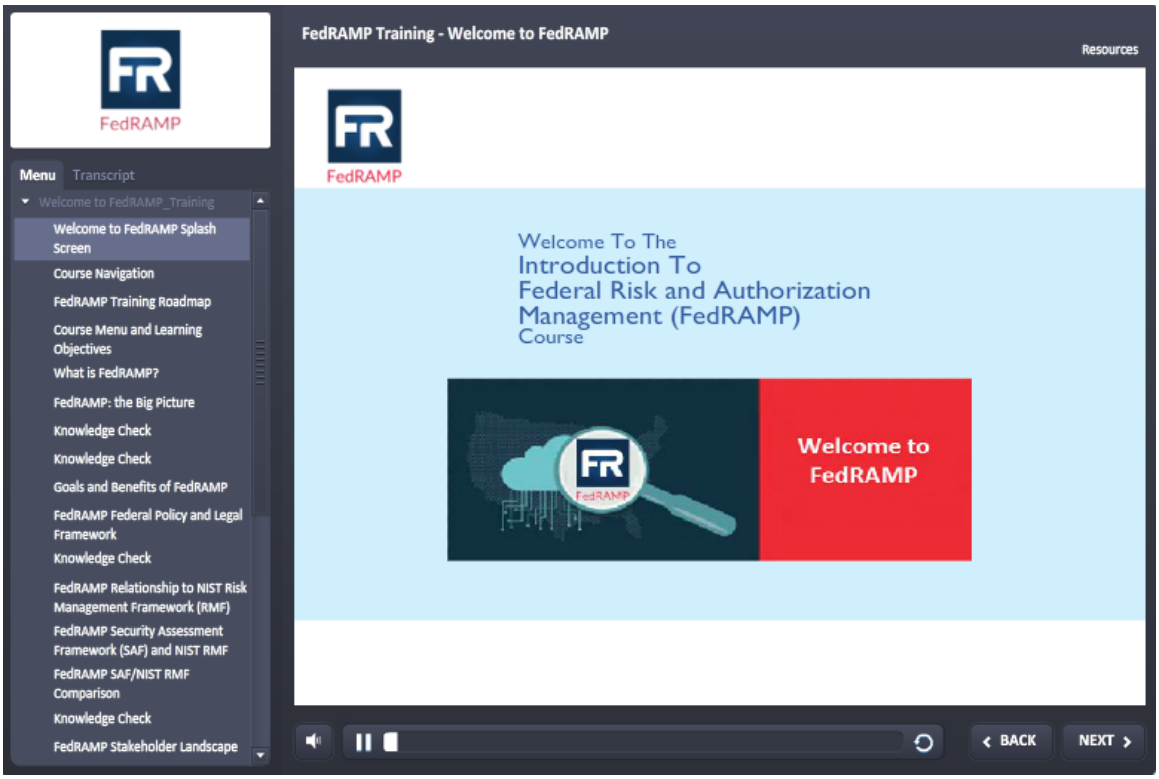
FedRAMP Training - Welcome to FedRAMP

1. Welcome to FedRAMP_Training

1.1 Welcome to FedRAMP Splash Screen



Notes:

Transcript

Title

Welcome to the Introduction to the Federal Risk and Authorization Management Program (FedRAMP) Course

Text

Introduction to the Federal Risk and Authorization Management Program (FedRAMP). Presented by: GSA FedRAMP Program Management Office (PMO). Select the Next button to begin.

Image

Image of FedRAMP logo.

Audio

<N/A>

1.2 Course Navigation

Notes:

Transcript

Title

Course Features and Functions

Text

Select each icon to view the topics and learning objectives

Image

Screen capture of the course including the FedRAMP logo, Transcript and Menu tabs, Navigation buttons, and Resources button.

Audio

Let's take a moment to familiarize ourselves with the features and functions of this course. To navigate the course, you may select the Back and Next buttons located at the bottom of the screen, or you may use the Menu tab located on the left side of the screen to select the screen you'd like to view. Use the Play and Pause buttons located at the bottom of the screen to start and stop the screen content. You may also select the Replay button to view the content again. Use the Transcript tab on the left side of the screen to read a detailed description of the screen elements including the image descriptions, screen text, and audio script. You may also access the Resources button at the top right corner of the screen to open additional course resources.

