NIST-CSF 2.0.
DVMS Institute LLC Summary and Comments

Submitted By: Rick Lemieux
Co-Founder & Executive Director Programs
DVMS Institute
[redacted]
www.dvmsinstitute.com

One of the major discussion points that surfaced during the NIST CSF Workshop this past February is that the Framework could not be implemented. As noted in our comments below, that wording change (from "implement" to "adapt") still needs to be accomplished. To facilitate this, we recommend changing the labeling for the six "functions" (Govern, Ident, Protect, Detect, Respond, and Recover) to "capabilities." This wording helps support the change from "implement" to "adapt" (see comment about lines 230-231).

We do not believe cybersecurity governance should be separated or siloed from organizational governance. The new GOVERN function should more obviously suggest (if not require) integration with organizational governance. This is particularly important when one of the stated objectives for this revision is to expand its applicability beyond the original requirement to address critical infrastructure. The CSF 1.1 Executive Summary was clearer about the link between cybersecurity and business risk than the current draft for version 2 (see the comment below regarding draft line 445ff).

We recommend that cybersecurity risk be equated to and expressed in business risk terms (again, more in line with the Executive Summary from version 1.1). Also see the comment below re: lines 111 & 115.

Because of the extensive nature of the changes in version 2, we recommend that NIST create a short (30-minute?) video summarizing the enhancements in v2 for the CSF audience.

The DVMS Institute has a lot of experience in taking complex topics and breaking them down into explainer videos that help viewers connect the dots quickly so they can move on to adapting NIST-CSF 2.0. across an enterprise and supply chain. We are happy to help if NIST thinks that would be useful.

Line/Section	Source	Comment
Page 3 – Summary of selected Framework Changes	1. Increase guidance on CSF implementation 2. Emphasize cybersecurity governance	The Framework cannot be implemented; it can be adopted by the organization as part of a governance decision and adapted to fit the need. Suggesting the Framework can be implemented creates marketplace confusion.
Page 3 – Summary of selected Framework Changes	"Emphasize cybersecurity governance"	This wording suggests a silo between organizational governance and that for cybersecurity, allowing cybersecurity to be treated as an add-on versus integrating cybersecurity into what the organizational already does. This idea is also more in keeping with the concept of the CSF as a Framework versus something that can be implemented.

69ff - Executive Summary	Discusses cybersecurity risks. Organizational risk isn't mentioned before line 500	Cybersecurity risk should be equated to organizational risk in this section.
81-83	"These outcomes can be used to focus on and implement strategic decisions…"	It is essential to clarify that strategic decisions should be the primary factor in determining expected outcomes. The current wording doesn't mention the strategic decisions necessary for the organization to make a governance decision regarding adopting the guidance provided in the CSF. It is also essential to note the importance of explicitly adapting the guidance to fit organizational needs.
101	"Thus, organizations' implementations of the Framework, and approaches to managing risk, will vary."	As noted above, the Framework cannot be implemented; it can be adopted (organizational governance decision) and adapted to fit the need. NOTE: several more examples of this usage appear in the document and are not included in this response. NOTE 2: the comment re: page 3. Remove any hint or suggestion that the Framework can (or should be) implemented.
111 & 115	"Align policy, business, and technological approaches to managing cybersecurity risks…"	Explicitly state that cybersecurity risk is an aspect of business risk (as mentioned in line 69ff above). This approach means the organization will prioritize more efficiently as everything now relates back to business outcomes and associated risks. This approach facilitates prioritization of all activities (including those associated with a cybersecurity incident) based on a common rubric, making it easier for the organization to handle.
189 Section 2.1	Functions, Categories, and Subcategories	Changing the word "Functions" to "Capabilities" aligns with the idea of the Framework not being "implementable."
192 GOVERN	"Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy."	This wording is more of an Assurance capability than governance.

		GOVERN should set the stage for assurance based on organizational strategy. Thank you for suggesting that the GOVERN (capability) is cross-cutting. However, business risk should be the driver for prioritization.
230-231	"GOVERN is in the center of the wheel because it informs how an organization will implement the other five Functions."	The comment addresses two points: 1. Cybersecurity governance should be guided by (better integrated into) organizational governance that aligns with organizational strategy. 2. The context expressed for GOVERN (and the other core "functions") aligns with the idea of the Framework as implementable – it is not. It would be better to call these the 6 Core Capabilities, suggesting that the organization must work to develop and constantly improve them. These two ideas align better with the idea of a separate document for implementation examples.
301	3.1 Creating and Using Framework Profiles to Understand, Assess, Prioritize, and Communicate	If the comments above are accepted, with particular attention to lines 230-231, it is easier to understand the intent of this section. Profiles mapped to capabilities serve to minimize the current perceived link that the Framework can (should) be "implementable." It also makes it easier to tie the Framework to the need for the business to establish priorities based on business risk, not cybersecurity risk. This approach also contributes to making the Framework perceived as scalable; organizations make the governance decision to ADOPT the Framework and then ADAPT it to meet organizational needs.
445	3.3 Using Framework Tiers to Characterize Cybersecurity Risk Management Outcomes	Cybersecurity risk should not be siloed, i.e., isolated from business risk.

		Consider this from the Executive Summary of the NIST CSF 1.1: *"Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management."* These sentences at least suggested a direct relationship between cybersecurity and business risks. That idea should be explicitly stated and serve as the basis for adopting and adapting version 2.0 of the Framework. Note: section 4 is a good start and may or not be read and understood without the overall "arc of the Framework story." consistently discussing capabilities, adopting, and adapting the Framework.
Appendix C: Framework core		• Suggest GV.OC-06: Cybersecurity governance is integrated into organizational governance, not considered as a separate entity. • Change the wording of GV.RM-06 to clarify the link between cybersecurity and business risk. • GV.SC-x should include supply chain risk management as an extension of ERM.
GENERAL NOTES		• It's essential to do more than consolidate the governance controls into a new Core (capability). • The presentation of category and subcategory is clearer than previous versions.