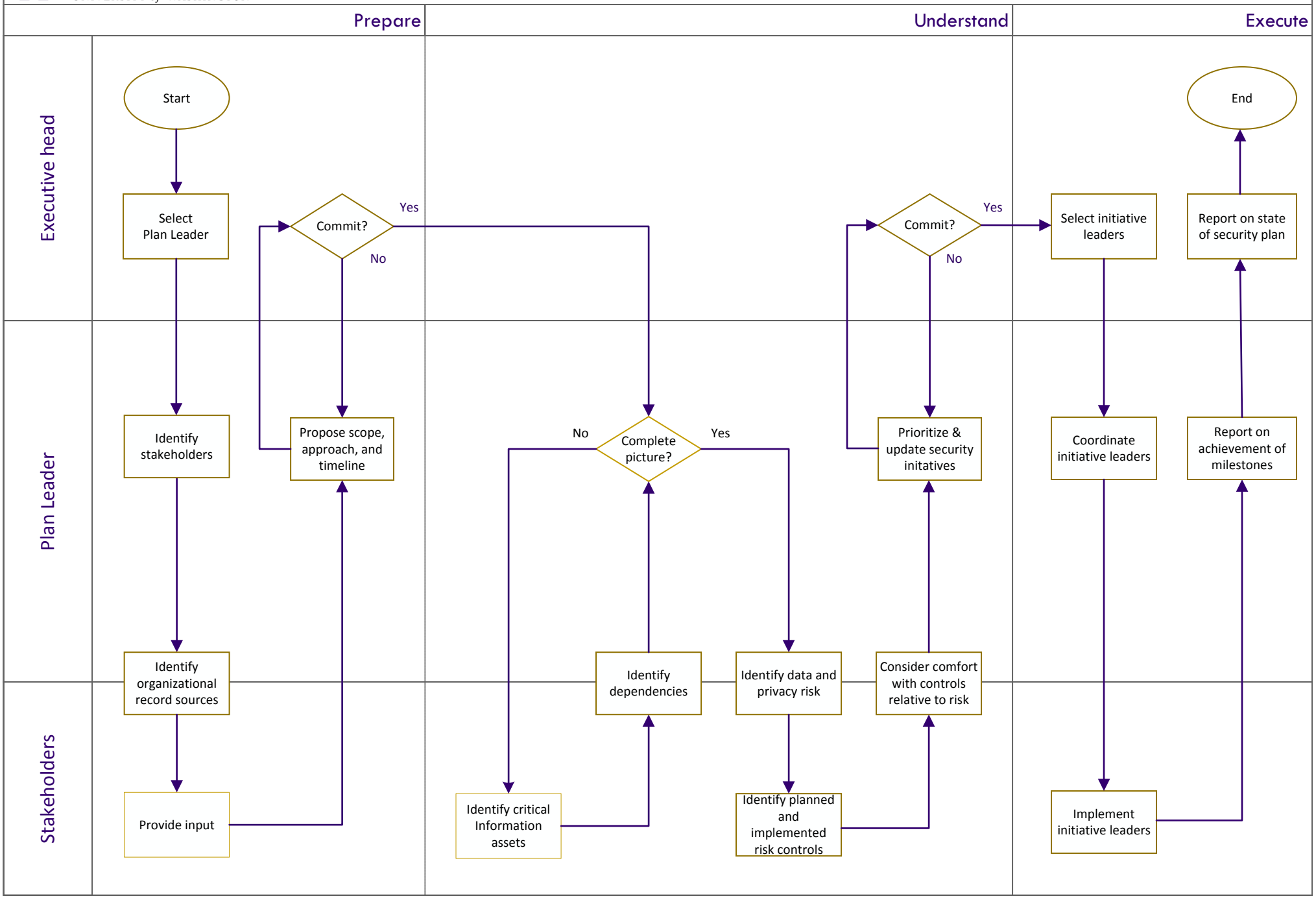
OFFICE OF THE CISO
UNIVERSITY of WASHINGTON

INFORMATION SECURITY PLAN WORKFLOW



INFORMATION SECURITY PLAN WORKFLOW

Notes

Roles

Executive Head (of University Organization) formally responsible for producing and maintaining a plan that demonstrates the exercise of *due care* in managing the risks associated with the *critical information assets* of the organization.

Plan Leader is delegated (or already has) the necessary authority to marshal resources and stakeholders with the necessary information for security planning.

Stakeholders include internal personnel, service managers, vendor contacts, and clients with a significant role related to a critical information asset.

Stages

Prepare Before diving into the planning effort, it is necessary make general decisions about the scope (depth & breadth) of the planning effort, who is expected to be involved in the effort, and who is leading the effort. It is recommended to have some sort of goal in mind and to estimate how much of the effort involves searching for records, versus reviewing records whose locations are known.

Understand The planning process is largely about examining how the organization depends on critical information assets, the interdependencies between critical information assets, and the levels of concern around how those assets and dependencies are currently secured. The set of initiatives that are "planned" for future endeavors should reflect priorities realized from that examination process.

Execute Execution of the planned initiatives *follows* the actual committed plan. However, part of the continuing duty to demonstrate due care is to maintain a record of the state of the initiatives being implemented

Important

One size does *not* fit all
The scope, substance, and approach to security planning is greatly influenced by the mission and nature of the organization making the plan.

Reference centralized services
Rather than explain how centralized services work, describe how the service is used within the organization.

Reference outsourcing
Identify key vendors, know what critical assets rely on the vendor, and how both the vendor's service and the *relationship* with the vendor is managed.

Map asset dependencies
An asset may be critical because of its own value or because other assets depend on it.

Use existing sources
Leverage documentation, information resources, and systems that already exist.

Together We Will

Office of the CISO offers consulting services. Contact **ciso@uw.edu** We are here to help!

OFFICE OF THE CISO
UNIVERSITY of WASHINGTON

Published August 15, 2016