[redacted]

Subject: EXT :FW: Feedback on CSF 2.0 Call for Comments
Date: Thursday, March 9, 2023 1:28:44 PM
Attachments: image001.png
image002.png
image003.png
image004.png

FYI

[redacted]

Sent: Wednesday, March 1, 2023 2:51 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Feedback on CSF 2.0 Call for Comments

Hi NIST CSF 2.0 team,

My name is Nigel Hedges, I am the Group Head of Cybersecurity (CISO) for Kmart Group (Kmart and Target) in Australia. (50,000 employees, $4bil USD revenue)

1.1: Agreed.

1.2: It should be noted that NIST CSF is used extensively in many Australian enterprises, across retail (bricks & mortar and online), pharmaceuticals, health, financial sector, retailers etc. Australian Government refers their Information Security Manual to several SP800 documents as informative references.

https://www.cyber.gov.au/acsc/view-all-content/advice/using-information-security-manual [gcc02.safelinks.protection.outlook.com]

1.3 The International Cybersecurity and Privacy Resource site, should contain a list of working committees for international parties (inclusive of membership organisations, such as the Australian Information Security Association) that can be listed as parties willing to work on 2.0 and future versions. It would be good if NIST CSF 2.0 could highlight these resources.

2.1: Agreed.

2.2: Agreed. A diagram that connects the RMF, PF and other important SP800 documents such as SP800-53 would be excellent. I don't think it is particularly and clearly understood that NIST CSF and SP800-53 have a wonderful relationship between high level governance guidance + recommendations around execution.

2.3: Agreed, excellent. Will this extend to flexible maturity models? Some large organisations here in Australia use CMMI as the maturity yard stick.

2.4: ISO27001:2022 and ISO27002:2022 have effectively mapped to NIST CSF functions within their ISMS governance + management. Would it not be suitable to make sure the informative references for 2022 editions are updated?

2.5: I would not be able to provide Australian Government ISM or Cyber mitigation mappings by end of 17 March, but would like the opportunity to provide it before a future deadline? If it's already covered – great.

2.6: Agreed. Can't wait for SP800-63. Hugely valuable.

3.1: Companion Guide option. I think for organisations using CMMI 5 levels of maturity, these implementation examples to CMMI would be extremely helpful. It would allow for contribution for specific maturity frameworks by community.

3.2: Agreed.

3.3: Agreed, please make the website more Internationally friendly. I appreciate it is primarily for the US domestic market, but maybe an international section?

4.1: Agreed, excellent. Will you align with the ISO27001 governance suggestions? Understand organisational context, get leadership support, adequately plan, establish support and competency, operationalise, establish performance metrics/mgt, and establish continuous improvement.

4.2: Agreed. (RMF/31000) Also, the FAIR methodology around Cyber Quantification of Risk is gaining a lot of traction. Is there an opportunity to also include the value (pros and cons) of Qualitative and Quantitative approaches? I think FAIR has a very good way of creating financial cost analysis of risk scenarios, that can provide a narrative for change.

5.1: Great. A welcome expended coverage. Gartner's ***2022 Strategic Supply Chain Technology Themes*** document published 25 March 2022, discusses Security Mesh as a vital pillar, and describes the definition as "…a structured framework of governance, collaboration and applied technology applications that are orchestrated from within supply chain." Worth a read, and potential footnote? Document ID: G00759007.

Agree on Secure Software Development Framework.

6.1: Agreed, as previously mentioned would be good to see if CMMI could be more prominent.

6.2: Understood, the examples of CMMI would be sufficient.

6.3 Agreed, excellent.

6.4: Sure, but this is where CMMI can be a useful maturity mechanism.

Potentially Missing:

- NIST CSF 2.0 should be clear that Cyber is “pushed” from Risk, but “pulled” by Business Strategy. I always felt that in v1.1 page 12, the diagram of “information and decision flows” missed an opportunity to express how NIST CSF could be used to connect to business and tech strategy. The purpose of doing this, is as organisations apply NIST CSF – they can be clearer on what initiatives are GAPS or DUPLICATION of effort. This helps establish confidence in folks executing NIST CSF.

  SABSA, is a business security architecture model that focuses on aligning cyber with tech strategy and business strategy. There’s an opportunity to impress upon NIST CSF consumers to align cyber strategy to business strategy, the “Through-Life” method is a great abstraction, probably best captured in diagrams for audience… maybe a reference to SABSA?

https://sabsa.org/sabsa-executive-summary/ [gcc02.safelinks.protection.outlook.com]

Mostly really pleased with the direction that 2.0 is going, thank you. Can’t wait to see the draft.

Best regards,
Nigel

Nigel Hedges

Group Head of Cybersecurity
Kmart Group Technology

[gcc02.safelinks.protection.outlook.com]
[gcc02.safelinks.protection.outlook.com]
[gcc02.safelinks.protection.outlook.com]

[redacted]
