[redacted]
To: [redacted]
cyberframework
[redacted]
Subject: [redacted]
Date: Feedback to NIST CSF 2.0 Core - Discussion Draft
Sunday, May 21, 2023 5:06:45 PM

Dear NIST CSF team,

Thank you for the opportunity to provide feedback. My feedback for NIST CSF 2.0 (Discussion Draft, sent in your e-mail May 31, 2023) follows-up on the topic mentioned in my e-mail March 3, 2023 (https://www.nist.gov/document/2023-03-03-individual-rainer508redactpdf :: inclusion of the 'three-lines-of-defense' model).

I agree with the current draft that does not explicitly mention the 'three-lines-of-defense model' on the level of subcategory GV.RR-02, because this would be too specific for the respective abstraction granularity. However, I would **recommend including the 'three-lines-of-defense-model' for cybersecurity functions in the 'CSF 2.0 Implementation Examples' column of GV.RR-02**.

To illustrate this input, let me provide a potential formulation: ***"Example …: Cybersecurity roles and responsibilities are established in the first (business/risk management), second (support/risk control), and third (internal audit) line of defense"***

In the 'Informative References' of GV.RR-02, the respective **basic paper of the IIA** (The Institute of Internal Auditors) could be mentioned: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

Background information: in many jurisdictions and most corporate governance sound practices frameworks, the 'three-lines-of-defense model' is suggested for all risk related functions, including cybersecurity functions (cf., e.g., https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance).

In case of questions, please do not hesitate to get in contact. I wish you all the best for the “2.0 finalization” and I am looking forward to including the new version in my teaching as soon as it is published.

Best regards,
Rainer

--

Rainer Kessler LL.M., M B.A., CAS Cybersecurity & Information Risk Management (CSIRM)
Cert. Software Engineer, Cert. EU-GDPR Specialist, Cert. BSI Practitioner, MI/SOF Major ret.
University Lecturer for Cybersecurity, Artificial Intelligence Safety, Emerging Technology Assurance, Operational Risk Management and Operational Resilience
[redacted]