As of: 4/27/22 6:48 AM
Received: April 25, 2022
Status: Pending_Post
Tracking No. l2f-2ecr-yoqa
Comments Due: April 25, 2022
Submission Type: Web

PUBLIC SUBMISSION

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-0051
Comment on FR Doc # N/A

Submitter Information

Name: Andrew Micone
Ad[redacted]ess:
,
Email: [redacted]

General Comment

See attached file(s)

Attachments

Response to NIST Cybersecurity RFI

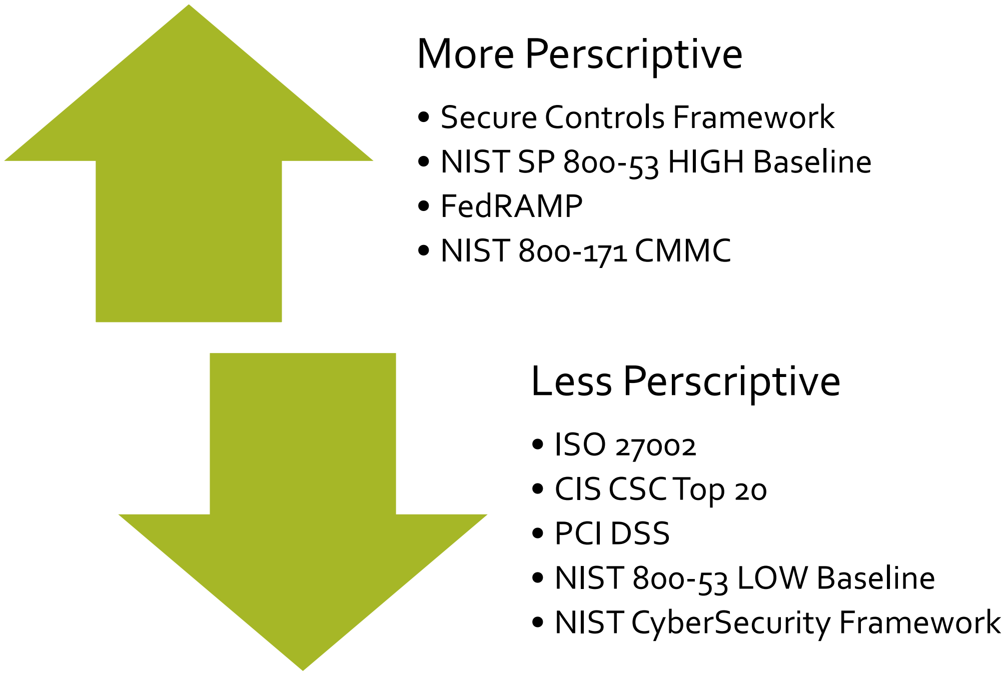
RESPONSE TO NIST CYBERSECURITY RFI

Document Citation: 87 FR 9579
Agency/Docket Number: 220210-0045
Document Number: 2022-03642

This document is in response to *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.* Andrew Micone is a Futurist who previously participated in previous NIST supply-chain forums as part of the supply-chain and logistics body RosettaNet, the original National Cyber Security working groups at UCSD, at the invitation of NIST to respond for the health care industry vertical for the framework at NCU, and as part of the recent industry feedback session for the National Privacy Framework at BSU. His current academic work is part of the futurist think-tank TechCast, a special project of the policy institute of George Washington University.

USE OF THE FRAMEWORK

In general, the framework has proven useful as a way to understand an organizational CyberSecurity approach and align organizational processes to best security practices. Understanding the five functions of the framework helps align the relationship between security control families and the processes involved in implementing and operationalizing those processes. The framework in this capacity works much like European security standards like ISO 27002, without being overly prescriptive as FedRamp or NIST 800-171 CMMC.



More Perscriptive

- Secure Controls Framework
- NIST SP 800-53 HIGH Baseline
- FedRAMP
- NIST 800-171 CMMC

