

November 3, 2023

Transmitted Via E-mail to cyberframework@nist.gov

*National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
cyberframework@nist.gov*

NIST Cybersecurity Framework Program,

Introduction

Thank you for your valuable contribution in creating the NIST CSF v2.0 draft initiative. The introduction of the new 'Governance' function and categories is a significant advancement. In particular, the establishment of 'Governance' as a distinct function can provide clarity regarding the role of board directors and their contributions to the organization's cybersecurity program.

Boards of directors are increasingly expected to have oversight and governance roles in cybersecurity matters, which may surpass their current knowledge and capabilities. NIST's assistance is urgently needed. By making a few small adjustments to the NIST CSF v2.0, the Framework can play a pivotal role in helping board directors become aware of enhancing their oversight and governance responsibilities, ultimately leading to improved cybersecurity program health and outcomes. In line with this objective, the following revisions to CSF 2.0 are proposed for your consideration:

Proposed Revisions

1) Inclusion of board directors in the Framework's "primary audience"

This proposed revision aims to update and align the Framework with the evolving expectations and responsibilities of board directors in cybersecurity governance and oversight.

Rationale: At line 150 of the CSF 2.0 Draft, board directors are classified as being outside of the "primary audience" and are placed in a separate category labeled as "others involved in managing risk". This distinction minimizes the critical role that board directors play in cybersecurity program oversight and governance. Including board directors in the "primary audience" will rightfully acknowledge the substantial impact they make when overseeing and

governing core aspects of cybersecurity programs. These include resource allocation for cybersecurity; defining risk thresholds, tolerances, and appetites; setting cybersecurity policy and strategy; establishing the overall tone for oversight and governance; and sustaining the overall cybersecurity program. This proposal is forward looking in anticipation of emerging board director oversight and governance requirements by the time CSF 2.x and 3.x are released. Understanding their role and its significance is their first step toward fulfilling it. Therefore, it is important and timely that board directors are recognized as part of the intended 'primary audience' in this revision.

Proposed red-line revisions commencing at line 150: The primary audience for the Framework comprises individuals responsible for the development, leadership, operation, and governance of a cybersecurity program. This includes cybersecurity leaders and team members, as well as board directors who hold roles for cybersecurity oversight and governance. The Framework is a valuable resource that can also be used by others involved in risk management, including executives, boards of directors, acquisition professionals, technology professionals, risk managers, legal professionals, human resources specialists, and auditors in the fields of cybersecurity and risk management. It serves to inform and guide their cybersecurity-related decisions.

2) *Revise the CSF somewhere in the text to promote awareness for the concepts of 'cybersecurity program health' and 'cybersecurity program vital health metrics'*

Rationale: Incorporating a 'cybersecurity program health' label within the Framework could provide board directors with a valuable starting point. This would empower them to begin now to use their existing business and risk management expertise to enhance cybersecurity program health in their immediate oversight and governance efforts.

In the context of human healthcare, we rely on vital sign metrics, which typically encompass body temperature, blood pressure, pulse rate, and respiration. Surprisingly, without formal medical training, most of us can make a rough assessment of an adult patient's condition based on key vital signs. For example, a patient with a body temperature of 105°F, blood pressure at 180/90 mm Hg, a pulse rate of 150 bpm, and a respiration rate of 40 would likely be recognized by any of us as experiencing a severe medical emergency, requiring immediate medical attention. It took centuries of research and development for medical science to create and universally adopt current vital signs health metrics – which now interpretable and usable by anyone and a staple for highly trained physicians.

In the field of cybersecurity, and even with annual global expenditures in the hundreds of billions of dollars, we have yet to establish a clear and universally applicable set of 'cybersecurity program vital health metrics'. These core metrics could function as the

cybersecurity counterpart to the essential vital signs in healthcare, enabling board directors without extensive cybersecurity expertise to leverage their existing business and risk management skills effectively when participating in cybersecurity oversight and governance roles.

Cybersecurity program health metrics will differ from the risk and compliance metrics CISOs already report to their board. Program health metrics look horizontally across peer organizations, while CISO risk and performance metrics largely look vertically within their own organization and supply chain. We know when our body temperature is at a concerning level because we know what 'normal' looks like – due to statistical research involving large populations over decades. We don't yet know and don't yet have the protocol or instrumentation to precisely measure what 'normal' looks like for any cybersecurity health metrics – let alone have any consensus on what those metrics should be and how they are measured.

The return on investment (ROI) from a 'cybersecurity program health' approach will be visible and measurable in the form of positive cybersecurity outcomes. This approach comes with a higher likelihood of success and in a much shorter time frame as compared to attempting to transform current and future boards of directors into proficient cybersecurity experts. This 'cybersecurity program health' approach is sustainable. Note: even the best cybersecurity proficient board directors would greatly value 'cybersecurity program vital health metrics' – just as physicians continuously rely on vital sign metrics.

A focus on 'cybersecurity program health' in the Governance function would augment rather than compete with other CSF concepts such as Tiering. For example: achieving Tier progression from 1 to 4 is likely more achievable and sustainable from a healthy cybersecurity program.

An initial first step involves recognizing the substantial value that such metrics can bring to the roles of board directors in overseeing and governing cybersecurity – and the associated positive program outcomes. This recognition is vital for the overall enhancement of a cybersecurity programs' health.

Upon this acknowledgment, the subsequent step entails the introduction of the concepts of 'cybersecurity program health' and 'cybersecurity program vital health metrics' into NIST standards like CSF v2.0. Little effort would be required to introduce these concepts, but much effort over time would be required downstream to evolve and refine the concept. An introduction could be followed by a series of NIST-centered workshops, contributing to the development of a broader initiative, ensuring its progression, and guiding the deliverables.

This collective effort holds the potential to provide more depth and breadth to future revisions of the NIST CSF, including CSF 3.x or 4.x. The ultimate objective is improved cybersecurity program outcomes, brought about by improved cybersecurity program oversight and governance. Imagine the coming day when business and risk management skilled board directors can oversee the identification of early warning indicators from cybersecurity program vital health metrics and take governance actions to enhance their cybersecurity programs health.

Conclusion

The current CSF framework inadvertently minimizes and discourages the valuable contribution of board directors by placing them in a category outside of the 'primary audience.' However, the potential significance of their contribution and the outcomes derived from effective board director oversight and governance warrant their inclusion within the 'primary audience.'

In both realms of human performance and cybersecurity performance, 'health' significantly influences outcomes. Targeting improvements in 'health' can lead to positive results. Whereas, ignoring 'health' can lead to increased risk and poor outcomes. It's noteworthy that the term 'outcome' appears more than 90 times in the CSF 2.0 draft, while the term 'health' is absent. The proposed introduction of the concepts for 'cybersecurity program health' using 'cybersecurity vital health metrics' in CSF 2.0 represents an emerging idea that could significantly enhance future board director governance capabilities, irrespective of their cybersecurity expertise, and promote better cybersecurity program outcomes. The evolution of this innovation has the potential to drive substantial advancements in upcoming NIST standards including CSF revisions in the years to come.

About Board Vista LLC


Board Vista LLC is a startup dedicated to conducting research and development in the field of 'cybersecurity program health calibration', using 'cybersecurity program vital health metrics.' Our future product(s) will focus on providing an innovative, independent year-over-year perspective that empowers boards of directors and other c-suite executives with navigable insights and levers for their cybersecurity program governance. We welcome any further discussions related to these comments or their intended direction.

Thank you for your consideration of these comments.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Mark Chamberlain', with a stylized flourish at the end.

Mark Chamberlain, CISSP
Founder, Board Vista LLC


(website not yet established)