What is FedRAMP?

- Federal Risk and Authorization Management Program
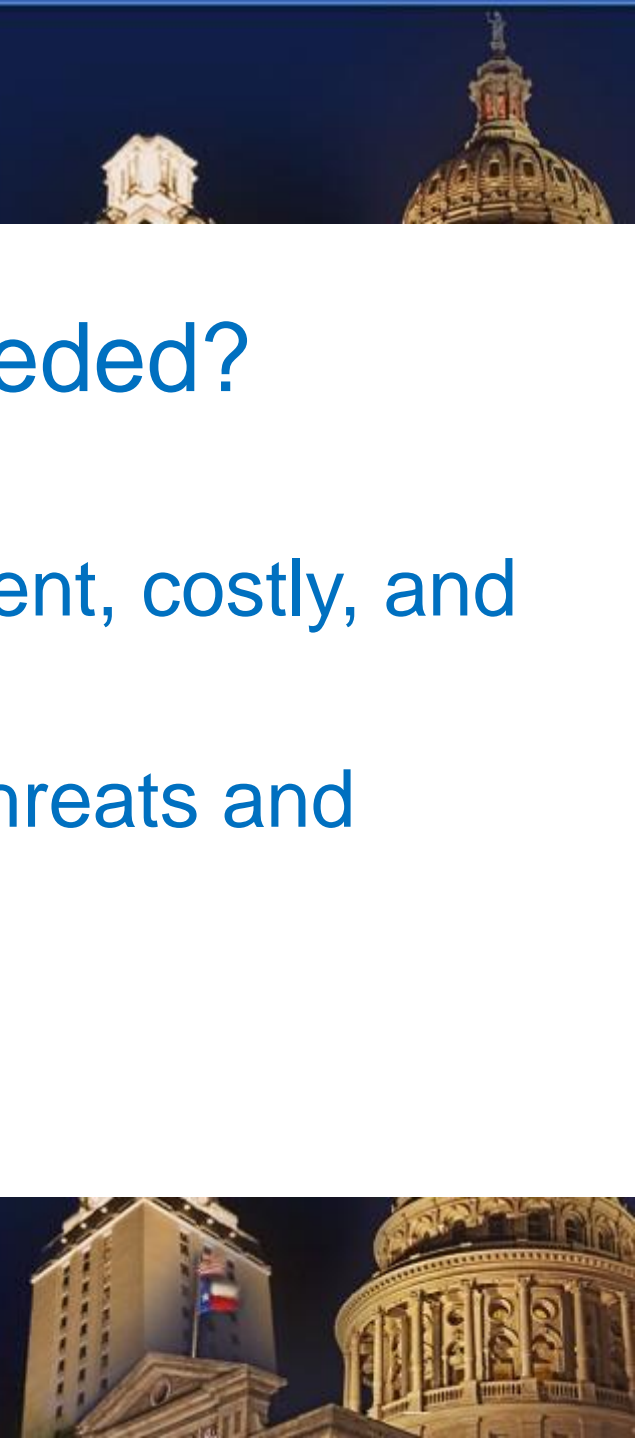- Government-wide program that provides a standardized approach to authorization of cloud services.

Why is FedRAMP needed?

- Eliminate duplicative, inconsistent, costly, and inefficient processes.
- Focus on real-time persistent threats and mitigation actions.

Goals of FedRAMP

- Reuse of assessments and authorizations
- Standardized security of cloud solutions
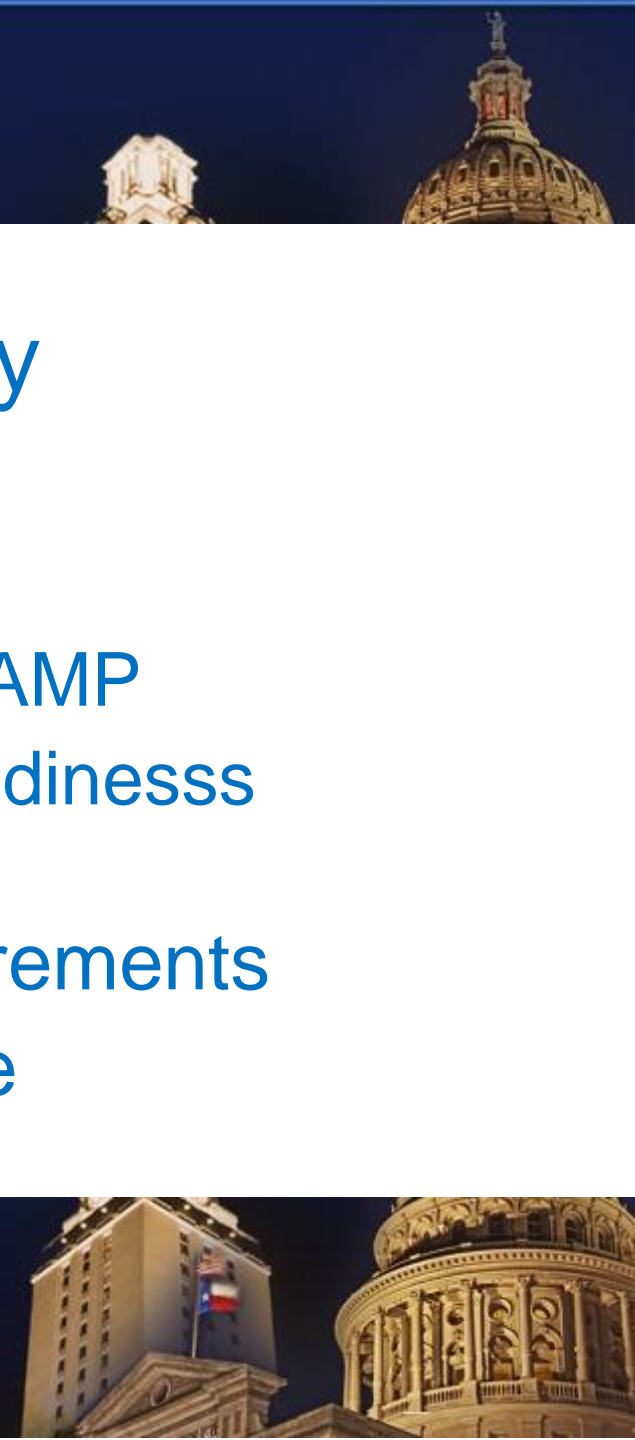- Consistent security authorizations

