From: [redacted]
To:
Subject: NIST CSF 2.0 Comments
Date: Thursday, November 2, 2023 3:36:24 PM

Hello,

Thank you all for the work you've done to evolve the framework. For the most part, I like the changes.

GV.PO-02 might need a rethink in the approach: The same policies used internally are applied to suppliers.

Most internal policies are a reflection of an organization's business environment, their regulatory requirements, and their risk management strategy. These will likely be very different for a supplier, and each company forcing a policy onto a supplier (who may have hundreds of customers) will create an unholy mess.

Instead, I would suggest that critical controls should be identified and applied instead of policies. It would be much better if you asked organizations to identify which controls are applicable and apply those to their suppliers.

Internal policy objectives should define which controls are applied externally.

Good luck getting this finalized. I cannot wait to see the final product. And thank you for the opportunity to comment!

All the best,

Michael