Assigning CSF Maturity Tiers to SP800-53 controls

Prepared for NIST 2.0 Public Consultation

4 March 2023

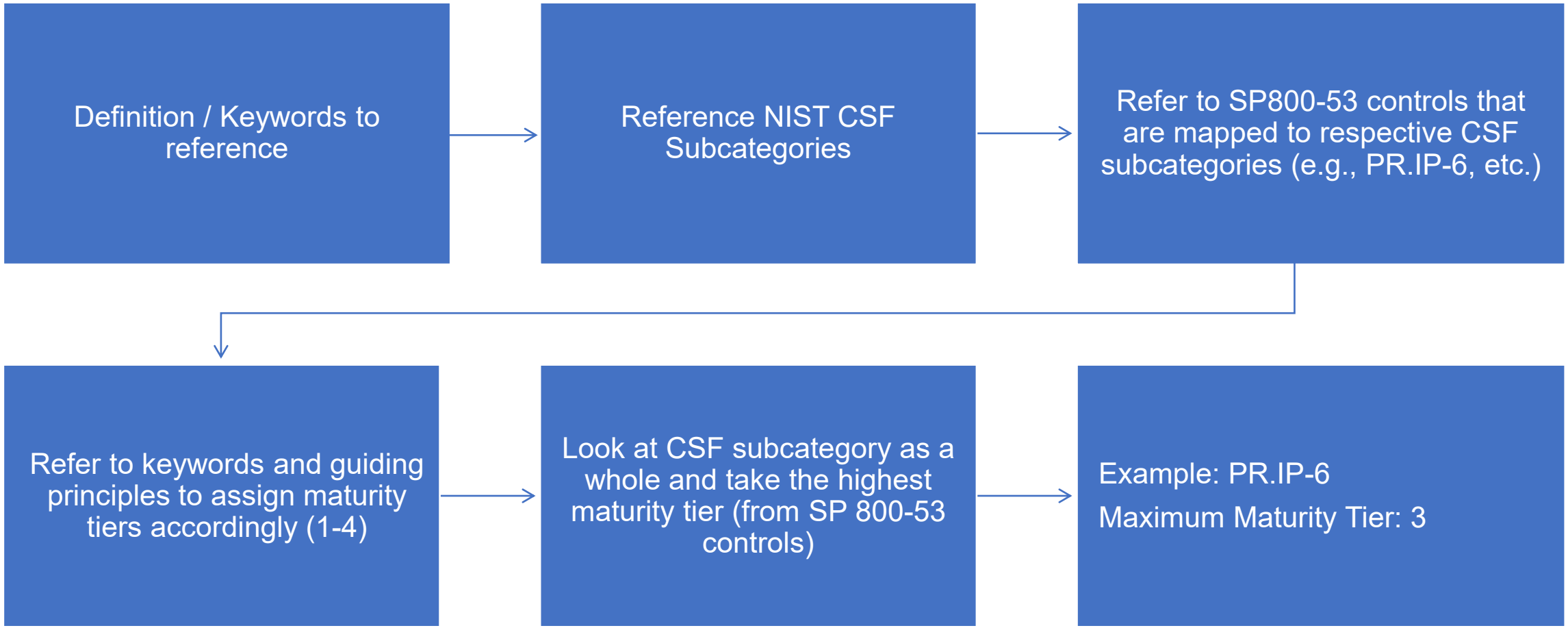
We assigned CSF maturity tiers to SP800-53 controls to achieve the objectives below

OBJECTIVES

1. Developing a common understanding that the maximum maturity Tier of a NIST CSF subcategory, e.g., ID.AM-1, may not be Tier 4 (Adaptive).
2. Allowing assessors to use this maturity tiering as a benchmark to calculate maturity scores using NIST CSF.

The process that we used to create the mappings is outlined below

MAPPING PROCESS



We researched different maturity frameworks to derive the keywords and guiding principles for mapping SP800-53 controls to CSF maturity tiers

MATURITY TIER KEYWORDS AND GUIDING PRINCIPLES

Maturity Tier	State	Final Keywords	Control Maturity Tier Guiding Principles
Tier 1	Partial	NA	Control is inadequate and is not applied consistently
Tier 2	Risk-Informed	Document, Assigned, Approved, Defined, Determine, Provide the means, Notify, Report, Risk-Informed, Advanced, Formalised	Control is adequate and implemented through a risk-informed approach but is not applied consistently, reviews are done on a specified periodic basis
Tier 3	Repeatable	Ensure, Audit, Authorized, Protect, Employ (the techniques, etc.), Retain, Established, Assess, Review, Repeatable, Enforced, Expert	Control is adequate and implemented through a risk-informed approach and reviews and improvement are done as and when the threat environment changes
Tier 4	Adaptive	Predictable, Managed, Automated, Capable, Consistent, Updated, Improved	Control is adequate and implemented through a risk-informed approach and reviews and improvement are done as and when the threat environment changes through automation and AI

