Comments Towards the Preliminary Cybersecurity Framework

Abstract

This document contains my comments towards the Preliminary Cybersecurity Framework.

Contents

1 Evolution of the Framework

The intended audience for the Cybersecurity Framework has been broadened. Section 1.0, "Framework Introduction", states that "The critical infrastructure community includes public and private owners and operators, ***and other supporting entities*** that play a role in securing the Nation's infrastructure." Section 3.0 "How to Use The Framework" states: "The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices." These statements are an acknowledgement that the Framework is intended to apply to the supply chain of critical infrastructure owners and operators.

Given this extension, The Framework must be evaluated from the perspective of the supply chain.

Appendix A of the Framework Core has evolved in a positive direction. The sub-categories, best described as requirements or controls, have been re-written to describe the desired outcome, rather than to describe "how to achieve" the objective.[1] Although any individual subcategory may require editing, the re-write is a substantial improvement. This re-orientation, in general, does not dictate a solution, but allows the user to develop the systems and tools best suited to their business.

The **Informative References** included in Appendix A of the Framework Core have been cut back to those that can be considered generic, or "common", across the critical infrastructure categories. The Compendium of Resources still exists for reference, but is not included in Appendix A. NIST has suggested that each Sector develop its own set of reference resources. If each of the Sectors further develops The Framework, an appropriate set of references must be included in this work.

2 Issues and Recommendations

2.1 Clarity of Scope

The Framework would benefit greatly from a clear and concise statement of scope of applicability. While the Framework clearly states that it may be used for the "management of cybersecurity risk", it does not clearly state to what The Framework is to be applied.

The Framework text is inconsistent on this topic. The Introduction speaks to "the reliable functioning of critical infrastructure". However the Categories and subcategories in Appendix A refer to the organization and its own business objectives. We should not assume that National Security interests are one and the same as an organization's business objectives.

> For example, "Asset Management (AM): The personnel, devices, systems, and facilities that *enable the organization to achieve business purposes* are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy."

2.1.1 Recommendation (1 of 2)

For the purpose of cost effectiveness, as required by the EO, *the scope of application of The Framework should be defined as "those processes and IT/ICS assets directly involved in the delivery of critical infrastructure services".* Such clear scoping will allow organizations to focus their available resources towards achieving the objective of the EO. This is not to say that an organization cannot apply The Framework more broadly within its business, if it has the available resources and sees value in doing so.

[1] See Appendix A of the Framework Core

2.1.2 Application to the Supply Chain

Assuming that the scope of applicability for The Framework is clarified as stated in Section 2.1.1, above, the relationship of The Framework to the Supply Chain becomes much clearer.

Product or Service

The Framework is not a product security specification. It would be inappropriate for an owner/operator to require The Framework to be applied to a product or service. The owner/operator does have a right to understand how the product or service provided by the supplier affects his own Cybersecurity posture, e.g., what vulnerabilities it introduces, or what mitigations it might provide towards other identified vulnerabilities (See subcategory ID.RA-1).

Outsourced operations

Where the owner/operator of critical infrastructure services has outsourced any element of his business within the scope of applicability, it would be appropriate to apply The Framework to the outsourced element. Depending upon the scope of the outsourcing, and the roles and responsibilities of each party as defined in the agreement, assessment may well involve the collaboration of each of the parties.

Business continuity

If the nature of the relationship between an owner/operator and a supplier is such that an interruption of the provisioning of goods or services by the supplier would impact the delivery of critical infrastructure services, then the owner/operator of critical infrastructure has the right to question whether the supplier also considers cybersecurity risk and mitigation in its business risk management processes and business continuity plans.

2.2 Framework Profiles

The use of Framework Profiles by owners/operators of critical infrastructure in their supplier selection and supplier management processes will directly affect all parties. To be an effective tool, the methodology for development of Framework Profiles must be robust, so that the resulting profiles are valid and comparable between organizations.

