From: [redacted]
To: cyberframework
Subject: Comments on NIST Cybersecurity Framework 2.0 initial public draft
Date: Monday, October 2, 2023 5:39:34 PM

Please find my feedback on the draft framework:

70: I support the risk framing but suggest an additional component is added. The way that cyber risk is managed and the tradeoffs are pertinent. Specifically where cyber risk is managed based on vulnerabilities you risk a whack a mole approach which nets an increased risk overall. e.g. If you delay the implementation of data access control tool until all identity controls are fully automated you risk a net higher risk position. Suggested wording, "Cyber risk should be managed holistically. Mitigating activity should consider total risk over time to ensure a tactical action (or inaction) to address a vulnerability doesn't introduce a larger risk than the one being mitigated.

105: A practical observation is that those implementing the CSF often don't consider interdependencies. Common Criteria addresses this in a rather intense way (by contrast). I wonder if understanding cyber security risk should include understanding dependencies between Function categories. The most common example I see is asset management is marginalised but it is critical to most categories that follow. Suggested wording, "Identify dependencies between framework components and how a weakness in one area can materially impact the maturity of another". This is supported on line 226 which talks to the relationship between functions but could be reworded slightly to make clear that in addition to supporting each other, shortcomings in functions limit the effectiveness of other functions.

310: A framework profile is created for an organisation. Further on the framework highlights that a profile has a scope and an entity can use different profiles for different parts of its operation. Suggest adding "Scope" to the graphic to make clear early that the scope isn't limited to a (e.g.) company and everything it does.

315: I don't think outcomes an organisation is attempting to achieve should be in the current profile. They should be in the target profile as it is where the desired state is captured (trying is just a intent).

319: Suggest minor reword from, "A Target Profile takes into account anticipated changes.....", to "A Target Profile communicates anticipated changes...". Additionally threats are not part of the profile, they are influences of the profile. ie the profile address the risk associated with a threat, it does not document the threat.

327: Suggest it is worth noting that a where an organisation profile is lesser than a community profile, this constintutes a risk the organisation presents to the community.

333: Suggest expanding to explicitly reference benchmarking given the importance of relative performance with senior stakeholders. Add bullet, "Benchmark cybersecurity maturity against sector, organisational divisions or supply chain partners"

393: To reinforce the notion of a cybersecurity programme being ongoing suggest rewording, "implementing an action plan can take months or years", to, "the cyle of plan and execute could be annual, quarterly or monthly depending on organisational funding and delivery

models"

410: A common issue in risks management practices in cyber is that risk statements aren't relative. e.g. Cyber specialists often consider the residual risk of a threat actor compromising a critical asset to justify investment or change; instead of stating the inherent for the organisation and the residual risk relative to other risk types. To that end I think it worth emphasising that risk management should be relative to scope. ie You compare a cyber risk for a BU against other risks within a BU or against a cyber risk in another BU. You don't compare a cyber risk in a BU against another organisation as the comparison isn't consistent. Suggest adding, "Care should be taken to consider context when using cyber risk to communicate issues or prioritise investment.

458: Rather than complement the risk management frame work it should ideally link. A practical observation is that Cyber often makes progress but it doesn't show up in the risk system. Suggested rewording, "Tiers should be used to complement an organization's cybersecurity risk management methodology rather than take its place. For example, an organization can use the Tiers to communicate internally as a benchmark for a more organization-wide approach to managing cybersecurity risks as necessary to progress to a higher Tier. Not all organizations need to be at a particular Tier (e.g., Tier 3 or 4)", to, "Tiers should be used to complement or ideally align with an organization's cybersecurity risk management methodology rather than take its place. For example, an organization can use the Tiers to communicate internally as a benchmark for a more organization-wide approach to managing cybersecurity. Alignment could be achieved by predetermining what tier was required across control areas to material move the organisations residual cyber risk rating where the controls address threats or vulnerabilities that contribute to the elevated residual position. "

485: The term security posture is used inconsistently. Suggest rewording, "cybersecurity risks and posture", to, "cybersecurity posture as context for the risks resulting from it". To me the Framework allows you to create a profile that defines your posture and you can use that posture to determine your residual risk position based on your inherent risks.

