From: Ron Lear
Sent: Wednesday, March 8, 2023 2:35 PM
To: cyberframework <cyberframework@nist.gov>
Subject: NIST CSF 2.0 Team - NIST Concept Paper - ISACA Feedback and Comments

Dear NIST CSF 2.0 team:

Thank you for the opportunity to submit comments for, and participate in the recent CSF 2.0 workshops. As requested, the following contains ISACA's collective input regarding the Concept paper topics and questions.

ISACA Responses to CSF Concept topics:

1. Do the proposed changes reflect the current cybersecurity landscape (standards, risks, and technologies)?

    - ISACA Response: For the most part, yes, with some additional considerations:
        - A balance must be struck between ease of entry and adoption and enough detail with proven implementation practices (examples and options)
            - For example, high-level is needed to explain the CSF to C-Suite and practitioners (different audiences/different messages/takeaways), but example implementation detail is helpful to give adopting organizations/functions ideas of HOW to implement and they will vary based on industry/domain. Lastly, should consider how (and where) in an organization the framework is needed vs. regulatory or other standards.

2. Are the proposed changes sufficient and appropriate? Are there other elements that should be considered under each area?

    - ISACA Response: Some additional considerations of either missing items or items that need more emphasis:
        - "Systems thinking" approach – holistic, inclusive and integrated from beginning of life cycle (whether business, development, service, supply chain) – should not be "bolt on" approach, but integrated within the framework (so for example, don't make SCRM a separate category – comes across as somewhat "after-thoughtish" or "bolt on" vs. integrated where needed in the CSF subcategories). Systems thinking describes a complex network of events, relationships, technologies, processes and people interacting in expected and unexpected ways. It is a holistic approach that focuses on the way a system's parts interrelate rather than focusing on a system's component parts.

- Continuous monitoring/continuous improvement – compliance approach is one thing, but doesn't address currency, relevance, and performance-thinking vs. compliance-only
- Data governance and data/information thinking are also needed, not just systems thinking– data governance, data security, data use, data quality, predictive modeling; and should include data created, data transmitted, data transformed, data at rest, and data destroyed/archived
- Alignment of cybersecurity requirements and clear flow-down to critical suppliers (not necessarily all suppliers) – should be driven by clear criteria, key or critical components, single-points of failure/risk, critical infrastructure and operations, etc.
- Assessment and performance are continued to be talked about together, and while there is a connection between the two – consider making it clear that assessments focus on evaluating and "benchmarking" compliance and performance against the CSF, assessment method is needed to ensure consistency, integrity and fidelity of implementation. From an assessment perspective, a separate assessment methodology with clear "leveling" criteria (Many folks at the workshop referenced CMMI as the way they measure – by either capability or maturity levels. NIST should drive this for consistency in assessment quality and fidelity, but also allow flexibility for adoption – consider self-evaluation, interim evaluation (by internal teams or independent teams) up to full formal assessments to assign capability or maturity levels. ISACA is happy to explain and share our current CMMI, COBIT, and Digital Trust Ecosystem Framework (DTEF) assessment methodology, approach, and tools with NIST if that would be helpful.
- Whereas performance measurement is identifying target business, and then aligned/related performance measurement needed to demonstrate that the objectives can be met. Should be clearly defined operational definitions of measures, and alignment and understanding of status and reactive measurements vs. proactive and then eventually predictive – all are needed at various part of an organization and at various maturity levels.
- SCRM: As alluded above, not every entity in the supply chain will be necessary – but there should be a focus on prioritizing which suppliers, processes, objectives, and requirements are needed to achieve the required level of cybersecurity compliance and resilience.

3. Do the proposed changes support different use cases in various sectors, types, and sizes of organizations (and with varied capabilities, resources, and technologies)?

- ISACA Response: Some additional considerations of either missing items or items that need more emphasis:

    - Detail shouldn't be prescriptive, but more "how with options" – perhaps eventually consider a curated marketplace of detailed domain implementation guidance or different industry "views" submitted by industry and vetted/curated
    - Consider that eventually there will likely be different vertical or domain views that will arise – Consider how can these be promoted, shared, and how wide-spread adoption can be achieved

4. Are there additional changes not covered here that should be considered?

    - ISACA Response: Not at this time

5. For those using CSF 1.1, would the proposed changes affect continued adoption of the Framework, and how so?

    - ISACA Response: See above comments on balance between comprehensiveness and accessibility, people and organizations need a way to "ease" into the framework and digest it in manageable chunks – tied to "pain points" in their business to address first and show improvement.
    - Consider a separate "CSF Implementation Guide" that will aide an adopting organization in getting started, assessing, etc.

6. For those not using the Framework, would the proposed changes affect the potential use of the Framework?

    - ISACA Response: Refer to response to Question 5

Thank you again for the opportunity to participate and provide input. We look forward to our continued collaboration with the NIST team and community, and please don't hesitate to reach out to me directly as needed with any questions or additional input.

Ron Lear, CHMLA, LSSGB, ISO Lead Auditor
Vice President, Frameworks and Models