Less Perscriptive

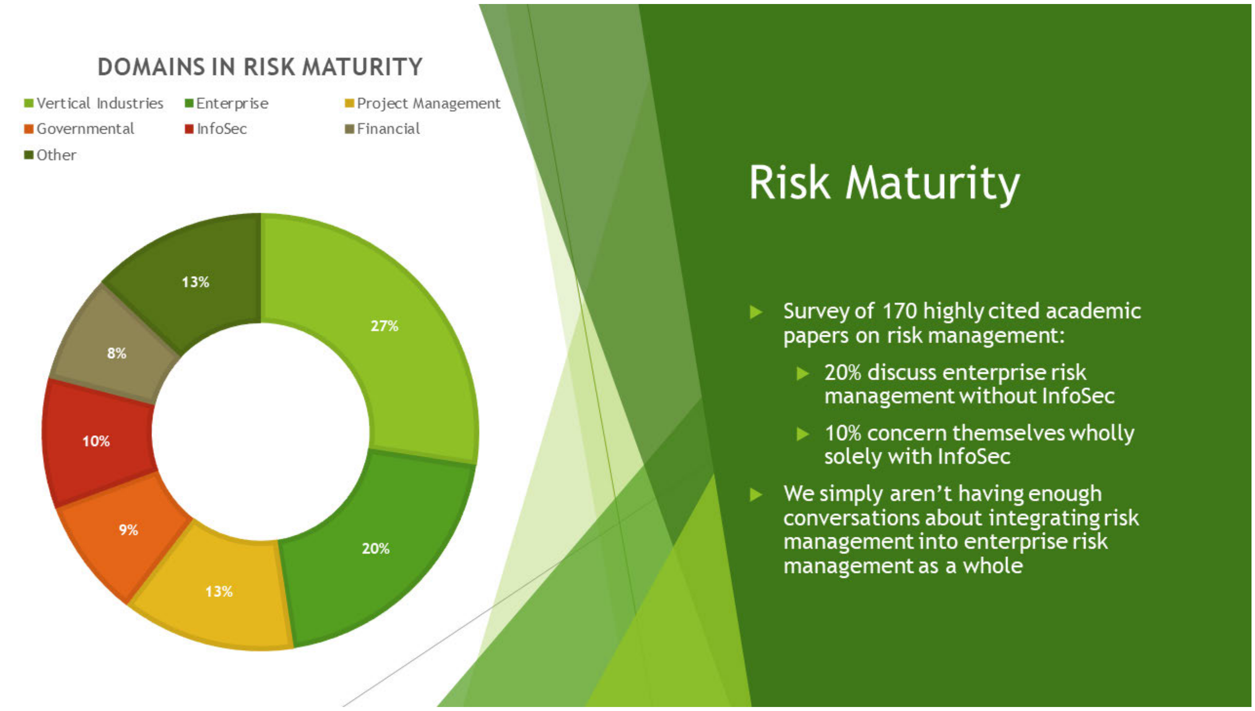
- ISO 27002
- CIS CSC Top 20
- PCI DSS
- NIST 800-53 LOW Baseline
- NIST CyberSecurity Framework

From inception, it was a just right approach that tried to adopt best practices from robust coverage frameworks without the bureaucratic baggage, checkmark compliance, and documentation fire-drills.

However, the main challenge for the adoption of the framework is that it is less prescriptive. At inception, the framework was conceived as a general framework for all organizational security operations across industries, sectors, and techniques. Industry profiles that were to be developed later were intended to fill in the gaps for specific industry organizational, technical, and process controls. These industry profiles were developed for a few critical infrastructure sectors, but most have not seen significant updates since 2015. Additionally, many accounting, legal, and lobbying groups initially viewed these industry profiles as sources of potential liability and future regulation, hampering initial adoption. Further, other voluntary frameworks have certification bodies attached to them, such as ISO 27001 and CMMI have become sales qualification tools in their respective industries, making them desirable for marketing purposes.

RISK MANAGEMENT

When discussing risk management practices and the CSF, we have to look overall at the maturity of risk management across industries. A survey of 170 highly cited academic papers on integrated risk management undertaken by the author of this document showed that 20% of papers discuss integrated enterprise risk management without discussing information security at all, 10% concern themselves with solely with information security risk management, and the other 70% concern themselves solely with vertical industry risks.

