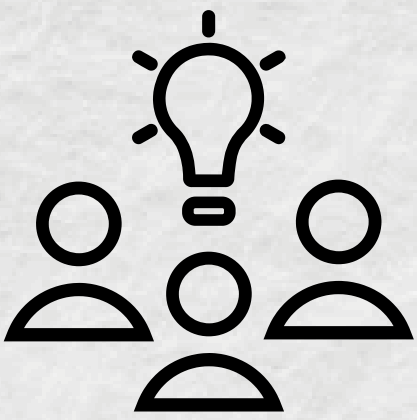
Where to start

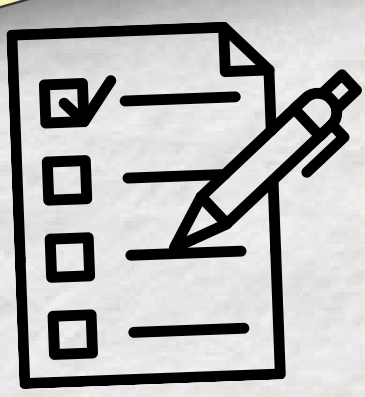
The Top Five "Dos" and "Dont's" When It Comes To Running an Effective Security Risk Assessment

01

Do: Assess risk holistically through the inclusion of the right cross-departmental participants and leadership members.

Don't: Limit your focus to the IT team exclusively.





02

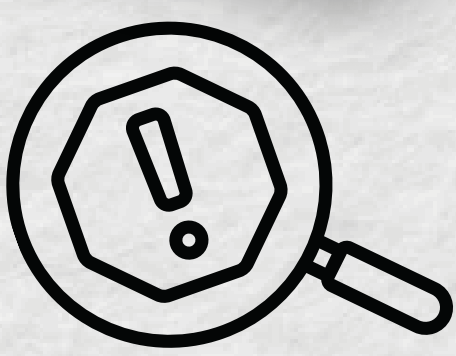
Do: Pick an established and defensible framework to assess your organizational risk against.

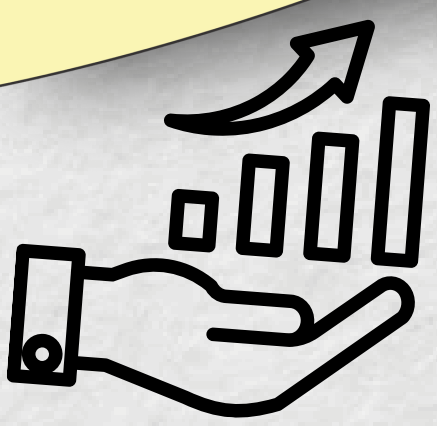
Don't: "Just wing it."

03

Do: Conduct risk assessments regularly and at the time of any material change of operations or systems.

Don't: Go long periods without intentionally considering the risk landscape within which your organization lives.





04

Do: Make meaningful, measurable progress on identified risks over time.

Don't: Use a risk assessment as a "check-the-box" activity without taking action on findings.

05

Do: Assess risk with a critical eye with the help of outside counsel and, where appropriate, experienced technical experts.

Don't: Think that an "all clear" assessment actually means you have no risk. It just means you need to look harder!

Learn more at:
hselaw.com/cyber-where-to-start-series

Attorney Advertising. Prior results do not guarantee a similar outcome.

HSE