The intention for use of the Framework Profile clearly extends outside an organization's own internal risk management activities, as stated in Section 3.3 "Communicating Cybersecurity Requirements with Stakeholders":

"The Framework provides a common language to communicate requirements among interdependent partners responsible for the delivery of essential critical infrastructure services. Examples include:

> An organization may utilize a Target Profile to express requirements to an external service provider (e.g., a cloud provider) to which it is exporting data.

> An organization may express its cybersecurity state through a Current Profile to report results or for comparison with acquisition requirements.
>
> A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey Categories and Subcategories.
>
> A critical infrastructure sector may establish a baseline Target Profile that can be used among its constituents as an initial baseline."

However, there is no defined methodology for developing a Framework Profile, resulting in results that are not comparable, making use of the Framework Profile for the purposes described above inappropriate.

Inconsistent selection of subcategories

Appendix A (see text below) does not prescribe that all of the subcategories must be used. It also indicates that additional subcategories may be added by the user (See snip, below). Therefore the selection of subcategories will vary from organization to organization, based on the individual situation of each. If each organization develops its own suite of subcategories, then there is no consistent base for comparison between organizations.

> Appendix A "presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. ***The Framework Core presented in this appendix is not exhaustive; it is extensible***, allowing organizations, sectors, and other entities to add Subcategories and Informative References that are relevant to them and enable them to more effectively manage their cybersecurity risk. ***Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile***. An organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation."

Calculation of Current and Target Profiles

As shown in the illustration below, profiles are built on a category/subcategory level. While not specifically linking the Framework Profile to the Implementation Tiers as in previous versions of the Framework, it is clear that there is a relationship.

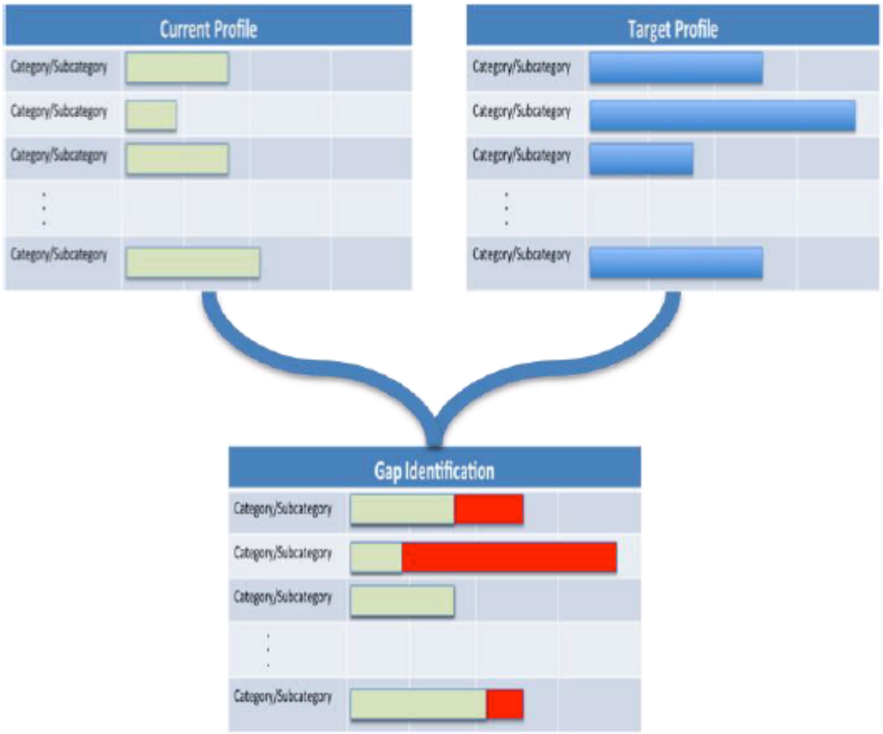

Figure 2:|Profile Comparisons

The Framework Tiers are subjective in nature – a maturity model concept. The tiers are described at an ***organizational*, ** rather than ***activity (subcategory)***, level, creating a disconnect between the subcategory descriptions and the tier descriptions. If there is a difference between the maturity of an activity and the overall maturity of the organization, how do you score that subcategory?

