PUBLIC SUBMISSION

As of: 4/25/22 12:48 PM
Received: April 24, 2022
Status: Pending_Post
Tracking No. l2d-jhvl-dw1e
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0034
Comment on FR Doc # N/A

Submitter Information

Name: Bachir Benyammi
Ad[redacted]
Email:[redacted]
Phone:[redacted]

General Comment

Throughout the years, NIST Cybersecurity Framework (CSF) proved itself to be the FRAMEWORK to manage cybersecurity in the enterprise, thus maintaining its relevancy and success over the years is essential for improving our cyberspace.

In this document, I present some ideas to be considered in future framework releases.

See attached file(s)

Attachments

Comments on RFI-2022-03642

Evaluating and Improving NIST Cybersecurity Resources:
The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comments on the NIST Cybersecurity Framework "RFI-2022-03642" | April 24th, 2022

Introduction

Throughout the years, NIST Cybersecurity Framework (CSF) proved itself to be the FRAMEWORK to manage cybersecurity in the enterprise, thus maintaining its relevancy and success over the years is essential for improving our cyberspace.

In this document, I present some ideas to be considered in future framework releases.

Intended audience

When the CSF was introduced in 2014, it was intended for critical infrastructures, however, nowadays every organization (large, small, public, private, commercial, or nonprofit) uses the framework as a reference for its security posture. Thus, for better adequacy, adoption, and acceptance by relevant stakeholders and decision-makers, the framework needs to be generic whereas variants (e.g., industry-specific profiles) of it can be made available to address specific industries, requirements, and risks

Interested parties

It is a good idea to list the various interested parties an enterprise might have and indicate how they can benefit from the framework and what is expected from them within the cybersecurity program

Organizational structure

While the framework mostly addresses the activities and outcomes within the business/process (Tactical) level, it needs more guidance and clarity at both the senior executive (Strategic) level as well as the implementation/operation (Operational) level.

At the strategic level, aligning cybersecurity objectives with business strategy is crucial for getting stakeholders' commitment, securing the resources, building adequate cybersecurity capabilities, maintaining, and improving the security posture. This helps preserve value while giving assurance to stakeholders that their concerns are addressed, and objectives are achieved.

Regarding the operations level, detailed generic practices, activities, and tasks for each subcategory need to be presented to assist partitioners in achieving the decided outcomes. Such details can be generated by mapping and aligning relevant informative references controls for each subcategory.

While the CSF emphasizes the importance of roles and responsibilities of various stakeholders in improving the security posture, it needs specifics regarding common roles and responsibilities throughout the framework. RACI matrix can be introduced within the framework to present the involvement of each party, especially in terms of responsibility- (R) and accounting- (A) related tasks. For instance, roles are better specified for each subcategory within the framework Core section.

Informative references

Since the release of the previous version in 2018, several best practices, standards, and formworks have been introduced and/or updated. Reviewing the CSF in 2022 is a good opportunity to include those informative references (e.g., NIST SP 800-53 rev 5, CIS v8, ISO 27002:2022, COBIT 2019, ISO DIS 27005:2022, CMMC 2, PCI DSS 4.0, FAIR, MITRE ATT&CK …etc.).

The revision is also an opportunity to provide alignment with existing NIST frameworks (e.g., privacy and risk). NIST may also consider including other standards and controls related to zero trust, secure coding, application, mobile and IoT security, network, and cloud security…etc.

For ease of use of the framework, only generic, most relevant, and largely adopted informative references better be included in the main document, other references can be supplemented in separate excel sheets, same for old but still in use informative references.

NIST may also consider including control names or titles from the informative references instead of just putting numbers (e.g., "A.5.1.1. Information Security Policies" instead of just "A.5.1.1").

Capabilities and maturity assessment

Minimum capability and maturity requirements (e.g., baselines using C2M2 or CMMI) need to be considered and suggested for both Core, Profiles, and Tiers. Such baselines help set target profile expectations as well as perform assessments to identify the current state and gaps.

