From: Nury, Amandine
To: cyberframework
Subject: EXPERIAN | Appreciation, Feedback, and Questions on NIST CSF 2.0 Draft Version
Date: Thursday, November 2, 2023 11:27:15 AM
Attachments: image003.png

Dear NIST CSF,

As an organization deeply committed to cybersecurity excellence, we at Experian are truly grateful for the invaluable contributions of the NIST CSF. With immense appreciation, we would like to extend our gratitude for the recently released CSF 2.0 draft version. The NIST CSF has been an instrumental framework for us, serving as a cornerstone in our cybersecurity practices across various functions of our organization. We have found immense value in leveraging the CSF to fortify our defenses, mitigate risks, and promote a culture of proactive cybersecurity within our company.

Having thoroughly reviewed the draft, we are eager to offer our feedback and pose a few questions to further solidify our understanding and maximize the benefits of the CSF 2.0. We highly value your expertise and would be grateful for any insights and answers you can provide. Your guidance will undoubtedly strengthen our implementation of the framework and enable us to continue safeguarding our data and the interests of our clients and partners.

1. Lack of clarity regarding maturity measurement in sub-category:
In our exploration of the new governance function (GV.OV-1,2 and 3), we have observed mentions of risk management activities and performance. However, there appears to be a lack of clarity when it comes to maturity assessments and measurement. While we appreciate the addition of this new aspect, we believe it would be beneficial if the CSF could provide more specific guidelines and a well-defined framework for assessing cybersecurity maturity, tracking progress, and establishing improvement objectives.

2. Cloud VS on-premise specifics:
Different security considerations often arise when comparing cloud-based environments with traditional on-premises setups or when both environments are equally present.
How does the NIST CSF 2.0 address the challenge of assessing the maturity of mixed environments, considering that certain questions may have distinct answers for cloud and on-premises setups? Are there specific guidelines or provisions in the framework that account for the unique security considerations and control requirements of both environment?

3. Limited Metrics and Measurement Guidance:
Although the NIST CSF encompasses various functions that involve metrics and reporting, it is notable that the newly introduced governance function or the restructured aspects in the identify function have not received similar attention in terms of metrics and measurement guidance. While the framework offers a solid foundation for managing cybersecurity risks, identifying and adopting relevant metrics to assess the efficacy of cybersecurity programs remains limited. Therefore, comprehensive guidance on the selection and implementation of appropriate metrics would greatly enhance the usefulness of the CSF in this regard.

4. Privacy Considerations:
Although the NIST CSF acknowledges the importance of privacy, its coverage of privacy risks is not exhaustive in 2.0. This raises concerns, particularly for companies like Experian that handle vast amounts of data. Organizations would greatly benefit from more in-depth information and practical implementation examples regarding privacy controls and how to effectively tackle privacy-related challenges.

5. Mention of AI:
The NIST CSF 2.0 does not explicitly address the rapidly evolving field of artificial intelligence (AI) and its associated cybersecurity implications. Would you confidently say that the newly developed framework fully encompasses the risks and challenges related to artificial intelligence (AI)?

6. Moving the subcategory *'GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities*' from Govern to Respond makes sense if the focus is on incident management and response.
It aligns the ownership with the corresponding function responsible for those activities.

7. Moving the subcategory *'PR.PS-04: Log records are generated and made available for continuous monitoring'* from Protect to Detect seems reasonable if the logs are primarily used for monitoring and detection purposes. Placing it under the Detect function ensures better alignment with the function responsible for monitoring and detection activities.

8. Question: The subcategory 'RS.MA-05: The criteria for initiating incident recovery are applied' in the Respond function implies that there are specific criteria that must be met before initiating the incident recovery process.
Although criteria for initiating incident recovery can vary depending on several factors, including the nature of the incident, the organization's risk tolerance, and the criticality of the impacted systems or assets; Is it more beneficial for the objective of the subcategory to be focused on defining the criteria for initiating incident recovery?

Thank you for your unwavering commitment to cybersecurity excellence and for considering our feedback.

Best regards,
Amandine Nury
EGSO | Senior Strategic Cyber Maturity Program Lead
[redacted]
www.experian.com