Further, each tier describes 3 perspectives: Risk Management Process, Integrated Program, and External Participation. There is no defined methodology how to determine a single score combining these 3 perspectives.

Illustration 1

For Category ID.GV-1: Organization information security policy is established.

Risk Management Process – If I have an established policy, then am I a Tier 3 or a Tier 4? – This is a yes/no answer – not a maturity model answer.

Integrated Program - If I have a security policy, how does this relate to an integrated program? How do I judge maturity? Or is this perspective not applicable?

External Participation – How do I judge the Tier level? None of the descriptions in the Tiers for this perspective appear to be applicable to this subcategory. So is this “not applicable”?

Here I now have a question of how to calculate a score. If I consider that having a policy qualifies me to claim that perspective as a Tier 4, and I do not consider either the integrated program or external participation perspectives as applicable, then do I claim Tier 4 as default? Or?....

Illustration 2

For ID.RA-1: Asset vulnerabilities are identified and documented.

Situation: The organization has completed a vulnerability assessment, has established communications channels to receive vulnerability updates from vendors, and has included the requirement for provision of vulnerability information into its purchasing processes. However, the organization's overall risk management processes are immature and somewhat reactive.

> Risk Management Process – How do I relate the maturity of the activity to the maturity of the risk management process if these are at different maturity levels? I might consider that the maturity of the activity reaches a Level 4 Tier intent, but the maturity level of the risk management process (as described in the Tier description) would best be described as a Tier 2
>
> Integrated Program – Again we may have a disconnect between the level of maturity for the activity and the level of maturity of the organization. Perhaps the maturity of this particular activity is very high, but it is an anomaly within the organization. Do I score a Level 4 or a Level 1?
>
> External Participation – First, we may again have a disconnect between the level of maturity for the activity and the level of maturity for the organization. Second, complicating the assessment, we need to choose between these descriptions:
>
> Tier 1 – Partial - An organization may not have the processes in place to participate in coordination or collaboration with other entities. *True for the organization, but not for the activity*
>
> Tier 2 – Risk Informed - The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally. *True for the organization, but not for the activity*
>
> Tier 3 – Risk Informed and Repeatable - The organization understands its dependencies and partners and receives information from these partners enabling collaboration and risk-based management decisions within the organization in response to events. *True for the organization, but not for the activity*
>
> Tier 4 – Adaptive - The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before an event occurs. *Is it appropriate to share a vulnerability assessment with a partner?*

Third, am I double scoring this issue? There is a separate subcategory describing interaction with external parties: "ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources."

How do I score this subcategory? Am I Tier 3, based on the activity itself, and my interpretation of the Tier requirements, or am I Tier 1, based on the organization's maturity? Or am I somewhere in between?

2.2.1 Recommendation (2 of 2)

Remove all references to Framework Profiles from Section 3.0 "How to Use The Framework" until a methodology is developed and tested for comparability of results. Absent a described methodology for calculating a profile, valid, comparable results are not possible.

Add a statement to Section 2.2 "Framework Profile" that an organization may develop a process for determining its organization's current and target profile, which may be used for its internal use only. There should be a further statement that, absent an agreed described methodology for calculating a profile, valid, comparable results are not possible, and that use of Framework Profiles for purposes of communication with external parties is not appropriate.

3 Cross Sector Suppliers

As the macro business ecosystem evolves, we need to be cognizant that suppliers may play a role in more than one critical infrastructure sector. To an increasing extent, the Information Technology Sector and the Communications Sector are merging. In turn, these sectors are increasing their presence in the delivery of services of other sectors.

The more that we push the further development of The Framework out to the Sectors, without requiring coordination between the Sectors, the greater the odds that result may, in practice, 16 different Frameworks. If a supplier is active in more than one sector, he may be faced with conflicting requirements.