

# Federal Risk and Authorization Management Program (FedRAMP)

## FedRAMP Security Assessment Process

Matthew Goodrich

FedRAMP Program Manager

GSA Office of Citizen Services and Innovative Technologies





# FedRAMP and the Security Assessment and Authorization Process

## FedRAMP

- Maintains Security Baseline including Controls & Continuous Monitoring Requirements
- Maintains Assessment Criteria
- Maintains Active Inventory of Approved Systems

### Consistency and Quality

#### 1 Assessment

##### **Independent Assessment**

- Before granting a provisional authorization, Cloud Service Provider systems must be assessed by an accredited 3PAO Third Party Assessment Organization

#### **Independent Assessments**

1. CSPs must retain an independent assessor from FedRAMP accredited list of 3PAOs

### Trustworthy & Re-useable

#### 2 Provisional Authorization

##### **Grant Provisional Authorization**

- Joint Authorization Board reviews assessment packages and grants provisional authorizations
- Agencies issue ATOs using a risk-based framework

#### **Authorizations:**

1. Provisional ATO - Joint Authorization Board
2. ATO – Individual Agencies

### Near Real-Time Assurance

#### 3 Ongoing A&A (Continuous Monitoring)

##### **Continuous Review of Risk**

- Oversight of the Cloud Service Provider's ongoing assessment and authorization activities with a focus on automation and near real time data feeds.

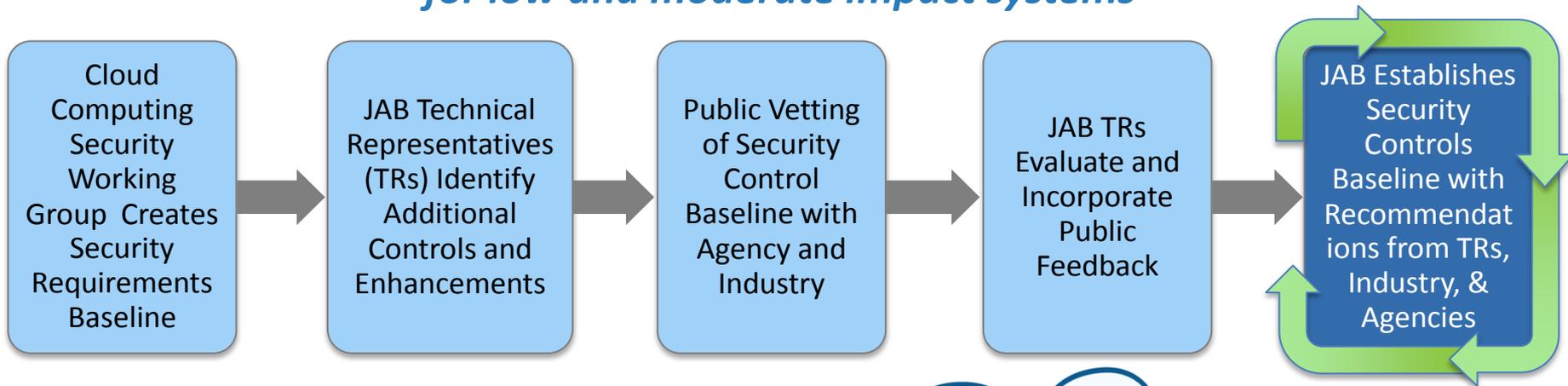
#### **Ongoing A&A Activities Will Be Coordinated Through:**

