ENSIGN INFOSECURITY

Draft of NIST Cybersecurity Framework 2.0 Core with Implementation Examples

Feedback to the Discussion Draft

6 November 2023

RESTRICTED

This Page is deliberately left Blank

[redacted]

6 November 2023

TO WHOM IT MAY CONCERN

National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899

RESPONSE TO THE REQUEST FOR FEEDBACK FOR THE DISCUSSION DRAFT OF THE NIST CYBERSECURITY FRAMEWORK (CSF) V2.0 CORE WITH IMPLEMENTATION EXAMPLES

We are pleased to provide our feedback on the latest proposed changes in the Discussion Draft of the NIST Cybersecurity Framework 2.0 Core dated 8 August 2023.

The opinions contained herein are Ensign's only. The opinions are provided for consideration in the development of the next version of the CSF only.

This document is prepared for NIST. Ensign InfoSecurity will not be held responsible for parties beyond NIST. The circulation of this document to parties beyond NIST must be communicated to Ensign InfoSecurity in writing.

We trust that you will find the contents of the document meeting your needs.

Please reach out to me at [redacted] for any further clarifications or collaborations.

Yours Sincerely

Mr. Teo Xiang Zheng

Vice President of Advisory

Ensign InfoSecurity (Singapore) Pte. Ltd.

[This is an electronic document and requires no signature]

Contents

1 About Ensign

Ensign InfoSecurity is the largest pure-play end-to-end cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address their clients' cybersecurity needs. Ensign's core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response. Underpinning these competencies is inhouse research and development in cybersecurity.

Ensign has more than two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region. More information can be found at https://www.ensigninfosecurity.com/.

The following input is prepared by Ensign Advisory, who provides cybersecurity advisory and assurance services to our clients.

2 Ensign Advisory's Context of Adopting NIST Cybersecurity Framework (CSF) in our Service Offerings

Ensign Advisory leverages the NIST CSF to advise our clients on their cybersecurity posture. The NIST CSF is the primary reference framework for Ensign Cybersecurity Maturity Framework and maturity assessments, where we determine our client's sophistication in understanding and implementation of cybersecurity and cybersecurity controls. After the maturity assessments, we devise improvement programs for clients referencing the NIST CSF. In addition to maturity programs, NIST CSF is a supplementary framework for other assessments, where other frameworks are dictated by client's scope of work.

3 Feedback to Discussion Draft of the NIST Cybersecurity Framework 2.0 Core with Implementation Examples

Ensign's input to NIST on the latest draft is as follows:

1. **Concrete improvements to the Examples**

   Ensign proposes that all implementation examples for respective subcategories should be aligned with Implementation Tiers (i.e., Partial, Risk-informed, Repeatable and Adaptive). We have provided illustrative examples for five (5) subcategories, namely **GV.RM-01**, **GV.SC-05**, **PR.AA-04**, **PR.PS-01** and **DE.A-07**. Kindly refer to **Table 1. Proposed Implementation Examples**.

2. **Whether the Examples are written at an appropriate level of specificity and helpful for a diverse range of organisations**

   Ensign proposes that Implementation Examples should be written and updated according to the technology landscape and common technology platforms, which may include, Information Technology (IT), Operational Technology (OT), Internet of Things (IoT), and others.

3. **What existing sources of implementation guidance might be readily adopted as sources of Examples (such as NICE Framework Tasks)**

   Ensign proposes the consideration of MITRE's additional useful resources such as the MITRE ATT&CK's mitigations, detections and data sources, MITRE D3FEND framework, and MITRE Engage framework. These are in addition to the already considered resources of NIST SP 800-53 and ISO 27001.

4. **How often Implementation Examples should be updated**

   Ensign proposes that the Implementation Examples be updated annually.

5. **Whether and how to accept Implementation Examples developed by the community**

   Ensign proposes that NIST consider how community/industry contributions to the MITRE ATT&CK framework is performed and selected contributions are then implemented into the 6-monthly updates to the MITRE ATT&CK framework. This could be supported by a permanently manned email account to collect and consolidate submissions and subsequently reviewed for inclusion into the annual update.

