Poster: A Template for developing NIST CSF Profiles

Shreenandan Rajarathnam
College of Communication and Information
University of Tennessee, Knoxville
Knoxville, USA
srajarat@vols.utk.edu

Vandana Singh
College of Communication and Information
University of Tennessee, Knoxville
Knoxville, USA
vandana@utk.edu

***Abstract*—In this study, we propose a template for NIST CSF profiles. NIST CSF profiles are useful tools for the industry to identify, assess, and manage cybersecurity risks. We systematically analyzed the existing profiles to develop a generalized template for industries/domains that currently do not have a profile, which will provide a simplified starting point for developing a customized profile for any domain. A visual and text-based template was developed and is being presented here.**

Keywords— National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF), Framework Profile

I. Cybersecurity Framework & Profiles

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [1] was developed as part of the Exec. Order 13636 [2] to improve critical infrastructure security in the US by helping stakeholders identify, assess, and manage cybersecurity risks, but has since been widely adopted voluntarily by organizations across all industry sectors in the US due to its proven flexibility [3]. The current version, NIST CSF v1.1 [1], consists of the following:

A. Framework Core

The Framework Core includes five (5) high-level cybersecurity risk mgmt. functions, which are divided into 23 categories and 108 sub-categories representing activities and desired outcomes. It also maps the activities and outcomes to relevant industry standards and best practices for reference.

B. Framework Implementation Tiers

These are descriptors of an organization's implementation of cybersecurity risk management processes, systems, and practices. The Implementation Tiers range from Partial (Tier 1) to Adaptive (Tier 4); reflecting a progression from reactive approaches to agile and risk-informed approaches.

C. Framework Profile

A profile is an alignment of an organization's business objectives to the Framework Core in a particular implementation scenario. The Framework Profiles of an organization's current state cybersecurity implementation can be used to roadmap the progress towards the target state.

NIST website provides examples of Framework Profiles [4] for various industry sectors and areas such as ransomware mitigation [5], manufacturing [6], etc. In this article, we review the examples Profiles based on the NIST CSF v1.1, and answer the following research questions:

RQ1: What are the common elements among the Profiles examples?

RQ2: What are the key differences among the Profiles examples?

The goal of this study is to provide the cybersecurity field with a generalizable template that can be used to develop new Profiles in the areas not covered in the NIST examples [4].

II. Common Elements & Differences

Table 1 outlines the following common elements that are included (or not) in the purposefully selected (published by NIST) 14 Profile examples [4] based on a document analysis:

A. Introduction and Context

An introduction to the NIST CSF [1] and context regarding the specific industry sector or area of interest for the Profile, such as manufacturing, election infrastructure, etc.

B. General Tips

General tips for addressing cybersecurity concerns and problems such as the following for ransomware mitigation: "Block access to untrusted web resources", and so forth [5].

C. Methodology / Development Approach

This section outlines the approach used to develop the Profile example such as workshops with stakeholders in the area of interest. E.g., The Election Infrastructure Profile [7] outlines activities like "for each mission objective, identifying and ranking the top three CSF categories (out of 23 available) that participants consider most important for accomplishing that objective securely" in the workshop conducted by NIST with relevant stakeholders.

D. Business / Mission Objectives

This section outlines the business / mission objectives of an organization in the specific industry sector / area of interest of the Framework Profile Example that is being developed. E.g., "Maintain Human Safety", "Maintain Production Goals", etc. specific to the manufacturing sector [6].

E. NIST CSF Mapping

This section maps the business objectives in the specific industry sector / domain of the Profile example to the NIST CSF v1.1 Framework Core [1]. This allows the Profile users to streamline efforts to improve their cybersecurity posture.

F. Implementation Measures and Prioritization

This section outlines the suggested application or implementation measures that can be taken to manage and mitigate cyber risks and improve the overall cybersecurity posture of the organization based on the mapping of business objectives to the Framework Core. Additionally, the suggested implementation measures can be prioritized based on the level of risk or impact on the business objectives.

G. Reference to Other Standards

In addition to mapping the business / mission objectives to the NIST CSF v1.1 Framework Core, some Profile examples also

TABLE I. COMMON ELEMENTS THAT ARE INCLUDED (√) OR NOT INCLUDED (X) IN THE EXAMPLES OF FRAMEWORK PROFILES [4]

