From: Altaz Valani <avalani@securitycompass.com>
Sent: Tuesday, September 24, 2019 3:49 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Hi,

For the current working draft, I would like to propose some comments for your consideration:

Figure 6:
- The diagram seems to imply a hierarchy. This does not promote cross-functional risk management. In fact, the diagram should indicate bi-directional communication across the layers with the mid layer explicitly being the policy to procedure glue that binds the Executives and Implementation teams.
- Governance of privacy should minimally include privacy, risk, legal, and IT teams. This is not clear in the diagram.
- It largely describes privacy governance. The cybersecurity governance layers should also be included at the mid and bottom layers. A suggestion for the mid layer could be: translate risk based security policies into technical requirements. A suggestion for the bottom layer could be: configure, develop, and test for security.

Table 2 - COMMUNICATE-P:
- In CM.PP-P1, there should be a clear and traceable way of deriving the privacy gaps of the organization based on process governance.

Thanks,
Altaz

Altaz Valani

Director of Research

Security Compass
p: +1 (888) 777-2211 x237

t: @altazvalani