Institutional MFA Decision Tree

Reconsider your first answer; observe how others are answering.

Start
Do you have services/systems w/ risk profile requiring MFA today (or soon)?

No → Are you really sure?

No → (to Reconsider box)

Yes → End

Decide how/ where to deploy MFA

Yes →

Do many of those services share a common SSO today?

No → Do some of those services share a user base with significant overlap?

Yes → Are the services and their access method easily integrated with an SSO you use today?

Yes → Integrate w/SSO

Yes → Add MFA support to that common SSO system.

Are there still services needing MFA not covered by that approach?

No → End

Yes → (to Decide how/where)

Do some of those services share a user base with significant overlap?

No → Is there an effective way to integrate MFA with each service/ access method individually?

No → Consider a network/VPN/password portal approach: MFA required to VPN or portal, services only available thru that.

Yes → Use MFA solution that integrates with each of those services/apps.

Are the services and their access method easily integrated with an SSO you use today?

No → Consider a network/VPN/password portal approach...

Posit: Security effectiveness of passwords alone is diminishing, and we've exhausted usable approaches to "shoring up" password security

If the/a primary service access method is "non-web" (e.g. ssh, some mobile apps) and/or "fat client", solution has to account for that.

Who has the budget? That may also impact the decisions/choices/ integration options

End → Done for now