The review process could take an open or closed approach. The open approach will require possibly the use of the same consultation feedback management approach where the proposed implementation examples in a given period is published for feedback and then subsequently reviewed before inclusion into the final documents. The closed process will just skip the public consultation process and be handled by experts within and/or designated by NIST.

APPENDIX 1 - Proposed Implementation Examples

No.	NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	Proposed Implementation Examples
1	**GOVERN (GV)**		
	Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)	**GV.RM-01:** Risk management objectives are established and agreed to by organizational stakeholders (formerly ID.RM-01)	• **[Partial]** There is little to no visibility on risk management objectives in the organisations. Risk management activities are guided by decisions by senior leaders in response to ad-hoc events (e.g., major incidents, regulatory changes). • **[Risk Informed]** Objectives of cybersecurity risk management are discussed and established by senior leaders. However, risk management activities may not be aligned to such objectives (e.g., due to poor communication of objectives or poor measurements). • **[Repeatable]** Objectives of cybersecurity risk management are established as part of annual strategic planning and translated into measurements for risk management activities. Stakeholders, including third parties, understand such measurements and conduct risk management activities accordingly. • **[Adaptive]** Objectives of cybersecurity risk management are established as part of annual strategic planning and translated into measurements for risk management activities. Stakeholders, include third parties, understand such measurements and conduct risk management activities accordingly. Such measurements are incorporated into performance reviews to identify areas for improvement. Objectives and measurements of cybersecurity risk management are adjusted based on lessons learned.

No.	NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	Proposed Implementation Examples
	Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-05:** Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)	• **[Partial]** Cybersecurity risks in supply chain are not discussed, except in response to ad-hoc events. Requirements* in contracts and other types of agreements with third parties do not address cybersecurity risks associated with respective third parties. • **[Risk Informed]** Cybersecurity risks in supply chain are understood, which translate to established security requirements for suppliers, products, and services. However, the requirements are not always commensurate with their criticality level and potential impact if compromised. • **[Repeatable]** Cybersecurity risks in supply chain are understood, which translate to established security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised. Such requirements and how compliance with the requirements may be verified in default contractual language. • **[Adaptive]** Cybersecurity risks in supply chain are understood, which translate to established security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised. Such requirements and how compliance with the requirements may be verified in default contractual language. Rights and responsibilities of parties, and protocols for information sharing between parties, including any sub-tier suppliers, are defined in contracts and other types of agreements (e.g., to identify areas of improvement, coordinate activities during incidents). *Requirements may include, depending on criticality and potential impact if compromised:

No.	NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	Proposed Implementation Examples
			▪ Requirements in service-level agreements (SLAs) for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle ▪ Requirements for suppliers to disclose cybersecurity features, functions, and vulnerabilities of their products and services for the life of the product or the term of service; ▪ Requirements for suppliers to provide and maintain a current component inventory (e.g., software or hardware bill of materials) for critical products; ▪ Requirements for suppliers to vet their employees and guard against insider threats; ▪ Requirements for suppliers to provide evidence of performing acceptable security practices through, for example, self-attestation, conformance to known standards, certifications, or inspections.

No.	NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	Proposed Implementation Examples
2	**PROTECT (PR)**		
	Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	**PR.AA-04:** Identity assertions are protected, conveyed, and verified	• **[Partial]** Protection of identify assertions for each system and / or physical operating site (e.g., office, server room, data centre) is **left to the discretion of the system custodians / owners** (e.g., direct adoption of vendor guidelines and industry best practices). • **[Risk-Informed]** Protection of identify assertions for each system and / or physical site is supported by **technological solutions** such as Active Directory. The practices are **largely manual** and would be informed by cyber threat landscape, business / mission requirements, organization risk objectives (e.g., multi-factor authentication) and / or technological landscape at a point in time. • **[Repeatable]** Protection of identify assertions for each system and / or physical site is **largely automated** using Privileged Identity Management (PIM) and Privileged Access Management (PAM) and Identity Access Management (IAM) solutions, following a process. The protection process is **established** and **communicated** through an **organization-wide approach** by competent personnel. • **[Adaptive]** Protection of identify assertions for each system and / or physical site is **fully automated. Changes in status of identity** (e.g., user performing abnormal transactions) require **re-assertions of identity** when detected (i.e., adaptive authentication).