FedRAMP Training - Welcome to FedRAMP

Menu (Slide Layer)

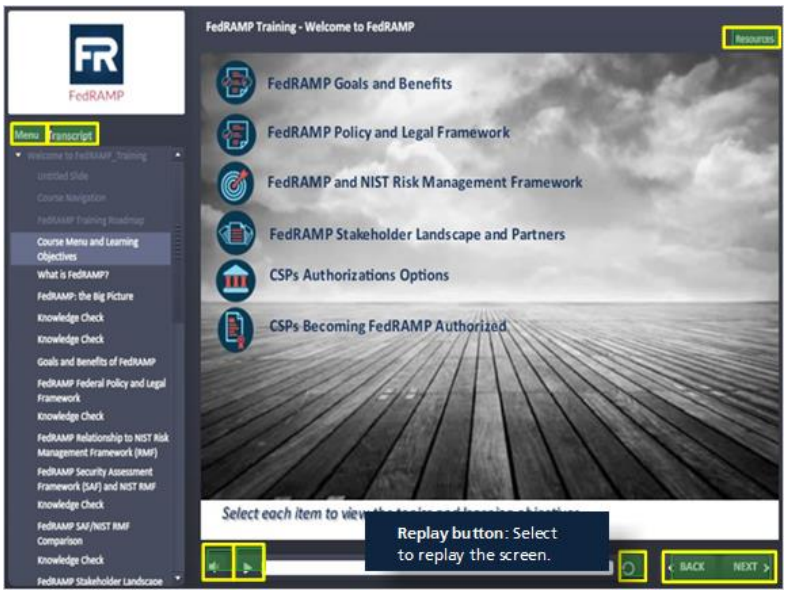
Transcript (Slide Layer)

FedRAMP Training - Welcome to FedRAMP

Resources (Slide Layer)

Play/Pause (Slide Layer)

Replay (Slide Layer)



Back/Next (Slide Layer)

Volume Control (Slide Layer)

1.3 FedRAMP Training Roadmap

Notes:

Transcript

Title

FedRAMP Training - Welcome to FedRAMP

FedRAMP Training Roadmap

Text

Here is where you are in your training. Select any of the map points to see where you've been and where you're going.

Course 100-A button, Welcome to FedRAMP. This course (being completed now) provides an overview of the FedRAMP program and how it works.

Course 200-A button, FedRAMP System Security Plan (SSP) Required Documents. You will learn how to populate the SSP.

Course 200-B button, How to Write a Control. You will learn to write a security control implementation description.

Course 200-C button, Continuous Monitoring (or ConMon) Overview. You will learn the CSP role and responsibilities for Continuous Monitoring.

Course 300 Series:

- Course 300-A: 3PAO FedRAMP 17020 Requirements: Understanding and Bridging the Gap
- Course 300-B: 3PAO FedRAMP Security Assessment Plan (SAP) Guidance
- Course 300-C: 3PAO FedRAMP Security Assessment Report (SAR) Guidance
- Course 300-D: 3PAO FedRAMP Assessment: Documenting Evidence Procedures
- Course 300-E: 3PAO Understanding and Documenting FedRAMP Vulnerability Scanning Requirements
- Course 300-F: 3PAO Review of FedRAMP Security Assessment Report (SAR) Tables
- Course 300-G: 3PAO Readiness Assessment Report (RAR) Preparation

Course 400-A button, Inclusion of FedRAMP in the Procurement Process, whereby Contracting Officers (COs) can get a clearer understanding of FedRAMP in the acquisition and procurement lifecycle.

Monthly Webinars (via Adobe Connect) button, an opportunity to participate in monthly webinars that cover a vast array of topics for the CSP community.

Image

Screen capture of a roadmap of all course offerings

Audio

This is the introductory course in the FedRAMP training series. Here is where you are in your training. Select any of the map points to see where you've been and where you're going.

Course 100-A button, Welcome to FedRAMP. This course (being completed now) provides an overview of the FedRAMP program and how it works.

Course 200-A button, FedRAMP System Security Plan (SSP) Required Documents. You will learn how to populate the SSP.

Course 200-B button, How to Write a Control. You will learn to write a security control implementation description.

Course 200-C button, Continuous Monitoring (or ConMon) Overview. You will learn the CSP role and responsibilities for Continuous Monitoring.

Course 300 Series:

- Course 300-A: 3PAO FedRAMP 17020 Requirements: Understanding and Bridging the Gap
- Course 300-B: 3PAO FedRAMP Security Assessment Plan (SAP) Guidance
- Course 300-C: 3PAO FedRAMP Security Assessment Report (SAR) Guidance

- Course 300-D: 3PAO FedRAMP Assessment: Documenting Evidence Procedures
- Course 300-E: 3PAO Understanding and Documenting FedRAMP Vulnerability Scanning Requirements
- Course 300-F: 3PAO Review of FedRAMP Security Assessment Report (SAR) Tables
- Course 300-G: 3PAO Readiness Assessment Report (RAR) Preparation

Course 400-A button, Inclusion of FedRAMP in the Procurement Process, whereby Contracting Officers (COs) can get a clearer understanding of FedRAMP in the acquisition and procurement lifecycle.

