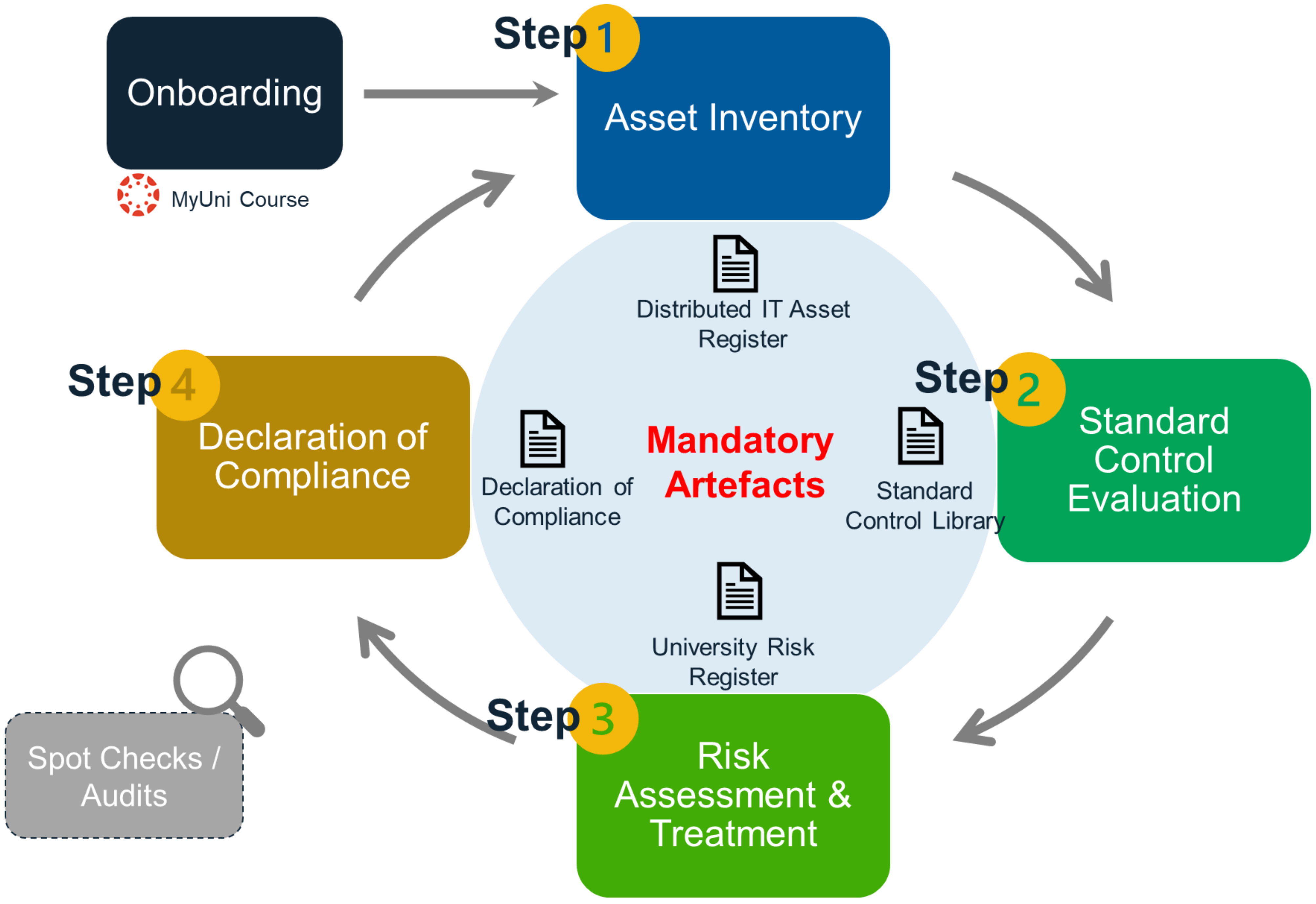
Distributed IT Governance Process



Step 1. Create Distributed IT Asset Inventory

Business areas must develop or update a Distributed IT Asset Register with associated attributes and metadata that help to characterise each asset.

Step 2. Assess against Standard Control Library

The SCL has a minimal set of “baseline” security controls that a typical Distributed IT owner must aim to implement to reduce security risks. The IT Custodian must go through each of the SCL items and specify whether the control has been fully or partially implemented (or not applicable).

Step 3. Assess Risk and create Treatment plans

Business Owners must assess the risk of their Distributed IT and where the risks are unacceptable, develop treatment plans to mitigate risk.

Step 4. Declare Compliance with Framework

Area Managers must complete an annual Compliance Declaration, with information from their Business Owners, ensuring that their area has complied with the Framework.

THE UNIVERSITY of ADELAIDE