Begin data identification process (DLP + manual inventory & risk assessment)

Sensitive or Restricted data identified through inventory

Data owner, data type, data controls identified (see Data Classification Standard)

3. Determine mitigation strategy with data owner

Provide data owner with local policy templates, standards, and any other requirements

Policies and controls are implemented

End DDRA process

Remove the data

Move data to OIT Secure Network

Keep data in place with mitigating security controls (encryption, multifactor authn, ITSO standards)

Document data or system in repository

Annual Data Risk Assessment