FY17 IT Risk Assessment Quick Reference Sheet

Texas A&M IT-RMP: Facilitates the university IT risk management activities on behalf of the CISO to meet state requirements.

Division Risk Assessment Coordinator (D-RAC): a liaison between his/her unit and Texas A&M IT concerning the annual IT risk assessment process. Each college and division may have up to two D-RACs.

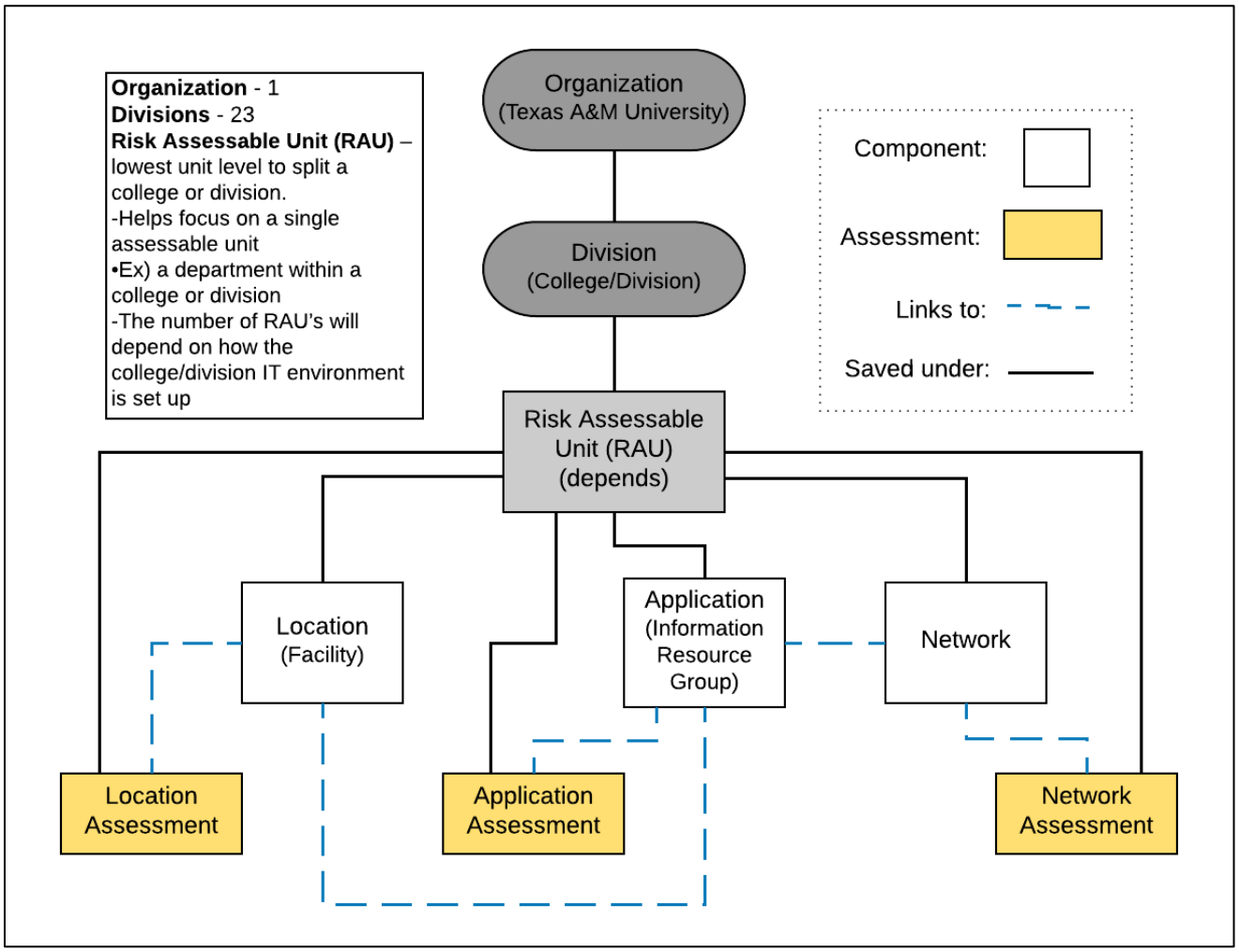
Assessor: The Assessor is a staff or faculty member who will answer the assessment questions and then be responsible for responding to Findings generated from the assessment results.

Staff and faculty will be split into two groups (i.e. IT professionals and non-IT professionals) when it comes to IT risk assessments. Staff and faculty are split because non-IT professionals are not allowed to do an IT risk assessment unless they have been formally approved by their respective dean or VP.

> **IT professional** - A staff or faculty member whose primary duties are to manage information systems or directly support, in the technical sense, personnel who manage information resources (e.g. Database Administrator, Systems Analyst, Web Developer, etc.)
>
> **Non-IT professional** - A staff or faculty member whose primary duties do not include directly supporting an information resource (e.g. research scientist, lecturer, professor, etc.)

Reviewer: will be another person who reviews an assessment to help ensure its accuracy. The Reviewer role is generally a secondary role for a D-RAC and/or Assessor. An individual cannot hold the Assessor and Reviewer roles for the same assessment.

SPECTRIM Hierarchy:



Component and Assessment Information

1. Application – a group of information resources that have a similar security profile / like configuration settings.

Application Assessment –

Required: all Applications

2. Location – where information resources are located.

Location Assessment –

Required: Data center that a unit maintains

- Data center definition – has redundant power feeds, independently controlled environment, & fire suppression system.

Optional: a building and/or room with information resources

3. Network – a physical network separate from the College Station campus network run by Texas A&M IT

Network Assessment –

Required: if a unit manages a physical network separate from the College Station campus network run by Texas A&M IT

Not required if a unit:

- Only utilizes the College Station campus network (*TAMU Network-711-*) for public networking
- Manages address space (e.g. Infoblox, NIM, DHCP) on the College Station campus network
- Runs patch cables between information resources and College Station campus networking equipment
- Operates an independent physical or virtual (e.g. software networking, VLANs, etc.) network for private communication between information resources

3-Phased approach to complete all risk assessments

Phase 1: Inventory Management/Resource Identification

- Identify all information resources in respective unit (college/division/department)
- Ensure compliance with Texas Administrative Code 202 (TAC 202) requirements

Phase 2: Grouping and Assessment

- Group information resources into logical groups that have like security profiles
- Answer assessment questions (taken from the web based tool) about the recently created groups
- Respond to Findings generated by the answers to the assessment questions

Phase 3: Data Entry and Reporting

- Enter data from previous phases into the web based tool
- Generate reports

FY17 Due date (meaning Dean/VP required signature): April 28, 2017