[redacted]

CAUTION: This email originated from **outside** your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

FYI

[redacted]

Subject: NIST 2.0 Concept Paper FEEDBACK

Hello

Thank you for the opportunity to comment on the NIST CSF 2.0 Concept Paper. I have used NIST for six or seven years to guide my digital transformation and cybersecurity projects. I have conducted NIST-aligned internal audits.

I now teach project management at the bachelor, master, and PhD levels in Australia. I wrote *Shields Up: Cybersecurity Project Management* (2022) and finishing up *Cybersecurity Training: A Path to Readiness*. Therefore, I have practical and academic perspectives on the NIST CSF 2.0 Concept Paper for your consideration.

I recommend against creating a GOVERN function:

1. Adding a new function complicates the NIST framework.
2. Govern is strategically oriented, while the other five are more tactical. The five-function approach sits well with front-line cybersecurity teams that are tactically oriented.
3. Governance can be managed and optimized through categories and subcategories.
4. Quality management is also a "cross-cutting" best practice that could be elevated to a NIST function for the same reasons as governance.
5. Cybersecurity governance can be improved by following ITIL or COBIT service management frameworks; no need to reinvent the wheel.

Thank you for this opportunity to contribute and for your fine work.

Sincerely,

Greg

[redacted]

https://www.linkedin.com/in/gregoryskulmoski/ [gcc02.safelinks.protection.outlook.com]

Books in Print: *Shields Up: Cybersecurity Project Management*
Forthcoming Book: *Cybersecurity Training: A Path to Readiness*

STAND OUT BOND UNIVERSITY

[redacted]