From: Derek Jackson
To: cyberframework
Cc: CRA Team
Subject: Feedback - Revised NIST CSF v2.0
Date: Wednesday, November 1, 2023 12:22:34 PM
Attachments: image326967.png
image052876.png

Hello,
I wanted to let you know of my concerns regarding the revised CSF and believe you are potentially missing an opportunity to make the NIST framework clearer.

My thoughts below:

1. There is no such thing as a Risk Management Strategy or strategies. – There are no inherently different ways of doing risk management, so not really a subject for a strategy discussion. Ultimately risk management is being performed 24*7 the difference being whether its done formally or not by an entity.

   - I would urge you to refer to ISO 31000 2018 on Risk Management which gives the generally accepted way of doing risk management. I can see that GV.RM is intended to address the Corporate approach to risk management, but you incorporated cyber security risk management in some of the sub-categories, and I believe these references to cybersecurity should be removed so that GV.RM is kept where it belongs, at the Corporate level.

   I agree with you the Corporate way of doing risk management needs to be highlighted in the NIST Framework, if only to be able to demonstrate that cyber risk management is either done in the same way, or is performed in a different way to the Corporate method. – For example, the way of evaluating risk might be performed differently at the Corporate level, compared to the Cybersecurity function level.

   Suggest for RM.GV that you come up with sub-categories that describe the processes/procedures that follow ISO 31000 2018:
   - Identifying risk
   - Analyzing risk
   - Risk Evaluation
   - Risk Treatment
   - Monitoring & Review of risk

2. Again the term risk strategies appears under GV.PO and GV.OV as well which should be re-worded to reflect how risk management should be performed. With GV.PO for example the sub-categories should be aimed, at identifying the procedures for identifying risk, analyzing/assessing risk, mitigating risk (i.e. the decision making process when deciding on new controls) and monitoring risk (i.e. how the board get involved in monitoring risks).
3. Sub-categories RR-01 – RR-03 are referring to risk and it looks like RR-01 and RR-02 are pretty much saying the same thing.

I would urge you to look at making each sub-category mutually exclusive, so that each sub-category

is aimed at specific controls to avoid overlap.

Kind Regards,
Derek Jackson

Derek Jackson *Senior Cyber, Risk & Assurance Advisor*

Integrity360
your security in mind

Integrity360 | [redacted]