- The maturity tiers are aligned with the NIST CSF
- The keywords were identified from our research on available maturity frameworks to streamline the understanding of different tiers of cybersecurity maturity implementation
- The guiding principles were created such that the keywords can be used in conjunction with the guiding principles to reduce ambiguity in interpreting maturity tiers

We show an example of the mapping of maturity tiers for PR-IP-6

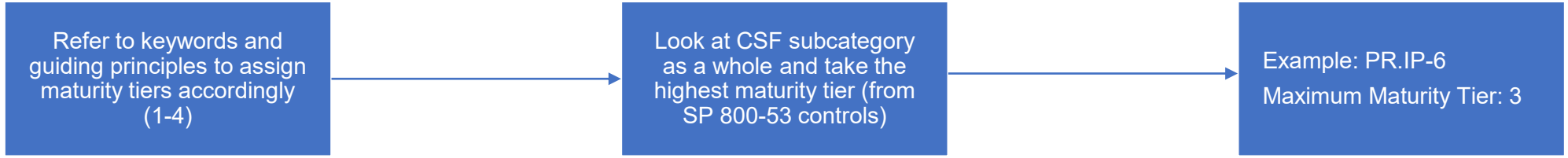
EXAMPLE OF THE MATURITY TIER ASSIGNMENTS TO SP800-53 CONTROLS (1/2)

Maturity Tier	State	Final Keywords	Control Maturity Tier Guiding Principles
Tier 1	Partial	NA	Control is inadequate and is not applied consistently
Tier 2	Risk-Informed	Document, Assigned, Approved, Defined, Determine, Provide the means, Notify, Report, Risk-Informed, Advanced, Formalised	Control is adequate and implemented through a risk-informed approach but is not applied consistently, reviews are done on a specified periodic basis
Tier 3	Repeatable	Ensure, Audit, Authorized, Protect, Employ (the techniques, etc.), Retain, Established, Assess, Review, Repeatable, Enforced, Expert	Control is adequate and implemented through a risk-informed approach and reviews and improvement are done as and when the threat environment changes
Tier 4	Adaptive	Predictable, Managed, Automated, Capable, Consistent, Updated, Improved	Control is adequate and implemented through a risk-informed approach and reviews and improvement are done as and when the threat environment changes through automation and AI

Function	Function Category	Subcategory	SP 800-53 Controls
PR: Protect	PR:IP: Information Protection	PR.IP-6: Data is destroyed according to policy	MP-6: Media Sanitization
			SR-12: Component Disposal

We show an example of the mapping of maturity tiers for PR-IP-6

EXAMPLE OF THE MATURITY TIER ASSIGNMENTS TO SP800-53 CONTROLS (2/2)



Function	Function Category	Subcategory	SP 800-53 Controls	SP800-53 Control maturity tier
PR: Protect	PR:IP: Information Protection	PR.IP-6: Data is destroyed according to policy	MP-6: Media Sanitization	3
			SR-12: Component Disposal	3

Maximum maturity tier for PR:IP-6 is 3.

Example MP-6:
The organisation:

Sanitizes [Assignment: organisation-defined information system media] prior to disposal, release out of organisational control, or release for reuse using [Assignment: organisation-defined sanitization techniques and procedures] in accordance with applicable federal and organisational standards and policies; and

***Employs** sanitiation mechanisms with the strength and integrity commensurate with the security category or classification of the information.

**We identify the keyword and use the guiding principles in order to assign the maturity tier of 3 to MP-6, and with both controls having the same maturity score of 3, we conclude that PR.IP-6 max maturity tier is 3, as its controls exhibit maturity tiers of up to 3.*

We referenced multiple frameworks to identify keywords to streamline our definition of the implementation tiers

ENSIGN'S DEFINITIONS OF IMPLEMENTATION TIERS (1/2)

Maturity Tier	State	Common Keywords	Example of Definition
Tier 1	Partial	Ad-Hoc, Initial, Undocumented, Reactive, Case by Case, Lack of Consistency, Basic	**Risk Management Processes**: Cyber teams lack the ability to prioritise and perform risk management activities in a consistent manner (adhoc), lack the ability to ensure the same outcome is delivered consistently via current risk management processes and / or lack risk management processes to guide activities / practices. **Integrated Risk Management Program**: Cyber risk management processes is driven by professional judgement, common consensus, best practices, reaction to an unexpected event, case by case basis, as-needed basis or a combination of the preceding options. Cyber risk management processes lack mechanisms to communicate risk to relevant stakeholders. Stakeholders making risk management decisions are poorly (inadaequately) informed of organisation's cybersecurity risk objectives, threat environment and business requirement, to manage cyber risk in a systematic manner. **External Participation**: Stakeholders (Organisation) do not exchange cybersecurity information with third parties. This results in poor understanding about the organisation's cybersecurity risks in (cyber) supply chain to itself and other organisations in the greater business ecosystem (e.g. sectoral, national, industry whether local, regional or international)
Tier 2	Risk- Informed	Risk-Informed, Advanced, Formalised	**Risk Management Processes**: Risk management practices are formalised within the cyber team. Cybersecurity practices are managed and enforced based on changes to the risk environment on periodically, rather than a risk- informed approach perspective. Integrated Risk Management Program: Cyber risk management processes is driven by professional judgement, common consensus, best practices, reaction on a periodic basis. Consistent methods are implemented to respond to risk changes. Cyber risk management processes are managed and communicated with relevant stakeholders. Stakeholders are informed of risk management decisions with organisation's cybersecurity risk objectives, threat environment and business requirement, to manage cyber risk in a systematic manner. **External Participation**: Stakeholders (Organisation) understands its own participation to sectoral, national and international ecosystem including its dependencies and dependents and periodically collaborates and exchange information for cybersecurity and complements it with internal information. while actively practice risk-informed approach in understanding the evolving cyber requirement.

