[redacted]

Hi Cherilyn,

I've received some initial feedback from some our clients who have conducted various CSF engagements with Tevora. So far the 2 items that stood out to me were around Supplier Risk Management:

- A requirement or clarity around ID.SC-04 – Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
    - *Is there a way to define the "routinely" more? I.e. once a year for critical vendors?*

- ID.RA – I think there is mentions of potential business impacts and likelihoods are identified and recorded, but there is no mention of an organization performing a BIA for example.
- Ideally, I think one of the biggest shortfalls of ID.RA is not requiring organizations to have a defined Risk Management Program or a risk assessment to be performed (similar to PCI for example)

Please let me know if you have any questions!

Regards,

Anir Desai
Manager, Enterprise Risk
[redacted]
[redacted]
W tevora.com
TEVORA

[redacted]

[redacted]