Before You Apply

- Review guides
  - Guide to Understanding FedRAMP
  - Quick Guide to FedRAMP Readinesss Process
- Review baseline security requirements
- Assess current security posture

FedRAMP Authorization Process

- Directly apply or work with a sponsoring agency
- Implement the baseline security controls
- Submit system documents
- Hire an accredited 3PAO to perform assessment
- Create and submit an authorization package
- Provide continuous monitoring reports and updates

FedRAMP Authorization Process

- Website
  - http://cloud.cio.gov/fedramp
- Online initiation request
- Key Documents

Overview of Assessment

- Documentation
- Physical Security
- Logical Security
- Processes

Overview of Assessment

- Documentation
  - SSP
  - Contingency plan
  - Incident Response Plan
  - Configuration Management Plan

Overview of Assessment

- Physical Security
  - Locks/alarms
  - Cooling
  - Fire suppression
  - Power/backups
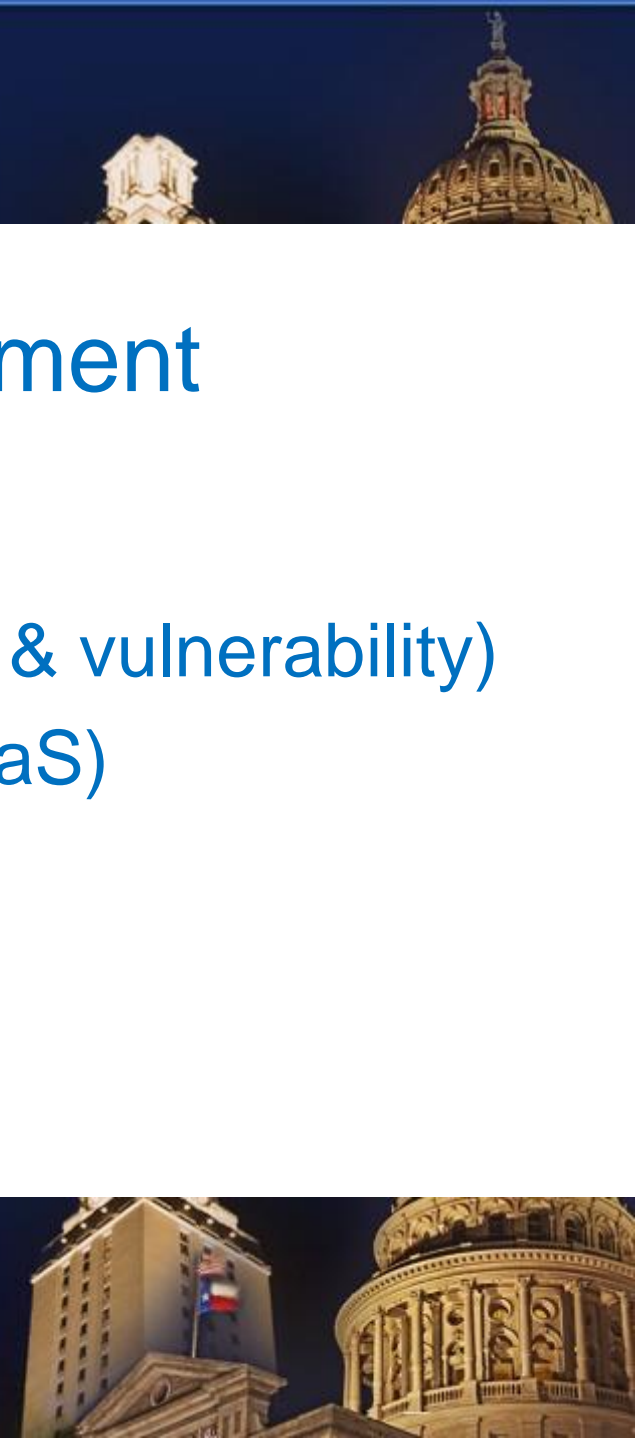 - Temperature/humidity controls/alarms

Overview of Assessment

- Logical Security
    - Platform scanning(compliance & vulnerability)
    - Application code scanning (SaaS)
    - Penetration testing
    - Configuration

Overview of Assessment

- Processes
  - User Access
  - Scanning/Auditing
  - Physical
  - Exercises - CPEx/IRPEx
  - Awareness/Training

Providers

- Third Party Assessment Organizations (3PAOs)
- Cloud Service Providers (CSPs)