Monthly Webinars (via Adobe Connect) button, an opportunity to participate in monthly webinars that cover a vast array of topics for the CSP community

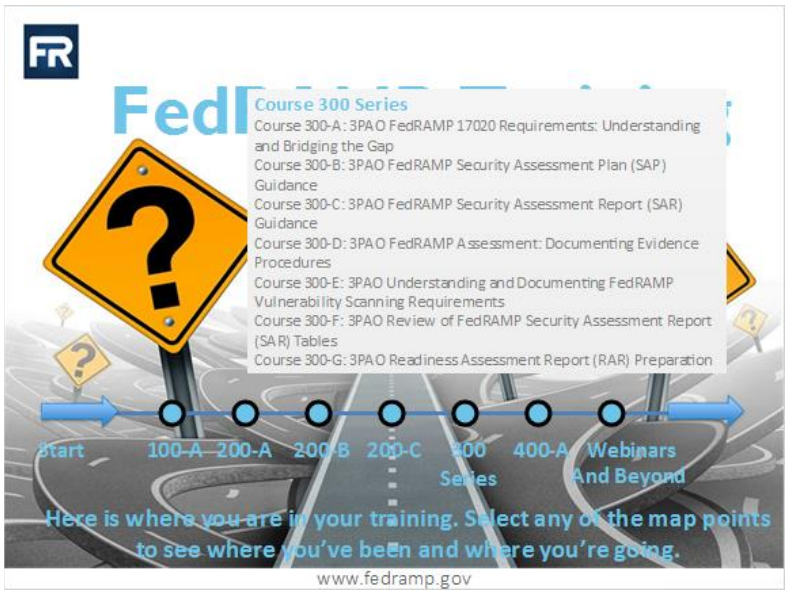
100-A Being Completed (Slide Layer)

200-A (Slide Layer)

200-B (Slide Layer)

200-C (Slide Layer)

300 Series (Slide Layer)



400-A (Slide Layer)

Webinars (Slide Layer)

100-A (Slide Layer)

1.4 Course Menu and Learning Objectives

Notes:

Transcript

Title

FedRAMP Training - Welcome to FedRAMP

Course Menu and Learning Objectives

Text
Select each item to view the topics and learning objectives

- FedRAMP Goals and Benefits
- FedRAMP Policy and Legal Framework
- FedRAMP and the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- FedRAMP Stakeholder Landscape and Partners
- CSPs Authorizations Options
- CSPs Becoming FedRAMP Authorized

Image

Black and white picture overlooking the sky

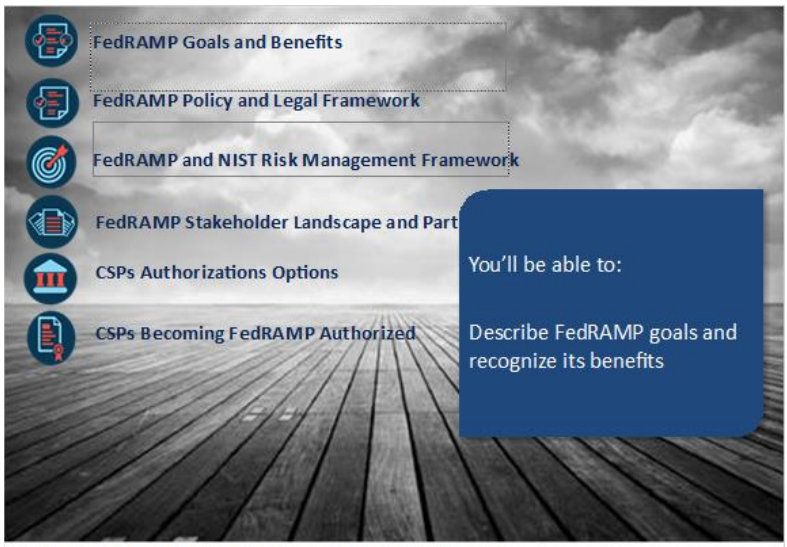
Audio

Today's training will provide an overview of the FedRAMP program and how it works. Select each item to view the topics and learning objectives.

At the end of the course, you will be able to:

- Describe FedRAMP goals and recognize its benefits
- Describe FedRAMP U.S. Federal Government policy and legal framework
- Identify FedRAMP Stakeholder Landscape and list FedRAMP partners
- Describe the relationship between FedRAMP and the NIST RMF
- List options available for a CSP to achieve authorization
- Describe how a CSP can become FedRAMP authorized

Goals and Benefits (Slide Layer)



Select each item to view the topics and learning objectives

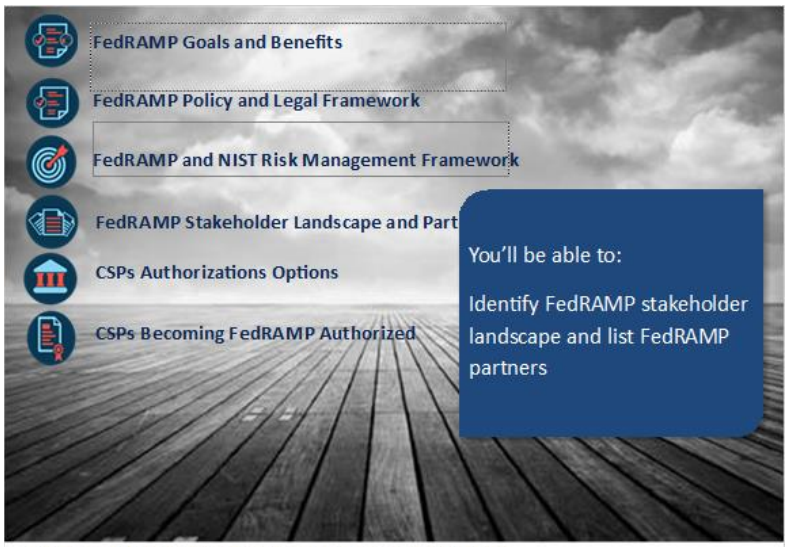
FedRAMP U.S. Federal Government Policy and Legal Framework (Slide Layer)