No.	NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	Proposed Implementation Examples
	Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-01:** Configuration management practices are applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)	• **[Partial]** Hardened baselines for hardware, software and services used by the organization are **left to the discretion of the system custodians / owners** (e.g., direct adoption of vendor guidelines and industry best practices). • **[Risk-Informed]** Hardened baselines are established, tested, deployed, and maintained. The practices are **informed** by cyber threat landscape, business / mission requirements, organizational risk objectives (e.g., principle of least functionality) and / or technological landscape **at a point in time**. This includes performing risk assessment, impact analysis and including remediation steps to address risks raised for configuration changes. • **[Repeatable]** Establishing, testing, deploying, and maintaining of hardened baselines are **largely automated** using Configuration Management Database (CMDB), following a process. The process shall be **established** and **communicated** through an **organization-wide approach** by **competent** personnel. This may include an established template for request of change documenting required information such as justification of request, assets / systems that will be affected, risk and impact of making these changes. • **[Adaptive]** Establishing, testing, deploying, and maintaining of hardened baselines are **fully automated**. Changes in cyber threat landscape, business / mission requirements, organizational risk objectives (e.g., technology, operational, regulatory, financial, reputational) and / or technological landscape are **actively adapted** to update the practices. For example, technical configurations in patch advisories are incorporated into hardened baselines as updates at a frequency that commensurate with the criticality of the vulnerability (i.e., CVSS).

No.	NIST CSF 2.0 Category	NIST CSF 2.0 Subcategory	Proposed Implementation Examples
3	**DETECT (DE)**		
	Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	**DE.AE-07:** Cyber threat intelligence and other contextual information are integrated into the analysis	• **[Partial]** Acquisition of cyber threat intelligence (e.g., vulnerability disclosures) for organization's hardware, software and services used, is **reactive** and **lack coverage**. The analysis of acquired cyber threat intelligence to identify potential adverse events is left to the **discretion of unqualified and / or untrained personnel**. • **[Risk-Informed]** Acquisition of cyber threat intelligence (e.g., vulnerability disclosures) for **all** of organization's hardware, software and services used, from **authenticated** sources (e.g., has mechanisms to validate legitimacy of information and origin) on a **regular** frequency. The analysis is **informed** by business / mission requirements, organizational risk objectives (e.g., technology, operational, regulatory, financial, reputational) and / or technological landscape **at a point in time**. • **[Repeatable]** Acquisition of cyber threat intelligence (e.g., vulnerability disclosures) is **largely automated** using Threat Intelligence Platforms (TIPs), following a process. The integration of cyber threat intelligence into the analysis shall be **performed** by **competent personnel.** • **[Adaptive]** Acquisition of cyber threat intelligence (e.g., vulnerability disclosures, threat landscapes) is **fully automated.** The integration of cyber threat intelligence into the analysis shall include **correlating** lower-order (operational and tactical) cyber threat intelligence into higher-order (strategic) cyber threat intelligence to **inform** executive-level decision making in taking actions to address potential risks and impact to the organization.

About Ensign InfoSecurity

Ensign InfoSecurity is the largest pure play cybersecurity company in Asia Pacific with over 800 cybersecurity professionals.

Our clients trust and rely on us to bring our collective capabilities across Advisory, Consulting, Systems Integration, Managed Services and Labs to deliver cyber excellence.

We work with our clients to transform them into cyber-resilient leaders, helping them **Conquer the Unknown**.