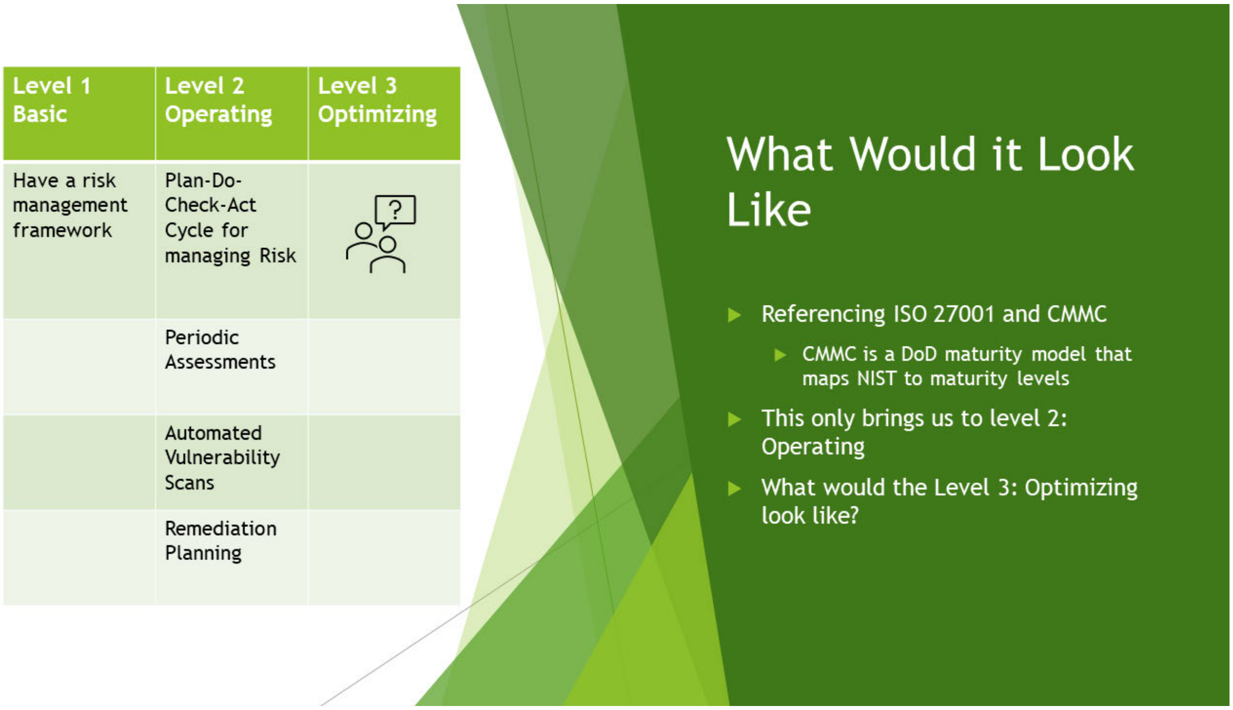


Risk Maturity

- Survey of 170 highly cited academic papers on risk management:
  - 20% discuss enterprise risk management without InfoSec
  - 10% concern themselves wholly solely with InfoSec
- We simply aren't having enough conversations about integrating risk management into enterprise risk management as a whole

In general, organizations simply aren't having enough conversations about integrating risk management outside of industry vertical concerns and risk management in specific practice areas For example, project management is one practice area that is deeply concerned with risk management, but not in a way that easily integrates information security risks. The minority of companies have robust risk management practices across organizational concerns that include information security. It should be then wholly unsurprising that supply-chain risk is a tertiary concern in enterprises, only gaining attention when high-profile, critical severity exploits become public.

Further, we must ask what a risk management framework would look like within the framework. The NIST RMF, especially as implemented in FISMA, is clearly showing its age. If we look at more prescriptive information security frameworks that support tiered adoption models, they themselves really have very little to say on the topic.