Select each item to view the topics and learning objectives

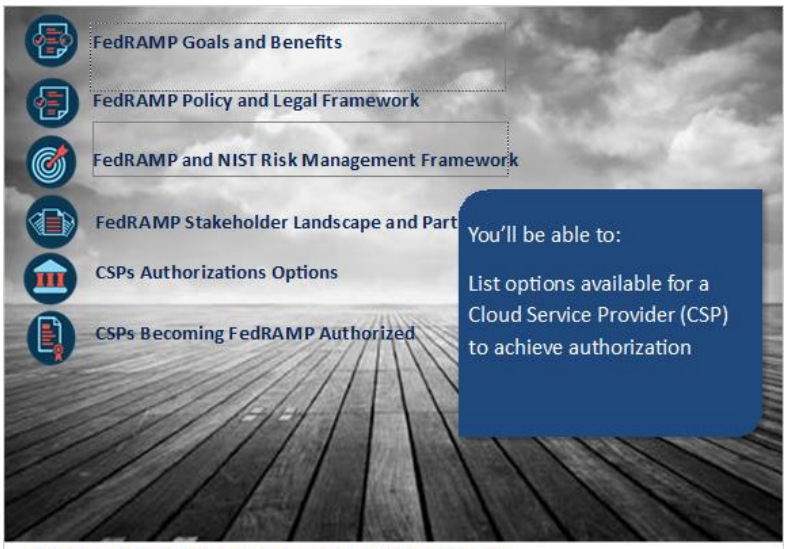
FedRAMP Training - Welcome to FedRAMP

FedRAMP and NIST RMF Framework (Slide Layer)

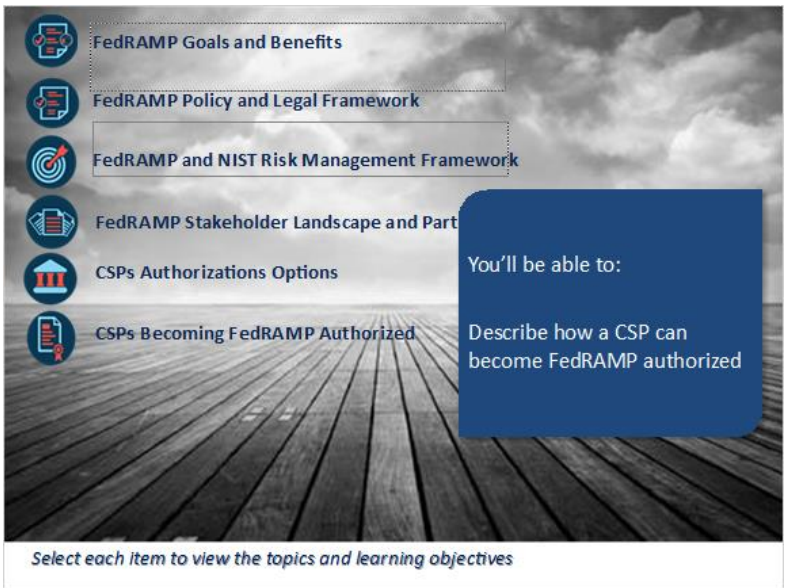
FedRAMP Stakeholder Landscape and Partners (Slide Layer)



CSPs Authorization Options (Slide Layer)



CSPs becoming FedRAMP Authorized (Slide Layer)



1.5 What is FedRAMP?

Notes:

Transcript

Title

FedRAMP Overview

Text

- Memorandum for Chief Information Officers, dated 12/8/2011, Subject: Security Authorization of Information Systems in Cloud Computing Environments established the need for FedRAMP
- Establishes FedRAMP as federal policy for the protection of federal information in cloud services
- Defines executive department and agency responsibilities in developing, implementing, operating, and maintaining FedRAMP. FedRAMP focuses on ensuring that the rigorous security standards of Federal Information Security Management Act of 2002 (or FISMA) are applied while introducing efficiencies to the process for cloud systems (key of which is re-use)
- Defines the requirements for executive departments and agencies using FedRAMP in the acquisition of cloud services as "Executive departments and agencies procuring commercial and non-commercial cloud services that are provided by information systems that support the operations and assets of the departments and agencies, including systems provided or managed by other departments or agencies, contractors, or other sources".

Before FedRAMP icon (user selects): Did you know that the federal government spends hundreds of millions of dollars a year securing its IT Systems and on cybersecurity efforts? The problem is complex: NIST requirements are interpreted differently from agency-to-agency; 2. Agencies did not adequately implement FISMA due to resource constraints; and 3. Agencies did not trust security authorizations from other agencies due to the differing interpretations and incomplete packages. Cloud service offerings were non-standardized and non-comparable when determining security capabilities; and not assessed in a comparable manner by independent third party assessors.

FedRAMP Training - Welcome to FedRAMP

With FedRAMP icon (user selects): FedRAMP standardizes the way the government does security authorizations for cloud products and services in four essential ways: 1. Doing security authorizations once and re-using them may reduce or minimize duplication; 2. Increasing collaboration and creation of a community across the U.S. Government and vendors that did not exist before - FIRST government-wide FISMA program; 3. FedRAMP validating security authorizations to ensure that there is uniformity among security packages; and 4. Enabling a centralized repository where Agencies can request access to security packages for expedient authorizations. With FedRAMP, there is a uniform risk management approach with a standard set of approved minimum security controls (Low, Moderate, High Impact), a consistent assessment process, and a Provisional Authorization To Operate (P-ATO) or an Agency Authorization.

Image

Image of "Before FedRAMP" logo and "With FedRAMP" logo; image of the Executive Office of the President of the United States emblem

Audio

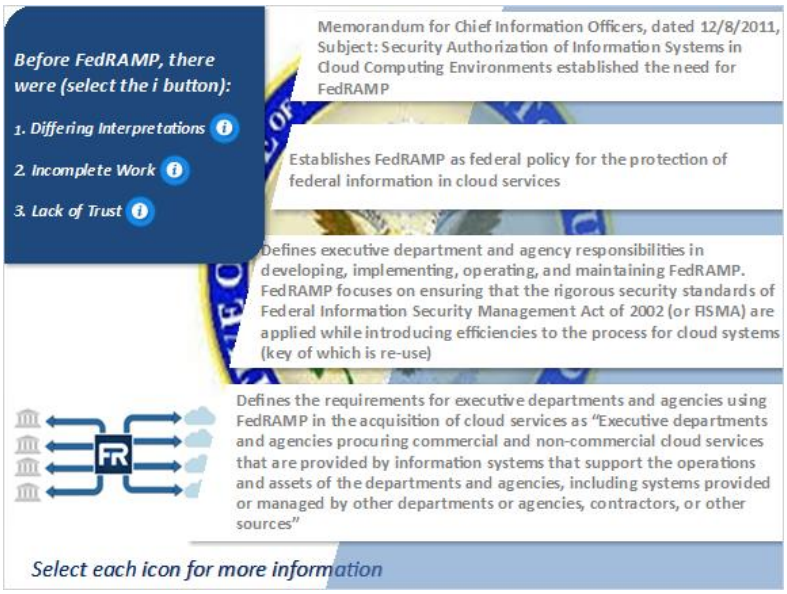
- A little history first. FedRAMP was created out of the Federal Cloud Computing Initiative to remove the barriers to the adoption of the cloud.
- Cloud computing offers a unique opportunity for the federal government to take advantage of cutting edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens.
- FedRAMP provides a cost-effective, risk-based approach for the adoption and use of cloud services. Established in December 2011, FedRAMP is the first government-wide security authorization program for FISMA which requires each Federal Agency to develop, document, and implement programmatic information security for systems that support the operations and assets of the agency. This also includes systems and services provided or managed by another agency, contractor, or other source. FedRAMP processes are designed to assist agencies in meeting FISMA requirements for cloud systems and addresses complexities of cloud systems that create unique challenges for complying with FISMA.
- FedRAMP defines executive department and agency responsibilities in developing, implementing, operating, and maintaining FedRAMP. FedRAMP focuses on ensuring that the rigorous security standards of Federal Information Security Management Act of 2002 (or FISMA) are applied while introducing efficiencies to the process for cloud systems (key of which is re-use)

Before FedRAMP icon (user selects): Did you know that the Federal Government spends hundreds of millions of dollars a year securing its IT Systems and on cybersecurity efforts? The problem is complex: 1. NIST requirements are interpreted differently from agency-to-agency; 2. Agencies did not adequately implement FISMA due to resource constraints; and 3. Agencies did not trust security authorizations from other agencies due to the differing interpretations and incomplete packages. Cloud service offerings were non-standardized and non-comparable when determining security capabilities; and not assessed in a comparable manner by independent third party assessors.

With FedRAMP icon (user selects): FedRAMP standardizes the way the Government does security authorizations for cloud products and services in four essential ways: 1. Doing security authorizations once and re-using them may reduce or minimize duplication; 2. Increasing collaboration and creation of a community across the U.S. Government and vendors that did not exist before - FIRST government-wide FISMA program; 3. FedRAMP validating security authorizations to ensure that there is uniformity among security packages; and 4. Enabling a centralized repository where agencies can request access to security packages for expedient authorizations. With FedRAMP, there is a uniform risk management approach with a standard set of approved minimum security controls (Low, Moderate, High Impact), a consistent assessment process, and a Provisional Authorization To Operate (P-ATO) or an Agency Authorization.

FedRAMP Training - Welcome to FedRAMP

Prior to FedRAMP (Slide Layer)



With FedRAMP (Slide Layer)

1.6 FedRAMP: the Big Picture

Notes:

Transcript

Title

FedRAMP: the Big Picture . . .

Text

- You should know that FedRAMP was created out of the Federal Cloud Computing Initiative. The initiative was designed to remove key barriers to adoption of cloud computing. Agencies expressed that security was the first concern, leading to the development of FedRAMP. Through the adoption of FedRAMP across the US Federal Government, all stakeholders (Cloud Service Providers, Agencies, Third Party Assessment Organizations) are becoming increasingly "cloud-savvy". It is important that you understand the FedRAMP Story.
- Select each image below to learn more. When you are done, select Close to move on to the next topic.

- Button 1: Cloud Computing and FedRAMP
  - FedRAMP was created out of the Cloud Computing initiative in order to remove the barriers for the adoption of cloud computing; in response to Agencies' first concern for Security, and in order to reduce our number 1 barrier: Security.
  - We'll discuss FedRAMP Goals shortly in this course.
  - Close button.

- Button 2: Why Must Cloud Service Providers and Agencies perform Security Authorizations?
  - In the Commercial Environment for CSPs, the goal is to securely compete on contracts with the federal government, and simultaneously protect intellectual property.

- In the Government Environment, it is required by the Office of Management and Budget (OMB) based upon the United States legislation, FISMA, to "define a comprehensive framework" to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law as part of the Electronic Government Act of 2002. FISMA and the Electronic Government Act of 2002 are designed to protect the created, transmitted, and stored data and information that supports the operations of our Federal Government."
- Close button.

- Button 3: The Legal Framework
  - Let's focus on the Legal Framework within our Government which consists of the following: 1. Law = FISMA or Federal Information Security Management Act; 2. OMB Circular A130 Revised 7/28/2016; 3. NIST Guidance and 800 Series Special Publications.
  - Select this link to learn more.
  - Close button.

The Legal Perspective link

FedRAMP is required for Federal Agencies

Notes:

Transcript

Title

FedRAMP is required for Federal Agencies

Text

FedRAMP Training - Welcome to FedRAMP

FedRAMP is required for Federal Agencies. The law states that each Agency must grant security authorizations.

LAW = FISMA - Federal Information Security Management Act REQUIRES Agencies to do cybersecurity

MANDATE = WHITE HOUSE - OMB states that when agencies implement FISMA, they must use the NIST framework (Circular A-130)

POLICY = FEDRAMP - FedRAMP says when using cloud, agencies must implement NIST via FedRAMP requirements

AUTHORIZE = AGENCY - each Agency ultimately must individually authorize a system for use

Image

Images of icons representing LAW, MANDATE, POLICY, AUTHORIZE

Audio

FedRAMP is required for Federal Agencies. The law states that each Agency must grant security authorizations. FedRAMP fits within the same framework Agencies are using currently to provide security authorizations of IT services.

So, let's breakdown how this work in a simple example:

With LAW = FISMA - Federal Information Security Management Act REQUIRES Agencies to do cybersecurity; in other words, this law (FISMA) mandates that Agencies authorize IT systems that store, process, or transmit Federal information.

With MANDATE = WHITE HOUSE - OMB states that when Agencies implement FISMA, they must use the NIST framework (Circular A-130); OMB dictates to Agencies through Circular A-130 that Agencies use NIST standards when authorizing systems according to FISMA.

With POLICY = FEDRAMP - FedRAMP says when using cloud, Agencies must implement NIST via FedRAMP requirements; OMB also further clarified that Agencies must follow the FedRAMP requirements when granting authorizations for cloud services.

With AUTHORIZE = AGENCY, where each Agency ultimately must individually authorize a system for use.

- Button 4: NIST SP 800-37 Revision 1 Framework
  - Let's keep going . . . with NIST SP 800-37 Revision 1 Framework, which is comprised of six separate elements: 1. Categorize Information System; 2. Select Security Controls; 3. Implement Security Controls; 4. Assess Security Controls; 5. Authorize Information System; 6. Monitor Security Controls.
  - Select this link to learn more.
  - Close button.

800-37-RISK MANAGEMENT FRAMEWORK link

The Six Phases . . .

Notes:

Transcript

Title

800-37 RISK MANAGEMENT FRAMEWORK

Text

Process flow of icons:

- CSPs Define Data Type
- CSPs Select Controls
- CSPs Implement and Document
- 3PAOs Assess

- Agencies Authorize
- CSPs/3PAOs Continuous Monitoring

Image

Images of icons representing Define Data Type; Select Controls; Implement and Document; Assess (Interview, Examine, and Test); Authorized (System for use; Accept Risk of System); Continuous Monitoring

Audio

The NIST Risk Management Framework has 6 steps - from defining your data to continuous monitoring. Let's briefly review each step:
1. CSPs Define Data Type: this may be defined by a simple example (such as email data), which is aligned to a governing standard like Federal Information Processing (FIPS) 199, using a Low, Moderate or High baseline

2. CSPs Select Controls: this refers to the NIST 800-53. In fact, security authorizations require vendors to implement hundreds of security controls (100+ for public data, 300+ for standard systems, and 400+ for high risk systems)

3. CSPs Implement and Document: this refers to the various documents that are required for authorization (such as the System Security Plan or SSP). Vendors must fully document and have an independent auditor validate the security of their system.

4. 3PAOs Assess: this refers to the process of interviewing, examining, and testing of specific controls by an independent assessor like the 3PAO or Third Party Assessment Organization; this takes thousands of pieces of evidence and also has a high cost to government and industry - in order to validate a vendors and thousands of pieces of evidence that take months to complete.

5. Agencies Authorize, whereby the system is ready for use through the use of an Authorization to Operate (ATO) Letter. While FISMA dictates that Federal agencies make individual decisions for security authorizations, FedRAMP's goal is to enable re-use.

6. CSPs/3PAOs conduct Continuous Monitoring, at monthly or yearly intervals.

- Button 5: Federal Stakeholder Landscape
    - There are six areas of FedRAMP Stakeholder Landscape, which include: 1. Joint Authorization Board (JAB) Charter V2.0 dated 1/26/2016, whereby the Federal Chief Information Officer (CIO) and directed CIOs of the Department of Defense (DoD), the Department of Homeland Security (DHS), and the General Services Administration (GSA) make up the JAB; 2. GSA FedRAMP PMO; 3. DHS, by monitoring and reporting on security incidents and by providing monitoring; 4. OMB; 5. Federal CIO Council; and 6. NIST.
    - Close button.

Image

Image of five big picture steps: Cloud Computing; Cloud Security; Legal Framework; NIST; Stakeholder Landscape

Audio

- You should know that FedRAMP was created from the Federal Cloud Computing Initiative, consistent with the President's International Strategy for Cyberspace and Cloud First policy, which was designed to remove barriers to the adoption of cloud computing. The number 1 barrier was/is Cloud security! Through the adoption of FedRAMP across the U.S. Federal Government, all stakeholders (Cloud Service Providers, Agencies, Third Party Assessment Organizations) are becoming increasingly "cloud-savvy". It is important that you understand the FedRAMP Story. After you select and read the text for each image below, you'll be able to advance to the next page by selecting the 'Close' button at the bottom right of each text box.

Layer 1 (Slide Layer)

Layer 2 (Slide Layer)

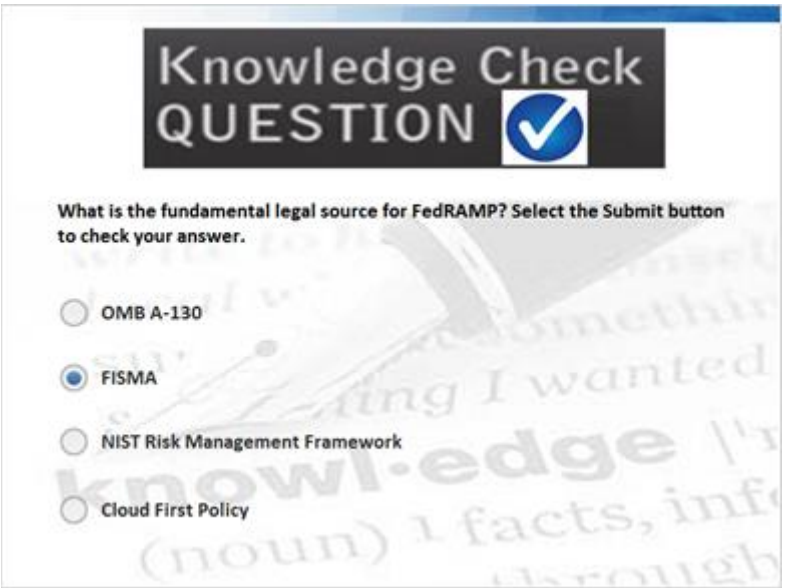
Layer 3 (Slide Layer)

Layer 4 (Slide Layer)

Layer 5 (Slide Layer)

1.7 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)



Correct	Choice
	OMB A-130
X	FISMA
	NIST Risk Management Framework
	Cloud First Policy

Feedback when correct:

