From: Sara Ricci
To: cyberframework; Sara Ricci
Subject: NIST CSF draft 2.0 comment
Date: Monday, September 18, 2023 4:13:11 AM

Dear NIST CSF team,

Thank you for the opportunity to provide feedback on the CSF Draft v2.0.
The updates immensely enhance the value of the framework as a guide to manage cyber risk. While v1.0 is a great start and has found wide appreciation, the addition of the new Governance domain takes it beyond an incident management focus to a more strategic level. It is developing into a more comprehensive Risk management framework in integrating cyber risk with ERM, calling out supply chain and other governance components.

I would like to offer a few recommendations for your consideration as follows:

NIST CSF Draft recommendations for update/clarification:

GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated (formerly ID.BE-04, ID.BE-05)
Add:
Ex4: Establish criteria for timing of Board reporting of cyber incidents e.g. breach of risk tolerance limit/level of impact e.g. compliance, financial, regulatory, operational, reputational Define what would require crisis communication of an incident to the Board based on materiality.
Add:
Ex5: Determine how the organization will communicate with external stakeholders such as customers, public authorities, industry organizations and general public. Establish a Corporate communication protocol to streamline the messaging in order to ensure clarity, accuracy and timeliness.

GV.RM-03: Enterprise risk management processes include cybersecurity risk management activities and outcomes (formerly ID.GV-04):
Ex1: Aggregate and manage cybersecurity risks alongside other enterprise risks (e.g., compliance, financial, regulatory, **operational, reputational**)
Ex3: Establish criteria for escalating cybersecurity risks within Enterprise Risk Management **– prioritization based on type and level of impact – compliance, financial, regulatory, operational, reputational**

GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated:
Ex1. Specify criteria for accepting and avoiding cybersecurity risk for various classifications of data **based on extent and type of impact of loss of data confidentiality, integrity or availability against risk tolerance levels within the risk appetite**

GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties:
Ex3: Identify how third parties will communicate with the organization about cybersecurity risks.

I believe this section refers to internal communication of risks emanating from suppliers and other third parties, not for third parties to communicate cyber risk.
Recommended update:
Ex3: **Identify how the risks from suppliers and other third parties will be communicated across the organization. Establish reporting structures, committees, etc. to share information about the third party's cyber risk to the organization. To gather the data from the third party, establish the frequency of communication with the third party as part of managing SLA and Third Party oversight, define triggers for ad hoc/crisis communication, establish a communication protocol for conducting third party audits.**
Add:
Ex4: Establish standardized taxonomy for cyber risk to be incorporated into or utilized in conjunction with ERM for clarity of communication

Within the Risk management section, an articulation of Controls is recommended. Cyber risk is an Operational risk that is also an Enterprise level risk that must be considered at the Executive/Board level

GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
Add:
Ex5: Periodically test that cyber risk control design is adequate and in compliance with internal policies and external legal, regulatory and mandatory security standards (e.g. HIPAA, PCI-DSS, privacy laws etc.)
Add:
Ex6: Periodically test effectiveness of controls i.e. key controls mitigate the inherent risk to an acceptable residual risk level and identify compensating controls or workarounds where they may be required
Add:
Ex7: Establish a process for Issue management for remediating control breaks- escalating those where there is impact to the organization- e.g. compliance, financial, regulatory, operational, reputational or any other criteria critical to the organization measured against risk tolerance thresholds
Add:
Ex8: Conduct lessons learned and thematic reviews to identify process improvements related to people, process and technology

GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
Add:
Ex5: Establish an Executive level Cyber Risk Management Committee or incorporate Cyber in Enterprise Risk Management Committee for Executive oversight
Add:
Ex6: Board should include members who have understanding of cyber risk. Information Security organization should conduct periodic training and awareness for the Board to elicit meaningful

discussion that can lead to strategic decision making
Add:
Ex7: With Board accountability for oversight of cyber risk, in conjunction with the information security function's accountability for managing cyber risk, D&O insurance coverages may need review.

GV.RR-03: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies:
Add to Ex1: **Discussion on cyber program maturity and gaps will help the Board and Executive management to align resources to fund budgets for program improvement.**

GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions
Ex3: Calculate, document, and prioritize positive risks alongside negative risks **(e.g. Disruptive Technology risk such as artificial intelligence - prioritize adoption and innovation to gain competitive advantage, along with balancing negative impact such as impact on privacy due to potential for misuse by bad actors)**

GV.SC-04: Suppliers are known and prioritized by criticality:
Ex1. Sentence needs to be updated- Criticality may include- **Organization's dependency on third party from a resilience perspective- e.g. is it a SPOF, single source/sole provider; level of spend; geo location to account for geopolitical risk to the supply chain**

GV SC 05- Ex10 and GV SC 06- Ex 3:
Replace "tier" by "subservice provider/subcontractor" to refer to the provider's suppliers i.e. supplier's Third Party/Fourth Party and so on, in the supply chain.
This will avoid confusion with Sourcing/Procurement that use Tiers for classification by spend and Resiliency Plans where tiers refer to business process criticality to identify critical providers

GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)
Ex5 is too vague - Plan for unexpected supplier and supply chain-related interruptions to ensure business continuity
Add:
Identify supplier dependencies in business continuity plans and plan for supplier redundancies or workarounds for critical processes where the supplier may be a SPOF. Understand the impact of unavailability of a critical supplier and plan for risk mitigation actions.
Add:
Ex6: Security should work with Procurement and Legal to ensure all security considerations are embedded in the contract. Supplier should be onboarded after security risk assessment is completed and any risk treatment measures that were identified have been addressed.

GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and

service life cycle:
Add:
Ex6: Escalate open issues related to critical suppliers and service providers so that they are remediated timely and any impact to the organization from the related risk is understood and managed appropriately

GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement
Ex3: Verify that supplier access to organization resources is deactivated promptly when it is no longer needed
Recommended update:
Ex3: **Perform timely offboarding of the third party at end of supplier relationship and** verify that supplier access to organization resources is deactivated promptly when it is no longer needed

Thanks again for your review and consideration of the feedback you have kindly solicited.

Regards,

Sara Ricci