Technology Risk Assessment Process

Initiate

Department Initiates Process and Submit Documentation

IT Risk Assessment begins and TX RAMP certification requested

Results

Assessment results provided to Department and other Units

Assessment

TX RAMP Certification Results and IT Compliance Risk Results finalized

Approval

Leadership Review
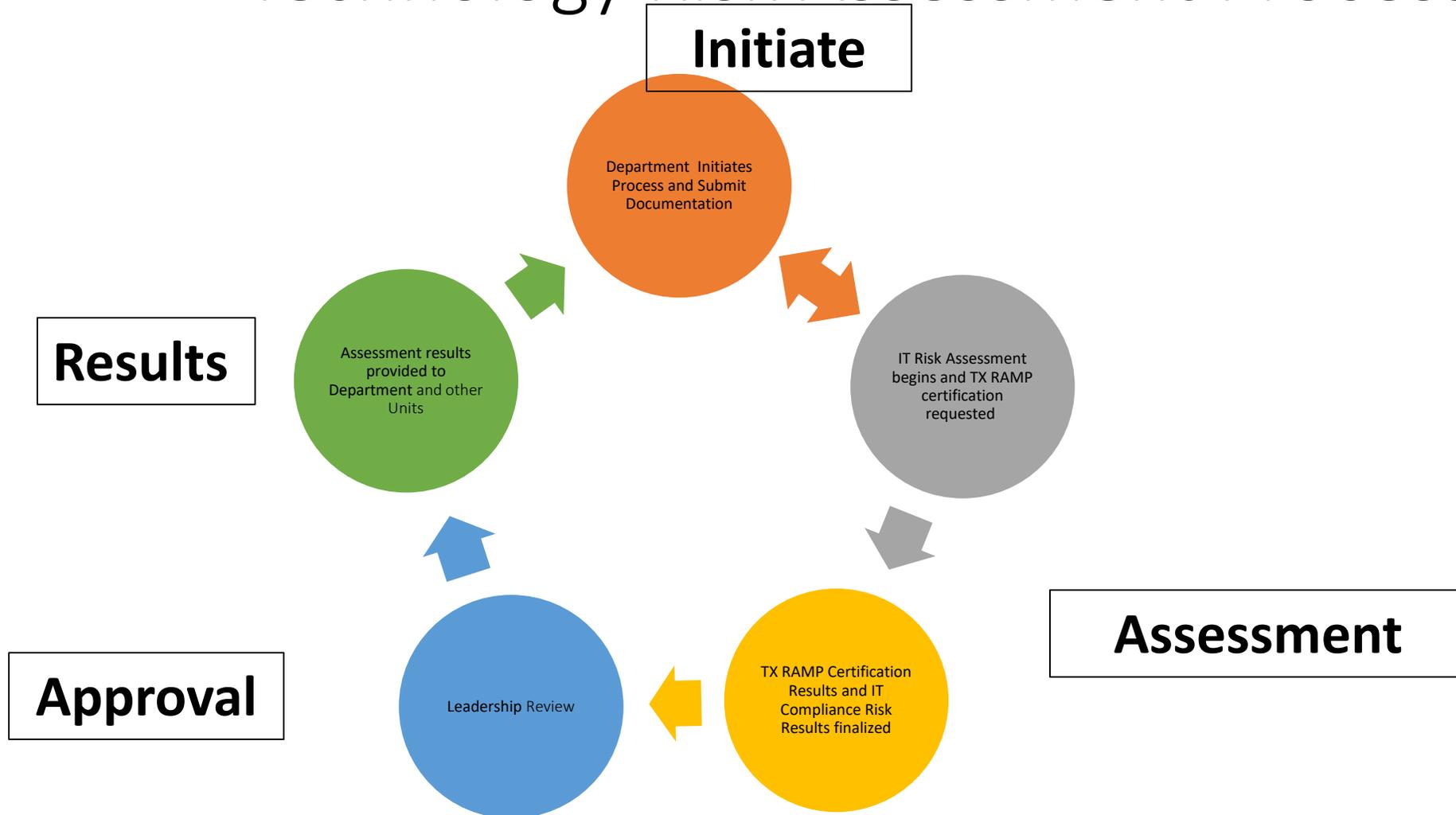
Initiate Process

1. (Department) Identifies technology.