Document Name	Intro & Context	General Tips	Methodology [a]	Business Obj.	NIST Mapping	Impl. Measures	Impact Tiers	References [b]
NISTIR 8183 – Cybersecurity Framework Manufacturing Profile	N/A - redundant, updated version below (NISTIR 8183r1 – Cybersecurity Framework Version 1.1 Manufacturing Profile Rev. 1 [7])							
NISTIR 8374 – Ransomware Risk Management: A Cybersecurity Framework Profile	√	X	X	X	√	X	X	√
NISTIR 8183r1 – Cybersecurity Framework Version 1.1 Manufacturing Profile Rev. 1	√	X	√	√	√	√	X	√
NISTIR 8310 (Draft) – Cybersecurity Framework Election Infrastructure Profile	√	X	√	√	√	√	X	√
NIST IR 8323 Revision 1 – Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of PNT Services	√	X	X	√	√	X	X	√
NIST TN 2051 – Cybersecurity Framework Smart Grid Profile	√	X	X	√	√	X	X	√
White Paper NIST CSWP 27 (Draft) | Cybersecurity Profile for Hybrid Satellite Networks (HSN) Final Annotated Outline	N/A - obsolete (Draft), updated version (Final) is just an annotated outline / whitepaper providing an overview of the Profile that will be created							
How to Use the Cybersecurity Framework Profile for Connected Vehicle Environments – U.S. Transportation	√	X	√	√	√	√	X	X
Cybersecurity Framework Profile Excel for Connected Vehicle Environments – U.S. Transportation	N/A - Excel file containing the mapping for the row above (How to Use the Cybersecurity Framework Profile for Connected Vehicle Environments – U.S. Transportation)							
Cybersecurity Framework Botnet Threat Mitigation Profile – Cybersecurity Coalition	√	X	X	X	√	√	X	√
Cybersecurity Framework DdoS Threat Mitigation Profile – Cybersecurity Coalition	√	X	X	X	√	√	X	√
The Profile – Cyber Risk Institute	√	X	√	√	√	√	√	√
Framework Payroll Profile – IRS Security Summit	√	X	X	X	X	X	X	√
Cybersecurity Framework Profile: White House Fact Sheet – Seamless Transition	X	√	X	X	√	X	X	X

a. Some of the documents don't have an explicit approach section but talk about it in the introduction / overview / context section.

b. Included as an Appendix item in some instances.

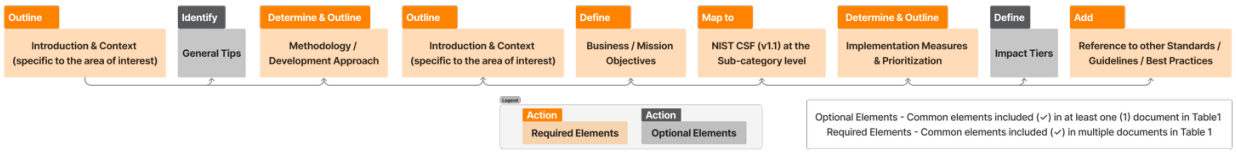

Fig. 1. Proposed template for a Framework Profile based on NIST CSF v1.1 [1] using common elements from Framework Profile examples [4]

include a mapping to other standards, guidelines, and industry best practices, such as COBIT 5 [8], among others.

III. CONCLUSION

Fig. 1 outlines a template comprising primary elements needed to develop new Framework Profiles based on the NIST CSF [1]. Once a new Framework Profile is developed using this template, it can be reviewed, socialized, updated, and then published so that organizations in the area of interest can use the Profile for their initiatives.

IV. LIMITATIONS AND FUTURE WORK

NIST is currently developing the NIST CSF v2.0 expected to be published by winter 2024 [8] and is currently developing a Framework Profile template in response to the Requests For Information (RFI) that they have received. Therefore, our proposed generalized template will only apply to organizations seeking to develop Framework Profile Examples based on the current version (v1.1) of the NIST CSF [1], or till they transition to NIST CSF v2.0 Profile template. Also, the proposed Profile template is not vetted by industry professionals, however, we will be pursuing it in the future.

REFERENCES

[1] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[2] The White House Office of the Press Secretary, "Executive Order -- Improving Critical Infrastructure Cybersecurity," whitehouse.gov, Feb. 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed Mar. 29, 2023).

[3] National Institute of Standards and Technology, "NIST Releases Version 1.1 of its Popular Cybersecurity Framework," NIST, Apr. 2018, Accessed: Mar. 29, 2023. [Online]. Available: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

[4] National Institute of Standards and Technology, "Examples of Framework Profiles," NIST, May 2021, Accessed: Mar. 29, 2023. [Online]. Available: https://www.nist.gov/cyberframework/examples-framework-profiles

[5] W. Barker, W. Fisher, K. Scarfone, and M. Souppaya, "Ransomware Risk Management: A Cybersecurity Framework Profile," National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8374, Feb. 2022. doi: 10.6028/NIST.IR.8374.

[6] K. Stouffer et al., "Cybersecurity Framework Version 1.1 Manufacturing Profile," National Institute of Standards and Technology, Oct. 2020. doi: 10.6028/NIST.IR.8183r1.

[7] M. Brady et al., "Draft Election Infrastructure Profile," preprint Draft NISTIR 8310, Mar. 2021. doi: 10.6028/NIST.IR.8310-draft.

[8] National Institute of Standards and Technology, "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework