



FedRAMP 3PAO Accreditation Requirements

July 28, 2015

Presented by: Laura Taylor

www.fedramp.gov



Agenda



Background



How we got to
where we are



Process Maturity of 3PAO Program

A2LA's Role



Evolution Process



Program
Changes



Level Set: Overview and Background

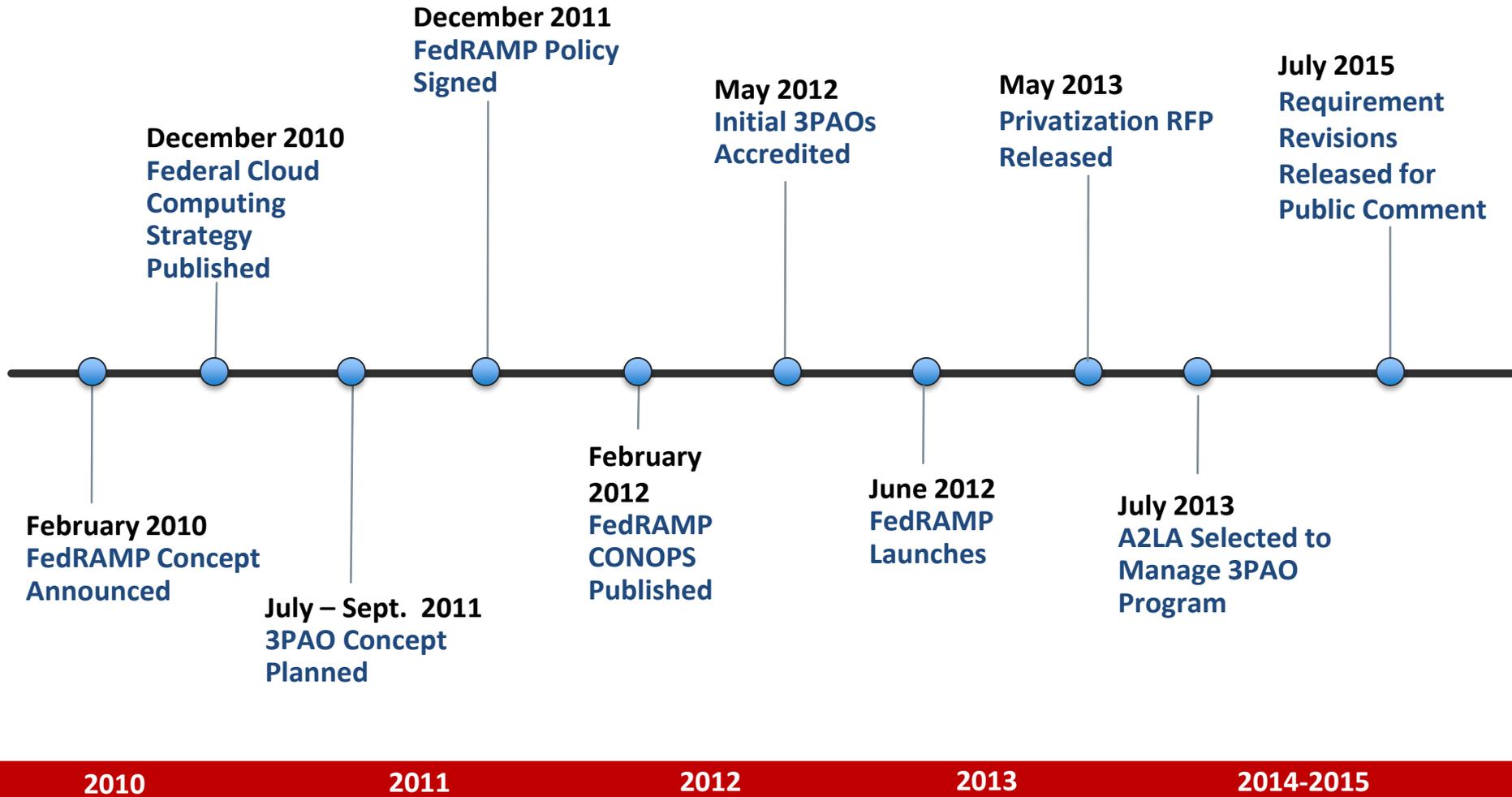


NIST

Conformity assessment team from the National Institute of Standards and Technology (NIST) played a critical role in developing the 3PAO program.



Timeline of 3PAO Program





Level Set: Overview and Background on 3PAO Program

Original Requirements

ISO/IEC 17020:2012
Conformance





Background: A2LA's Management Role



- Identify conflicts of interest with prior consulting services
- Provide application materials to new candidates
- Review new 3PAO applications and assemble evaluation artifacts
- Determine if applicant meets accreditation requirements
 - Onsite inspection and interview
 - Review quality management system
 - Review organizational quality manual
 - Confer with FedRAMP PMO
 - Evaluate knowledge of FISMA and FedRAMP
- Recertify 3PAOs every two years



Revision Focus Areas

Quality Control

How can we enable continuous improvement in quality?



Resource Requirements

Can one person do it all?



Protection of Sensitive Information

How can we better protect our systems?



Principles

What is important to us?



Training

What do 3PAOs need to be successful?

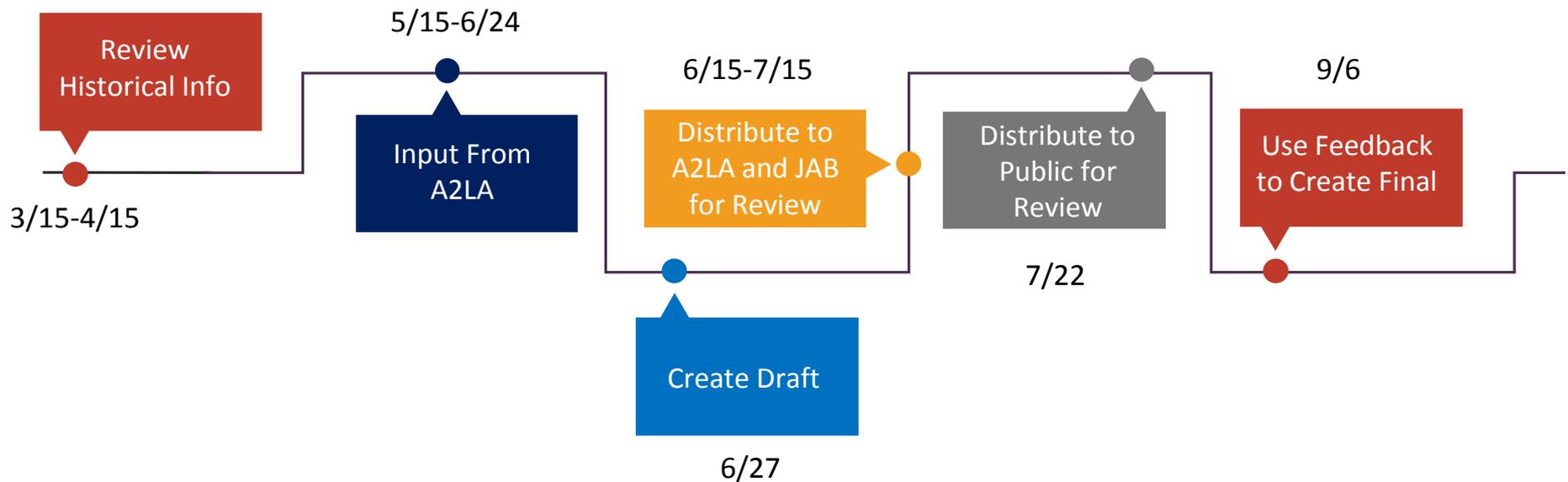


Assessment Report Requirements

How can we enable better decisions from reports?

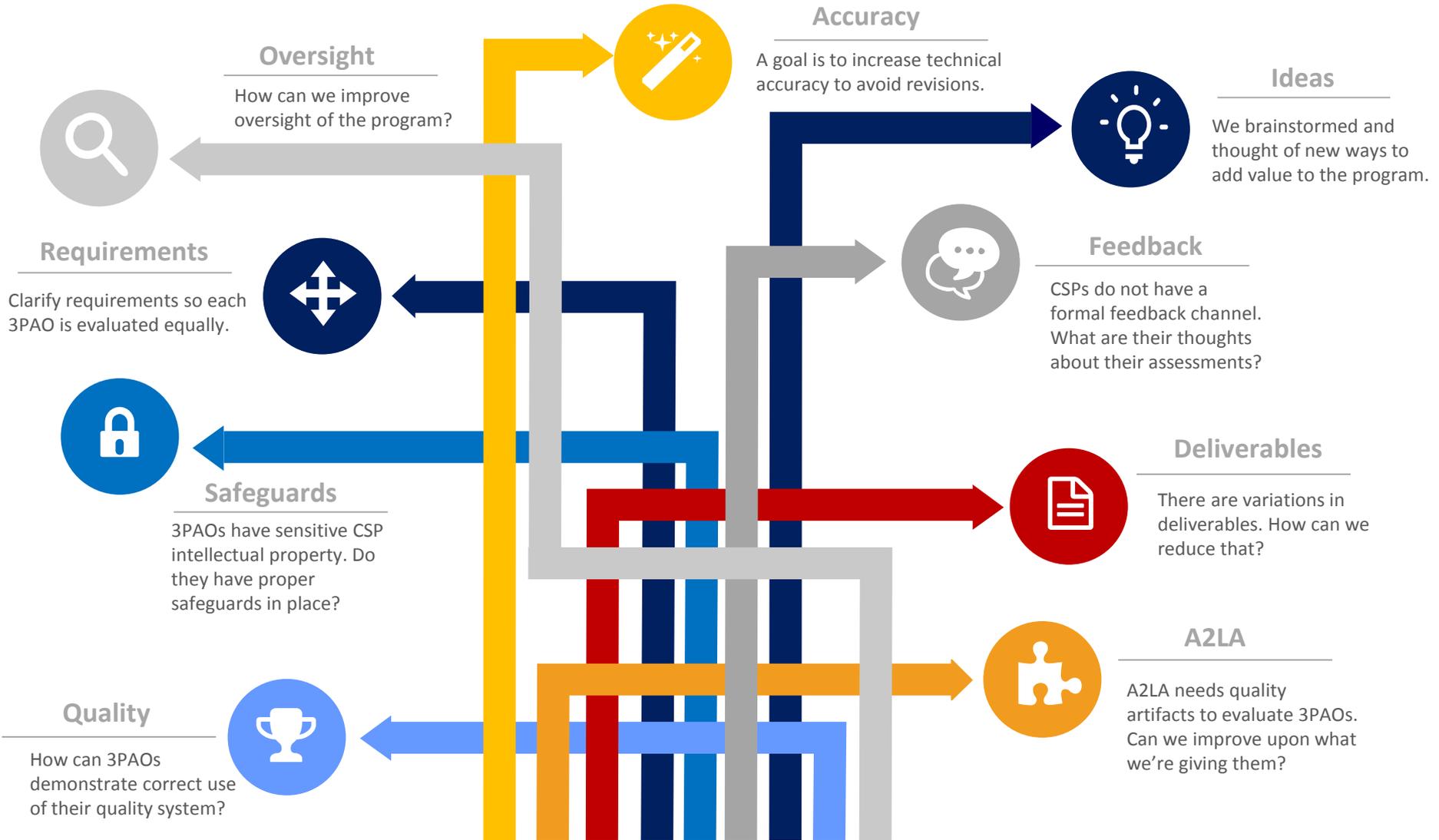


Process for Revision





Three Years of Observations





3PAO Resource Requirements

New!

1

Three People

...are required for each assessment. One of the three must be a designated penetration tester.

2

A Senior Assessor

...must be one of the three people that are part of the assessment team.

3

Position Descriptions

...must exist for each person on the team. It should include required skills and experience.

4

Subcontractors

...must be trained on how to use the 3PAO quality management system.

5

Software and Tools

...belonging to subcontractors must fall under the purview of 3PAO policies and procedures.



Protection of Sensitive Information

New!

3PAOs
must
safeguard
CSP info

Safeguard

What safeguards are
in place?

Implement
policies &
procedures

Implement

Have your policies and
procedures been put
into practice?

Demonstrate
compliance
with policies
& procedures

Demonstrate

How will you
demonstrate that your
assessors comply with
policies & procedures?

CSP must
approve of
release of
their info

Approval

It's not necessary to
give CSP information
to A2LA.



Training

- **New!** Must attend/register for all mandatory training and program update sessions provided by FedRAMP within 30 days of the training being announced by FedRAMP
- **New!** 3PAO POC must provide training certificates to FedRAMP within 30 days of date of training
- **New!** 3PAOs must develop their own internal training program for their employees working on FedRAMP assessments