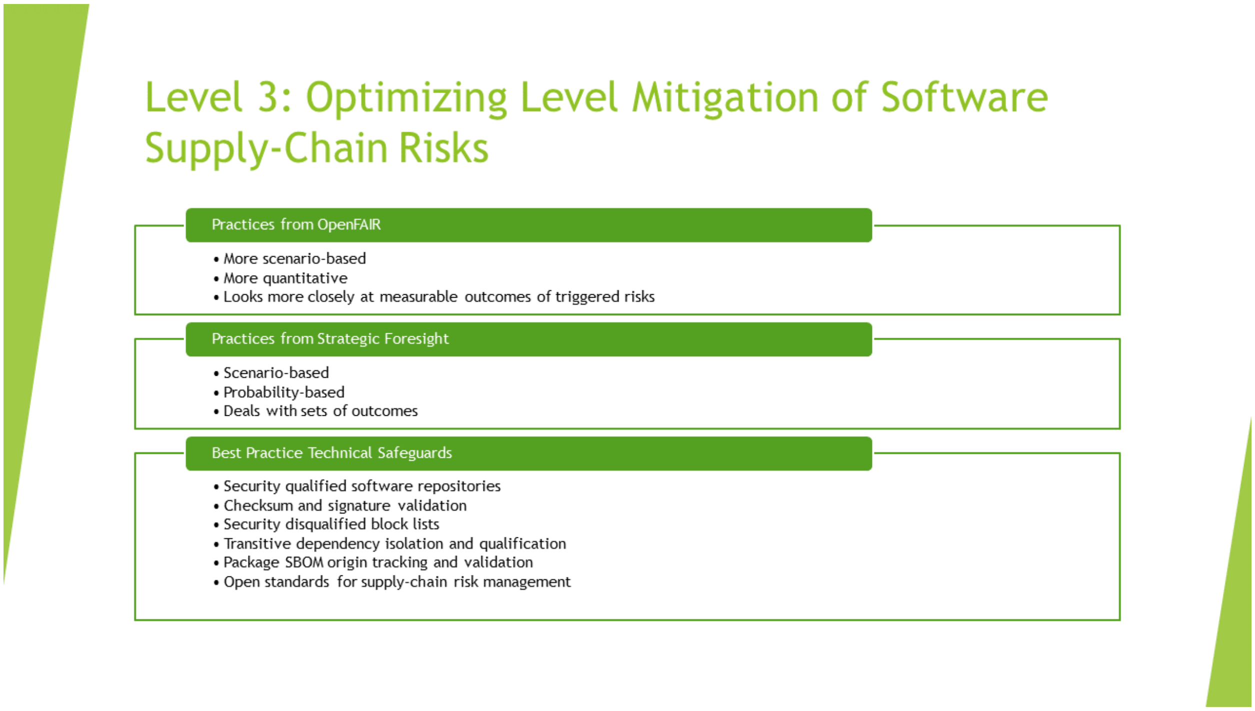


Level 1 Basic	Level 2 Operating	Level 3 Optimizing
Have a risk management framework	Plan-Do-Check-Act Cycle for managing Risk	?
	Periodic Assessments	
	Automated Vulnerability Scans	
	Remediation Planning	

What Would it Look Like

- Referencing ISO 27001 and CMMC
  - CMMC is a DoD maturity model that maps NIST to maturity levels
- This only brings us to level 2: Operating
- What would the Level 3: Optimizing look like?

Though this is clearly a more expansive discussion, if we consider the narrower case of what an optimized level of practice would be in software supply-chain risk management, we can see a few general practices across other frameworks along with several widely adopted technical safeguards adopted as best practices within the industry.



Level 3: Optimizing Level Mitigation of Software Supply-Chain Risks

Practices from OpenFAIR

- More scenario-based
- More quantitative
- Looks more closely at measurable outcomes of triggered risks

Practices from Strategic Foresight

- Scenario-based
- Probability-based
- Deals with sets of outcomes

Best Practice Technical Safeguards

- Security qualified software repositories
- Checksum and signature validation
- Security disqualified block lists
- Transitive dependency isolation and qualification
- Package SBOM origin tracking and validation
- Open standards for supply-chain risk management

TECHNICAL SAFEGUARDS

In general, the most effective means to mitigate supply-chain risks in software distribution outlined above have their own issues that must be dealt with. Looking at the common-industry safeguards:

- Security qualified software repositories
- Checksum and signature validation
- Security disqualified block lists
- Transitive dependency isolation and qualification
- Package SBOM origin tracking and validation
- Open standards for supply-chain risk management

There are synergistic concerns. For example, in a typical continuous integration pipeline, transitive dependencies may be pulled in a software's SBOM without the developer being aware of their origin or modification by intermediaries. Even with security qualified software repository subscriptions, developers must know enough to change their build systems not to pull in transitory dependencies, and this goes back to the lack of open standards for SBOM as developers have no way to determine if those transitory dependencies are contained in larger packages without standardization across different repositories. The continuous innovation in the industry without open standards for packages, for example, lead to one major public repository npmjs suffering from several supply-chain attacks in 2022 using obfuscation techniques over a decade old. Clearly, the risk management practices around supply chains are not keeping pace with advancements in software development, because the software supply-chain is not being treated as a cross-cutting concern.

SUGGESTIONS FOR CSF ADVANCEMENT IN SUPPLY-CHAIN MANAGEMENT

The CSF working groups had the right idea when they conceived the industry profiles, control group overlays specific to the vertical industry risks and controls that were primary concern. As previously indicated, most industries look at risks in terms of their vertical industry risk, not in terms of general risk from an integrated organizational perspective. Revitalizing those industry profile groups, therefore, should be an important priority.

As the Cloud Security Alliance has indicated, however, the CSF is sorely lacking in practice area controls for cloud safeguards. In the same way, the OWASP working groups note that CSF is lacking in web application controls. The primary suggestion for there CSF would be just as there are specific CSF profiles for industry verticals, there should be specific profiles for practice areas. For example, application developers, system reliability engineers, information risk professionals, and corporate risk professionals.

RECCOMMENDATIONS

The specific recommendations based on previous discussion for NIST would include:

1. Look at revitalizing the industry profile working groups for CSF.
2. Consider adopting a tiered adoption model for CSF, like CMMC or CMMI.
3. Create practice area profiles specifically related to supply-chain practice areas.
4. Software development should be the first practice area profile for supply-chain management.
5. If practice area profiles are adopted by the CSF, special concern areas should be:
    a. Software development and continuous integration
    b. Embedded software development.
    c. ICS related concerns, especially related to PLC automation methods

6. Consider whether there need to be supply-chain specific practices for industry profiles.
7. Consider whether adoption of organically developed open standards for SBOM's could be incorporated by prescriptive guidance on industry best practices.
8. Consider whether through private/public partnership that specific practice areas could be incorporated into certification standards that could be used for marketing or qualification purposes, such as the role the CMMS now plays in DoD procurement.