2. (Department) Works with their <u>local IT</u> support team to obtain the following:

    - Product information
    - Vendor contact information
    - VPAT (voluntary product accessibility template)
    - Ask vendors if they are TX-RAMP (Texas Risk Authorization Management Program) certified. If certified, ask vendor to provide evidence of certification.
    - (Department) Submit items listed in # 2 (above) in Service Now (<u>Technology Acquisition Questionnaire-TAQ)</u>

IT Risk Assessment and TX-RAMP Certification Requests

- (IT Compliance) Reviews TAQ for completeness and level assignment based on data usage and impact.

- (IT Compliance) Assigns TX-RAMP certification level for cloud computing products and services. Shares level, assessment templates, and vendor instructions with the Department (in ServiceNow).

- (Department) Notifies the vendor to seek TX-RAMP certification at the level identified by IT Compliance.

- (Department and IT support) Completes third-party assessment of other data protection and system security requirements and submits supporting documentation to IT Compliance.

TX-RAMP Certification and IT Compliance Risk Assessment Requirements

1. **TX-RAMP Certification Submission**
   - (Vendor) Submits TX-RAMP certification request to Texas Department of Information Resources (DIR) at https://survey.alchemer.com/s3/6510630/TX-RAMP-Vendor-Contact
     - Vendor can find more information at TX-RAMP Website and TX-RAMP Presentation for Vendors.
   - (DIR) Conducts assessment of compliance with NIST 800-53 makes assessment results available.
   - (IT Compliance) Confirms TX-RAMP certification with DIR.

2. **IT Compliance Risk Assessment**
   - (IT Compliance and Information Security) Review third-party assessment and supporting documentation. Determines if product or service meets other data protection and system security laws, frameworks, and standards.

Leadership Review

- (Campus Leadership) approves the product.

Assessment Results

- (IT Compliance) Send results of assessment review process to Department contact, IT Support, Procurement and Contracts (as applicable).

- (Department) Sends assessment results to Procurement and Contracts (as applicable).

Cloud Computing Services Not Subject to TX-RAMP

- Exception requests must be submitted to IT Compliance for review to determine if a product or service is out-of-scope of TX-RAMP.
- Below are the characteristics of out-of-scope cloud computing services identified by DIR:
  - Consumption-focused cloud computing services such as advisory services, market research, or other resources that are used to gather non-confidential research or advisory information.
  - Graphic design or illustration products.
  - Geographic Information Systems or mapping products that are not used for confidential purposes or tied to individual identities.
  - Email or notification distribution services that do not create, process, or store confidential information.

Cloud Computing Services Not Subject to TX-RAMP continued

- Social media platforms and services.

- Survey and scheduling cloud computing services that do not create, process, or store confidential information.

- Cloud computing services used to deliver training that does not create, process, or store confidential information.

- Cloud computing services used to transmit copies of non-confidential data as required by external governing bodies for purposes of accreditation and compliance; and

Cloud Computing Services Not Subject to TX-RAMP continued

- Low Impact Software-as-a-Service cloud computing services as defined by the following criteria:
  - The product meets the definition of a Software as a Service (SaaS), as defined by NIST SP 800-145, The NIST Definition of Cloud Computing.
  - The cloud computing service does not contain personally identifiable information (PII), except as needed to provide a login capability (username, password and email address), or create, process, or store confidential state-controlled data.
  - The cloud computing service is a low impact information resource as defined by 1 TAC §202.1; and
  - The cloud computing service operates within a TX-RAMP certified Platform as a Service (PaaS) or Infrastructure as a Service (IaaS).

Cloud Computing Services Not Subject to TX-RAMP continued

- In addition, the following cloud computing projects or services have been identified as out-of-scope of TX-RAMP <u>if the contract is not a new agreement or is not a renewal:</u>
  - Amendments to existing contracts
  - Adding additional licenses to an existing contract.

References

- More information about TX-RAMP can be found in DIR's Texas Risk and Authorization Management Program Manual found on their [TX-RAMP website](#).

- Contact [IT Compliance](#) (ITCompliance@untsystem.edu) if you have any questions about this process.