Generic timeframe (monthly, quarterly, yearly …etc.) can also be suggested for regular assessments.

Framework Core

While the functions do their job perfectly, categories and subcategories need to be renamed to reflect existing best practices. Titles such as objectives, outcomes, controls, countermeasures, practices, activities …etc. can be used to achieve such alignment. In addition, guidance (descriptions) for each subcategory should be provided to better understand the expected outcomes.

Dependency between subcategories can also be introduced. Same for the information flows (inputs and outputs or deliverables) exchanged between functions, categories, and subcategories.

Criticality levels or risk ratings (e.g., high, medium, and low) and/or weighing can be introduced to emphasize the importance of certain functions, categories, and subcategories compared to others, such levels can be determined based on the selected implementation tiers and/or desired profile.

Regarding the Core worksheet, it's recommended to put the functions into separate sheets (tabs). A main sheet (tab) can be added listing the categories and subcategories with the description of each.

An enhanced version of the Core worksheet can be provided for assessment purposes.

Framework Tiers and Profiles

The idea behind tiers and profiles is interesting, however, they are a bit confusing considering the maturity levels used within many industries (such as CMMI). Moreover, the mapping of tiers and profiles with relevant subcategories is not clear.

For better alignment with best practices, the desired security state of an organization (e.g., target profile) can be expressed using maturity levels (from 0: Incomplete to 5: Optimizing) whereas capability levels for functions, categories, and subcategories can be expressed using capability levels. A mapping can also be made between maturity and capability levels, the maturity level of the organization reflects the minimum capability level provided by its relevant subcategories.

Tiers and profiles can be linked together, tiers can be seen as baselines which we refer to while measuring the current profile and defining the desired profile. Metrics can be developed to assess and determine current and desired tiers.

Cybersecurity program implementation

The provided 7 implementation steps are given at a high level. More guidance is required to assist professionals planning and implementing a successful cybersecurity program. An implementation roadmap can be provided for the same. Metrics can be added to measure progress and efficacy.

Timeframes can also be suggested for the implementation phases and the review of the program.

Organization and personal certifications

Like the efforts made by ISO with the establishment of an information security management system (ISMS) and the compliance with the ISO 27001 requirements. A cybersecurity management system (i.e., CSMS) with a defined set of requirements can be made (in collaboration with the ISO organization) which can help organizations independently demonstrate their commitment to the framework following an external audit and certification from accreditation bodies. An extension to the ISO 27001 can be made to layout such a management system (something similar to the ISO 27701 standard that extends ISO 27001 to handle privacy-related requirements).

Similarly, professional training and personal certifications can be introduced to assert cybersecurity professionals' competency about the framework following ISO 17024.

Worldwide adoption

Following the successful adoptions and contributions to the CSF from outside the US, more efforts could be made to make it more relevant and applicable to any organization worldwide.

To increase the adoption of the framework, webinars can be regularly organized to explain the framework and present its use cases, successful implementations, adoptions, and adaptations.

Conclusions

NIST may also commit to a fixed timeframe (e.g., 3 to 5 years) for CSF revisions, this helps the community to align the newly updated/published informative references to the framework and prepares their contributions ahead of future revisions.

Several of the suggestions made above were inspired by the latest edition of ISACA's I&T governance and management framework (COBIT 2019). Throughout its various publications (core documents, information security, and risk focus areas, and especially the NIST CSF implementation document)[i] ; various concepts, ideas, metrics, and examples were already illustrated within those publications and can be considered in coming CSF releases.

Some links (URLs) within the document are no longer working, it is good to add an indication of when those were last visited. It is better also to keep (cashed) copies of the referenced resources within the nist.org and/or archive.org websites to maintain access to those links over the years.

While I had the pleasure to translate the CSF to French and have the NIST publish it online, I look forward to getting involved in future discussions and workshops around future CSF releases.

Regards,

Bachir Benyammi

[i] https://www.isaca.org/resources/cobit