Montreal, October 31, 2023

Discussion Draft of the NIST Cybersecurity Framework (CSF) 2.0 Core Cybereco members response, October 2023

Founded in 2018, Cybereco is the multisectoral reference in Cybersecurity in Quebec and Canada. Cybereco brings together an increasing number of members with the common goal of accelerating the development of a world-class workforce and effective technological solutions for a prosperous and secure economy.

Cybereco organized a series of workshops with some of its members to review the CSF 2.0 draft:

- Romain Bochy, Information Security Consultant, Neotrust
- Dr. Samrajesh Mault, Faculty and Academic Program Coordinator, McGill University
- Florent Petit, Security architect, Desjardins
- Pierre-Martin Tardif, Professor, Université de Sherbrooke
- Douglas Wiemer, CTO Cybersecurity, RHEA Group

We summarize here the output of those discussions. We organized the document in three sections: General Comments, Specific Comments related to the CSF 2.0 Function Tables, and Specific Comments relative to the use of the CSF by SMBs.

General Comments

We have identified some general concerns or elements which could be improved in the current CSF 2.0 draft. We list those elements below, along with suggested improvements.

Concern: Compliance management
There is no explicit compliance management section. It would be a good addition to the risk management as they complement each other.
Suggestion: Risk management is helpful to identify which security controls should be applied with which level of priority. However, some security controls are to be applied systematically. For example, authentication is required before accessing internal data or services in an organization. Compliance enables to define default security controls that the organization needs. From there, risk management will focus on a perimeter and the specific security controls it needs.

Concern: Human resource management
There is nothing addressing human resource management, i.e., how to ensure an organization has access to skilled resources, with the expertise needed to handle the organizations' security requirements.
Suggestion: Add a governance section about Resource Management, should it be Cost/budget, Expertise/HR, Information/Data and Technology/material.

Concern: Culture

The cybersecurity culture is not sufficiently exposed.

Suggestion: Add an introductory text about the importance of an Organization Cybersecurity Culture, and the tools needed to improve its adequacy (like awareness and training).

Concern: Budget is not emphasized in governance.
Suggestion: Add a governance section about Resource Management, should it be Cost/budget, Expertise/HR, Information/Data and Technology/material.

Concern: There is too much emphasis on Zero-Trust Architecture which is only a specific aspect of a more general Security Architecture, and a flavor of the moment.
Suggestion: Use a more generic term such as Security Architecture, instead of always talking about Zero-Trust Architecture. In a paragraph, it should be explained the more generic Security Architecture and the relevance of Zer-Trust Architecture as a particular solution.

Specifics Comments related to the CSF 2.0 Function Tables

GV.SC-02: *Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.*
Comment: "and supported by organizational leadership" would be a great addition for better support of cybersecurity management teams.

ID.AM
Comment: Proposition of new subcategory: Data is classified according to its sensitivity for the organization.

ID.AM-05 *Assets are prioritized based on* ***classification, criticality, resources, and impact*** *on the mission.*
Comment: Notion of "resources" is not clear: what is considered as resources? How may it impact the prioritization?
As a more general comment, *classification, criticality, resources and impact* are very specific criteria. A better approach could be to refer to the risks: *Assets are prioritized based on the risks they induce*. Moreover, it would enable the inclusion of risks in Asset Management.

ID.RA-06: *Risk responses are chosen from the* ***available options****, prioritized, planned, tracked, and communicated.*
Comment: "available options": for better clarity, it could be renamed "available treatment options"

PR.AA-06: *Physical access to assets is managed, monitored, and enforced commensurate with risk*
Comment: The physical access could be fully integrated with the other PR.AA subcategories. No distinction should appear between logical and physical access at this level. However specific implementation examples for Physical security would prove useful.

PR.DS

Comment: Proposition of a new subcategory: Likelihood and impact of risks are updated with incident analysis results.

PR.AT: *The organization's personnel are provided cybersecurity awareness and training so they can perform their* ***cybersecurity-related*** *tasks.*
Comment: "so they can perform their cybersecurity-related tasks": it should be any tasks with security in mind. Replace with: "so they can perform their tasks with cybersecurity risks in mind".

PR.AT-01 and PR.AT-02
Comment: Replace "security" with "cybersecurity" to be consistent with the other categories.

PR.AT-02: *Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind.*
Comment: We recommend adding a control under IDENTIFY to define which skills are required in the organization for cybersecurity purposes.

PR.PS-05: *Installation and execution of unauthorized software are prevented.*
Comment: This control is presented in a *blacklist* way. We recommend presenting the control in a *whitelist* way: *Only installation and execution of authorized software are made available*. We also recommend applying the control not only to software but also to *services*.

DE.CM
Comment: Proposition of a new subcategory: Threats not mitigated in residual risks are monitored.

Specific Comments relative to the use of the CSF 2.0 by SMBs

Small and Medium Businesses (SMBs) have limited resources to implement the CSF, and they do not know where to start. We suggest adding some elements to the CSF 2.0 framework to make it more easily actionable by SMBs.

Recommendation: Add a "SMB" tag to all subcategories that should prioritized by SMBs.

Recommendation: The implementation examples are a great start to make the CSF elements actionable by SMBs. Consider adding more real-world examples, specifically tailored to the context of small businesses. This could include specific software tools they might use or simpler methods for achieving the same security outcome.

Recommendation: Small Businesses often operate on tight budgets. Highlighting cost-effective solutions in the implementation examples could be very beneficial.