635: I think it worth making the point that risk provides a "currency" to compare risk types. ie Senior stakeholders may understand legal risk or cyber risk but are unlikely to understand both in detail. Risk becomes a currency to explain priorities between those two areas. Suggest adding a statement along the lines of, "Managing cyber risk consistently with other risk types allows for informed tradeoffs to be made between disparet risk types such as cyber and legal."

761: I think this template needs expanding to be a whole page showing cutouts of mocked up artefacts to show components fitting together and being used in different forum. The template is often used by technical specialists in a literal sense and is presented as an excel spreadsheet because that is what is in the framework. Stakeholders will often require rolled up views or extracts of key priority areas or subsets of information that is applicable to them. Showing a mockup of a couple of entries and how they would surface to each of the audiences listed in the framework would make clear it should not be verbatim. Information should be tailored so it can be consumed by the applicable audience. I could provide an elaboration of this concept but the feedback format doesn't allow so please let me know if further input is desirable on this point.

801: Some logic as the point for line 761

811: I think tiers should include the use of qualitative data in the higher tiers. Tier 4 talks about near real time information, I think this should be reinforced as near real time information supported by a defined and qualitative data set; or words to that effect.

824:

GV.OC: Applicable to all subcategories, the communication path is unidirectional. e.g. Stakeholders needs are determined and understood. For each there should be a feedback loop as part of governance so gaps too are understood. This is in part addressed through risk management but where a need/dependency is captured there should also be confrimation that it will be met or not. This could be captured at the top level or in GV.OC-05 as, "....and any gap between expecations and the current profile are confirmed"

GV.OC-02: I think there is a typo. I think stakeholders needs are determined. While I am sure the stakeholders are determined, I don't think that is the intent.

GV.OC-03: Suggest ethical obligations are added as these often support the mission.

GV.RM-06: Suggest adding, "...and controls.." to narrative. Standardisation of controls creates discipline over procurement of technology to manage cyber risk.

GV.SC-09: Potentially ambiguous wording and doesn't make clear the need for assurance that suppliers are managing their control obligations. Suggest rewording to, "Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and the discharge of their roles and responsibilities is assured through monitoring and reporting that is proportionate to the suppliers criticality for the life of the agreement. "

GV.PO-01: Suggest making the point that policy must be consumable.

ID.AM: Suggest a new subcategory that addresses the proliferation of unmanaged technology commonly associated with Cloud. Suggested wording, "New systems, hardware, software and services provisioned within the profile, without authorisation are detected and managed." This could be placed under detect but that implies hostile activity versus misguided enthusiasm.

ID.RA-05: Suggest rewriting to make a distinction between inherent and residual risk. This is important because without the context of inherent risk, residual risk is often hyperbolic in the way it is communicated. e.g. Security practitioners often conclude that a vulnerability if exploited would signify the end of an organisation through a rare event; rather than the vulnerability changes the residual risk associated with an existing inherent risk. Suggested wording from, "Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.", to, "Suggested wording from, "Threats, vulnerabilities, likelihoods, and impacts are used to determine inherent risk and inform mitigation to achieve a residual risk position that is within appetite."

PR.AA-06: Should this not include logical access.

PR.AT: An observation is that commonly cyber training and awareness is at odds with business processes. e.g. Phishing campaigns teach people to not click on links but half the business processes require someone clicking on a link in an email. Suggest adding a subcategory, "Security Training and awareness is reinforced through consistent business

processes that reflect the behaviours highlighted in said training."

I have two additional comments:

Benchmarking - Using the CSF for benchmarking is popular an sensible if relatively unsuccessful. Providing guidance on how to benchmark your organisation against industry etc and how this can be beneficial would have a positive impact. The method is probably the biggest challenge because in my experience the only institutions with the breadth to perform it are consultancies and inconsistency means it is too subjective. I think this goes beyond what I could put in an email but would be open to further discussion.

The CSF often highlights alignment to mission. I feel that elaborating to make clear that effectively managing security enables productivity; and that the practicalities of human nature need to be considered. e.g. 20 character random passwords mean a lot of written down passwords, leading to incidents and a lot of downtime with people locked out. Again open to further discussion on this.

Thank you for providing the opportunity to contribute.

Regards,

Simon Burson