1. DHS – CyberScope Data Feeds
2. DHS – US CERT Incident Response and Threat Notifications
3. FedRAMP PMO – POA&Ms

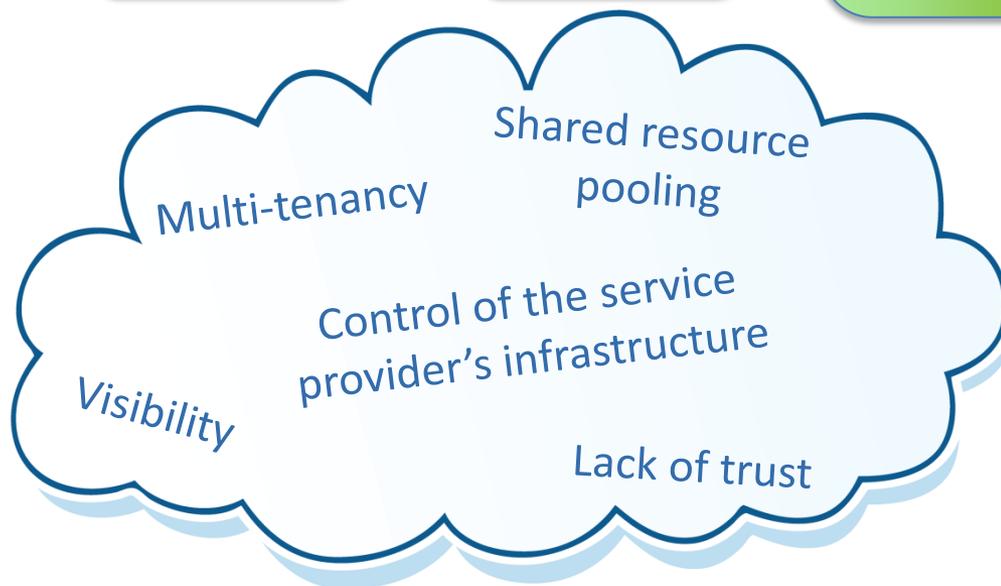


# Identifying Baseline FedRAMP Security Controls

*FedRAMP baseline security controls are based on NIST SP 800-53 R3 controls for low and moderate impact systems*

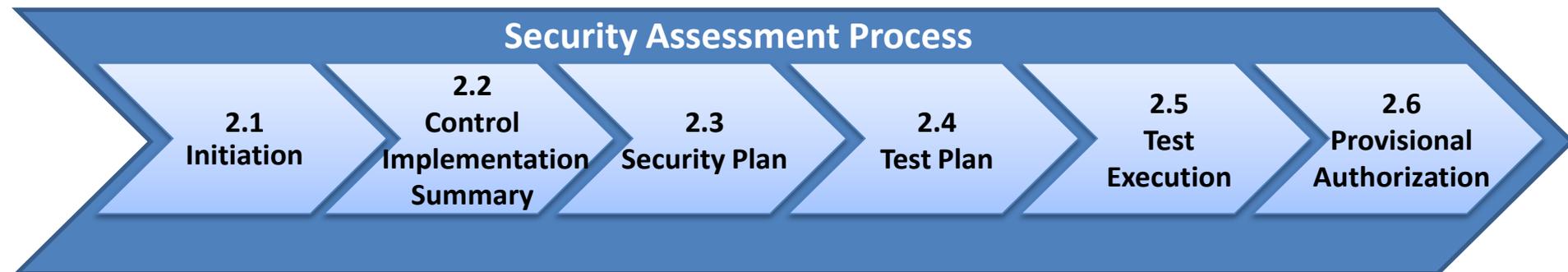


**Additional controls and enhancements address the unique elements of cloud computing**





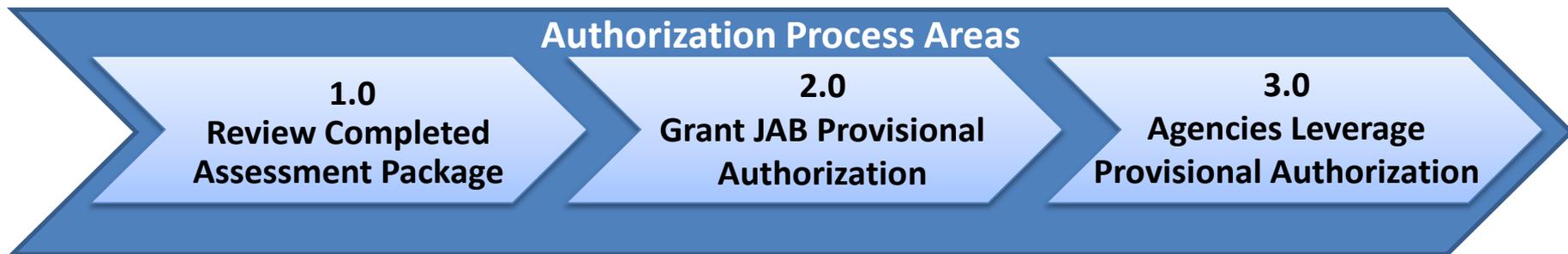
# FedRAMP Security Assessment Process



- All templates, guidance, requirements will be publicly available
- Aligns with NIST SP 800-37 Risk Management Framework
- This is the same process CSPs would follow with individual agencies



# FedRAMP Authorization Process Areas



- Authorizations or Authority to Operate (ATOs) required by FISMA
- JAB Provisional Authorization = “seal of approval”
- Agencies will leverage JAB provisional authorization to make risk-based decision to use a CSP
- ‘Do once, use many times’



# FedRAMP Ongoing Assessment & Authorization (Continuous Monitoring)



- Maintain ongoing awareness of vulnerabilities and threats to support risk management decisions.
- Maintain operational visibility of CSP information systems to maintain acceptable risk
- Focus on automation and real-time data feeds
- Work with DHS and NIST to evolve more standards for automation and real-time data feeds