We referenced multiple frameworks to identify keywords to streamline our definition of the implementation tiers

ENSIGN'S DEFINITIONS OF IMPLEMENTATION TIERS (2/2)

Maturity Tier	State	Common Keywords	Example of Definition
Tier 3	Repeatable	Establish, Expert, Defined, Repeatable, Enforced	**Risk Management Processes**: Risk management practices are formalised and enforced within the cyber team. Cybersecurity practices are adapted from the previous process with clear definition. Continuous improvement is performed for technology and processes to adapt to a changing threat and technology landscape. **Integrated Risk Management Program**: Cyber risk management processes is formalized and well-defined risk-informed policies, processes and defined procedures, implemented and reviewed to adjust for potential cybersecurity threats and event. Consistent and repeatable methods are implemented to respond to risk changes. Cyber risk management processes are managed and communicated with relevant stakeholders on a regular basis. Stakeholders are informed of risk management decisions with organisation's cybersecurity risk objectives, threat environment and business requirement, to manage cyber risk in a systematic and timely manner. **External Participation**: Stakeholders (Organisation) understands its own participation to sectoral, national and international ecosystem including its dependencies and dependents and periodically collaborates and exchange information for cybersecurity and complements it with internal information. while actively practice risk-informed approach in understanding the evolving cyber requirement. Stakeholders regularly collaborates and exchange information for cybersecurity and complements it with internal information. Organisation is capable of sharing cybersecurity information internally and externally taking a contributor role in its ecosystem. They possess real-time awareness of the cyber supply chain risks and proactively works with its vendors to maintain secure and strong supply chain relationships.
Tier 4	Adaptive	Predictable, Managed, Automated, Capable, Consistent	**Risk Management Processes**: Risk management practices are formalised and enforced within the cyber team. Cybersecurity practices are consistently adapted from the previous process with clear definition. Continuous improvement is performed for technology and processes to adapt to a changing threat and technology landscape, through automation and predictive technology **Integrated Risk Management Program**: Cyber risk management processes is formalized and well-defined with risk-informed policies, processes and defined procedures, implemented and reviewed to adjust for potential cybersecurity threats and event. Consistent and repeatable methods are implemented to respond to risk changes. Cyber risk management processes are managed and communicated with relevant stakeholders on a regular basis and decision-making is performed with full consideration for cybersecurity risks against business objectives. Stakeholders maintains a continuous appreciation of the changing risk position in view of real-time or near real-time measures of all risk dimensions, including cybersecurity risks, against internal and external conditions. **External Participation**: – Subject takes the leads for participating in the sectoral, national and international ecosystem including its peers, dependencies and dependents. Subject regularly collaborates and exchange information for cybersecurity and complements it with internal information. Subject shares cybersecurity information internally and externally providing detailed and timely information to its ecosystem. Organisation is capable of sharing cybersecurity information internally and externally taking a contributor role in its ecosystem and has a real-time or near real-time awareness of the cyber supply chain risks and proactively works with its vendors to maintain secure and strong supply chain relationships. Stakeholders regularly collaborates and exchange information for cybersecurity and complements it with internal information.

Ensign utilises the Mapping of SP 800-53 controls to calculate an organisation's maturity tier for a given sub-category

ENSIGN'S MEASUREMENT OF CYBERSECURITY MATURITY

Function	Function Category	Subcategory	SP 800-53 Controls	SP800-53 Control maturity tier	Control score
PR: Protect	PR:IP: Information Protection	PR.IP-6: Data is destroyed according to policy	MP-6: Media Sanitization	3	1
			SR-12: Component Disposal	3	1

Example:
Assessed Score for PR.IP-6 = (Total Control Score / Total SP 800-53 Control maturity tier) * Maximum maturity tier of 800-53 Control

*Assessed Score for PR.IP-6 = (2 / 6) * 3 = 1*

1. Use the formula for all subcategories in PR.IP.
2. Conduct the same formula over the 5 functions, ID, PR, DE, RS, RC and calculate the average.

Function	Current Score
Identify	1.9
Protect	1.5
Detect	1.7
Respond	1.0
Recover	2.2

Gain an understanding of organisation's maturity tier, measuring using the CSF and the mapped SP800-53 controls