Quality Control

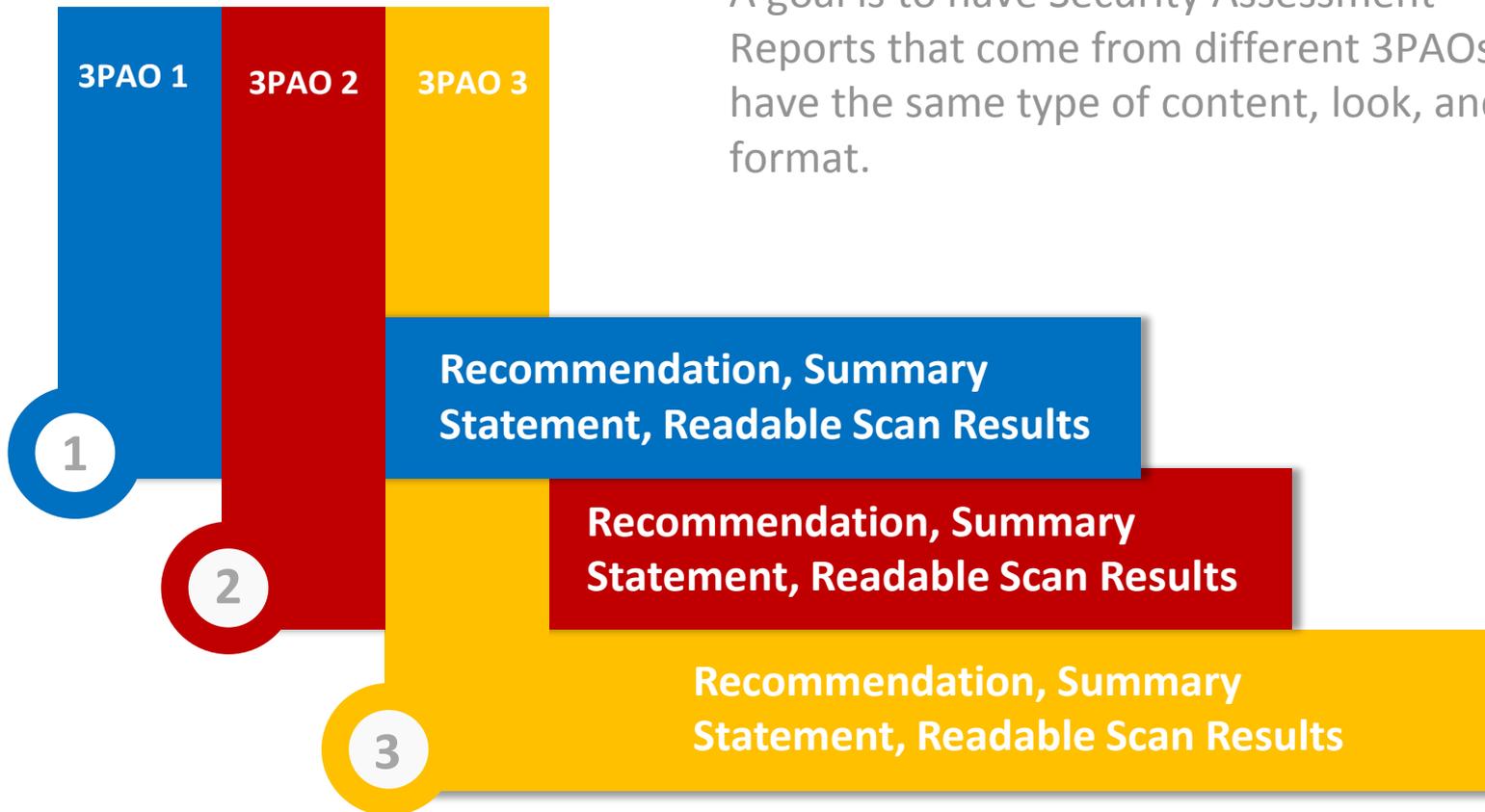
- Must demonstrate control of documents and information
- Must demonstrate quality control of assessments
- **New!** Accountability and sign off for each section of the SAR
- **New!** After Action Report required for each assessment
- **New!** 3PAO must ask CSP to evaluate their work
- **New!** All documents must be QAed before delivery to CSP in conformance with the 3PAO quality review process





