ENSIGN INFOSECURITY

# National Institute of Standards and Technology (NIST)

## Response to the Request for Feedback for the Discussion Draft of the NIST Cybersecurity Framework (CSF) v2.0 Core

26 May 2023

CONFIDENTIAL

This Page is deliberately left Blank

Ensign InfoSecurity (Singapore) Pte. Ltd.

[redacted]

**26 May 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**

We are pleased to our feedback based on the latest proposed changes in the Discussion Draft of the NIST Cybersecurity Framework 2.0 Core dated 24 April 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 approved by 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, Consulting

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 history 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 Consulting, who provides cybersecurity advisory and assurance services to our client.

# 2 Feedback on proposed changes to NIST CSF 2.0 Core

## 2.1 Proposed Revisions and Introduction of Considerations

| No. | CSF 2.0 Category | CSF 2.0 Subcategory | Comments from Ensign |
|---|---|---|---|
| 1 | **GOVERN (GV)** | | |
| 1a | | | We suggest that a **Crisis Communication** category be included under the GOVERN function to address the need to establish strategy and plans to engage internal and external stakeholders to maintain confidence, reputation, and manage the risks of Misinformation, Disinformation and Malinformation. |
| 1b | Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established and used to support operational risk decisions (formerly ID.RM) | GV.RM-08: Effectiveness and adequacy of cybersecurity risk management strategy and results are assessed and reviewed by organizational leaders | We suggest that GV.RM-08 should specify the need to establish Key Risk Indicators (KRIs) and specific risk thresholds as part of cybersecurity risk management strategy. |
| 1c | Policies and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures are established and communicated (formerly ID.GV-1) | | We suggest that a subcategory be introduced in GV.PO which details what should be included in an Incident Response Plan as it is no longer addressed in the RESPOND function.<br>Considering that the RESPOND function is more focussed on the operational effects and that the established policies and procedures are now part of the newly proposed GOVERN function.<br>**Example:**<br>*GV.PO-04: Incident Response Plan must include steps that cover preparation, detection, containment, investigation, remediation and recovery from an incident.* |

| No. | CSF 2.0 Category | CSF 2.0 Subcategory | Comments from Ensign |
|---|---|---|---|
| **2** | **IDENTIFY (ID)** | | |
| 2a | Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation),<br>organizational assets, and individuals | ID.RA-02: Cyber threat intelligence is<br>received from information sharing forums and sources | We suggest that a subcategory be included under ID.RA to address the development of a threat model based on the cyber threat intelligence received. This could be to revise ID.RA-02 as follows.<br>**Example:**<br>*ID.RA-02: Develop and maintain an organisation threat model based on cyber threat intelligence that is*<br>*received from information sharing forums and sources*<br>OR<br>to have a subcategory specifically for developing a threat model based on threat intelligence.<br>**Example:**<br>*ID.RA-11: Develop and maintain organisation threat model based on cyber threat intelligence*<br>We believe that by developing and maintaining an organisation threat model (and monitoring changes to the threat landscape), the organisation will be able to identify and take relevant actions to the risks that arise. |
| **3** | **PROTECT (PR)** | | |
| *Ensign has no comments on the PROTECT function* | | | |
| **4** | **DETECT (DE)** | | |
| 4a | | | We suggest introducing a category to address the need to perform sense-making between business, operations, and cybersecurity.<br>This is particularly to address the need to correlate dependencies, and maintain situation awareness. |

| No. | CSF 2.0 Category | CSF 2.0 Subcategory | Comments from Ensign |
|---|---|---|---|
| 5 | RESPOND (RS) | | |
| 5a | Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed (formerly RS.RP) | RS.MA-01: The incident response plan is executed (formerly RS.RP-1) | We suggest that RS.MA-01 can be revised to be more specific as follows:<br>**Example:**<br>*RS.MA-01: The incident response plan is executed to achieve containment, eradication, and recovery from an incident.*<br>This is to address the removals of the subcategories in the RESPOND function. |
| 6 | RECOVER (RC) | | |
| *Ensign has no comments on the RECOVER function.* | | | |

## 2.2 Improving expectations and evaluation through mapped implementation examples

We applaud the attempts to include implementation examples to each subcategory. We would encourage the further development to indicatively suggest the implementation example matching a given implementation tier. This should help to improve the expectation and evaluation of practices implemented.

## About Ensign InfoSecurity

Ensign InfoSecurity is the largest pure play cybersecurity company in Asia Pacific with over 500 cybersecurity professionals.

Our clients trust and rely on us to bring our collective capabilities across 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.