while impacting the organization.

Identify

ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained (formerly ID.AM-03, DE.AE-01)

> The organization's approved network communication should encompass both internal and external channels. Avoiding the separation of network data flows based on the type of communication is recommended.

Identify

ID.AM-04: Inventories of services provided by suppliers are maintained

> Services and assets should be included for inventories.

Identify

ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained

> Does the inclusion of metadata data include the logs designated to the data types?

Identify

ID.RA-01 / ID.RA-02

ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded

ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources

> The categories should encompass the requirement not only to receive cyber threat intelligence but also to seamlessly integrate it into the organization's risk management procedures. Additionally, the categories should outline actionable measures involving vulnerabilities in assets that need enhancement.

Identify

ID.RA-06: Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated

> Consider adding a section to address lessons learned from an incident to increase security.

Identify

ID.IM-04: Cybersecurity plans that affect operations are communicated, maintained, and improved (formerly PR.IP-09)

> Expand to all cybersecurity plans, rather than those that only affect operations.

Protect

PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization (formerly PR.AC-01)

> There should also be constant protection for identities and credentials of authorized users.
>
> Proposed change: Identities and credentials for authorized users, services, and hardware are managed and protected by the organization.

Protect

Awareness and Training (PR.AT):

The organization’s personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks

Organization’s personnel impacting cybersecurity should have defined roles and expectations in order to impose training.

Protect

PR.DS-01 / PR.DS-02

PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected

PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected

Consider moving PR.DS-10 under here for continuity as they are all correlated.

Protect

PR.DS-09: Data is managed throughout its life cycle, including destruction

Singling out “destruction” is too descriptive and should be addressed in implementation examples. Destruction is included in the life cycle already.

Protect

PR.DS-11: Backups of data are created, protected, maintained, and tested

Backups of data should also be verified. Consider incorporating “verified” into a category.

Protect

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

Log records that are generated should not only be used for continuous monitoring, but also for proactive change for strength of the framework.

Protect

PR.PS-05: Installation and execution of unauthorized software are prevented

For unauthorized software installation prevention - if software needs installation it is verified and added to the authorized list.

Protect

PR.IR-01: Networks and environments are protected from unauthorized logical access and usage

> Networks and environments should also be continuously protected from unauthorized logical access and usage.

Detect

DE.AE-02: Potentially adverse events are analyzed to better understand associated activities

> Adverse events narrows down the type of events that should be reviewed, when all impacting events should be reviewed.

Detect

DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis

> As cyber threat intelligence and other contextual information are integrated into the analysis, there should also be a proactive step included for cybersecurity protection.

Detect

DE.CM-01: Networks and network services are monitored to find potentially adverse events

> Not only to locate adverse events in the detect stage, but any event that may threaten the security of a system.

Respond

RS.AN-08: The incident’s magnitude is estimated and validated

> Incidents are not validated, rather they are irradiated and addressed for impact.

Recover

RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration

Integrity of backups and other restoration assets should be verified before storage too.

For additional comments, kindly explore the post "Enhancing Cybersecurity through NIST CSF 2.0" on Digital Data Hive: https://urldefense.com/v3/__https://digitaldatahive.com/nist-csf/__;!!Nhox7I4E!Obb4aUfn16NS1VQT0CJjNnIXxxwE1FGy_2Ewihk3Dw9lNi3HjSkuSq4OOw0f6QHIvjfvwU0nLaR-5vkFrsR4LADFDdAzWA$ <https://urldefense.com/v3/__https://digitaldatahive.com/nist_csf/__;!!Nhox7I4E!Obb4aUfn16NS1VQT0CJjNnIXxxwE1FGy_2Ewihk3Dw9lNi3HjSkuSq4OOw0f6QHIvjfvwU0nLaR-5vkFrsR4LABLVS9R1g$ >

In closing, Digital Data Hive would like to thank NIST for its continued leadership and partnership in developing the Cybersecurity Framework 2.0. I am open for discussion and look forward to the advancements with this standard.

Respectfully submitted,

Dr. Emilia Mancilla