Assessment Report Requirements

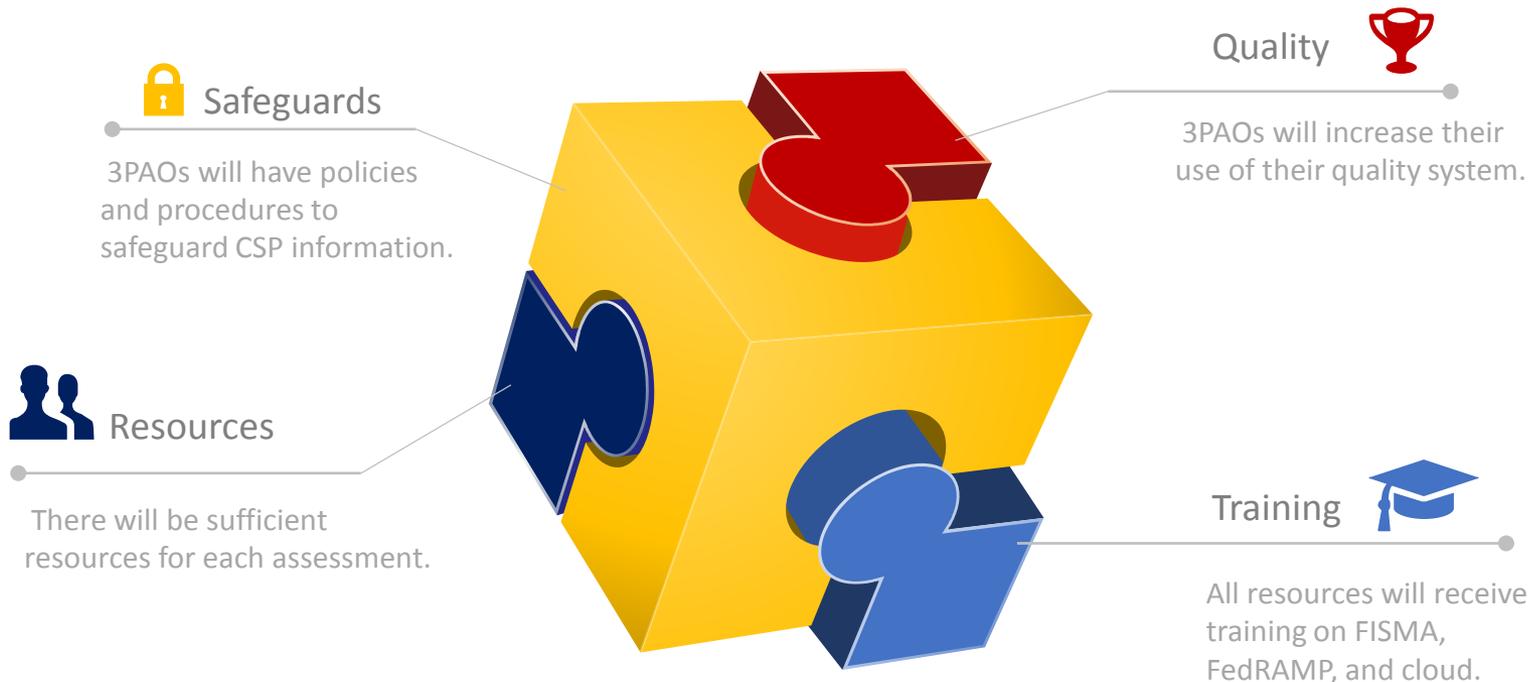
A goal is to have Security Assessment Reports that come from different 3PAOs all have the same type of content, look, and format.





Summary

Enhanced for Continuing Success

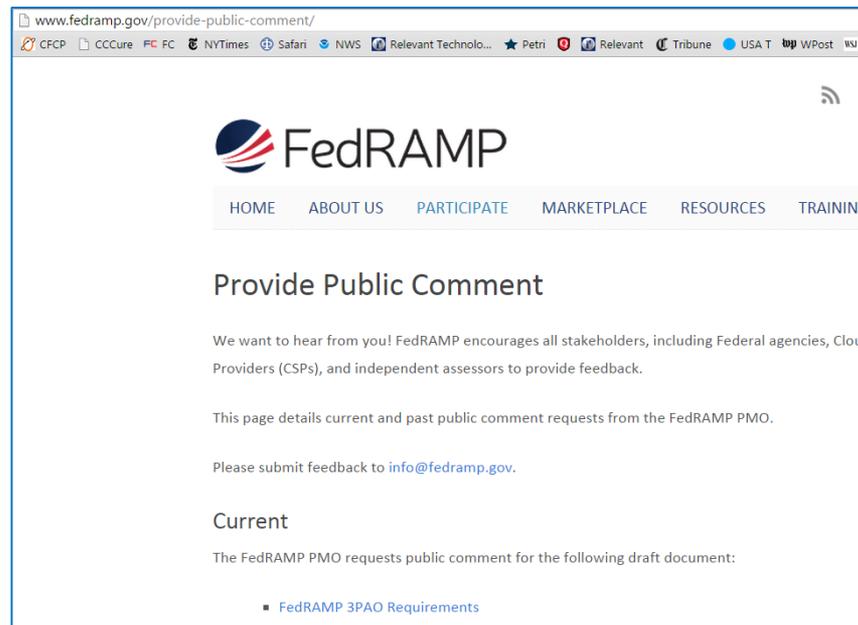




Send Feedback

- You can find the entire document to review at the following URL:

<http://www.fedramp.gov/provide-public-comment/>



- A recording of the webinar will be posted in the near future here:

<https://www.fedramp.gov/fedramp-webinars/>



Questions?

