[redacted]
Subject: EXT :FW: One imput re NIST CSF 2.0 concept paper
Date: Thursday, March 9, 2023 1:23:57 PM

FYI

[redacted]
Sent: Friday, March 3, 2023 6:31 AM
To: cyberframework <cyberframework@nist.gov>
Cc: rainer.kessler@fhnw.ch
Subject: One imput re NIST CSF 2.0 concept paper

Dear NIST CSF team,

I suggest to include the **security governance structure according to the three-lines-of-defense model**, as mandated by the Sarbanes-Oxley Act (SOX). Although not all companies have to adhere to SOX, the three-lines-of-defense model (line 1: risk management / line 2: risk control / line 3: internal audit) has become a global "quasi-standard" for good risk (and security) governance. I am very happy to provide additional information, but as an first input, check your thoughts on this topic.

(My relation to NIST CSF: I am a former global CISO of a SOX-relevant corporation; a former technology audit partner of a 'big-4 company'; a former military defense CISO; and since more than a decade I teach cybersecurity at university level - and have included the NIST CSF as backbone in the teaching of a CAS course on cybersecurity.)

Best regards,
Rainer

--
[redacted]