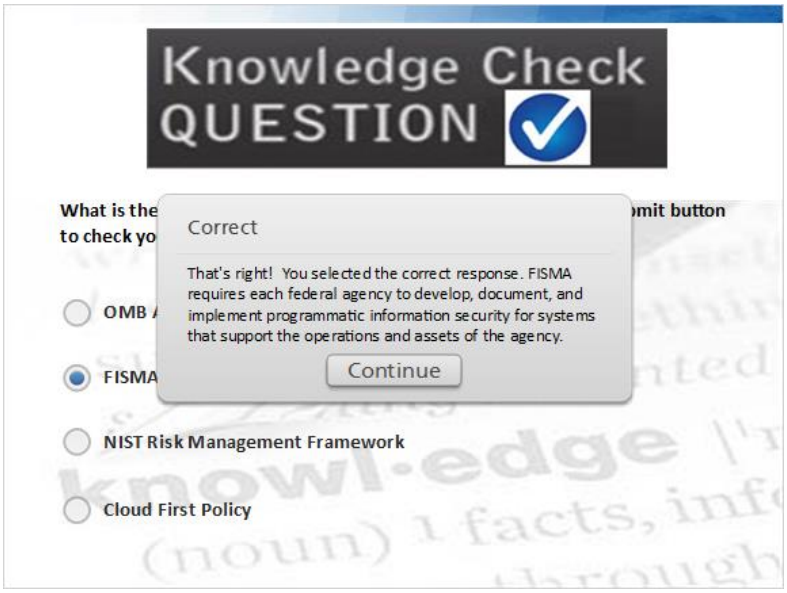
That's right! You selected the correct response. FISMA requires each federal agency to develop, document, and implement programmatic information security for systems that support the operations and assets of the agency.

Feedback when incorrect:

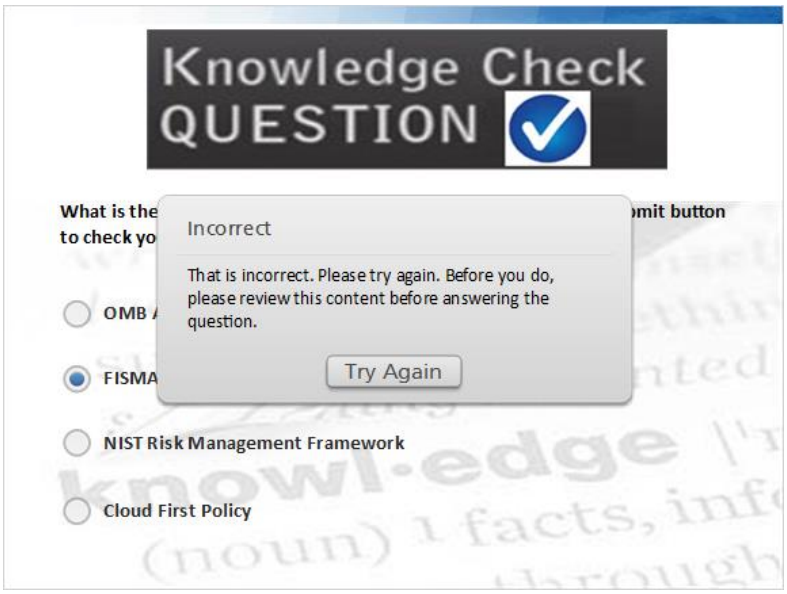
Incorrect! You should have known that the FISMA requires each federal agency to develop, document, and implement programmatic information security for systems that support the operations and assets of the agency.

Notes:

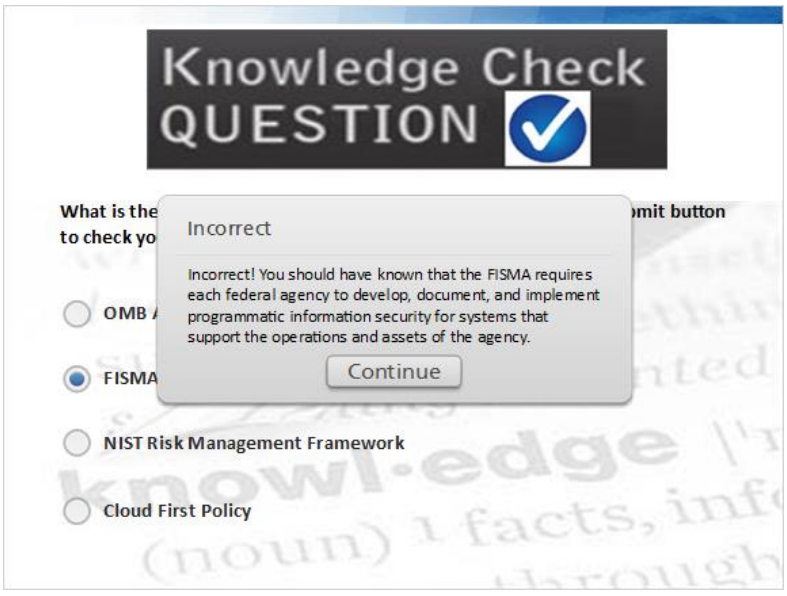
Correct (Slide Layer)



Try Again (Slide Layer)

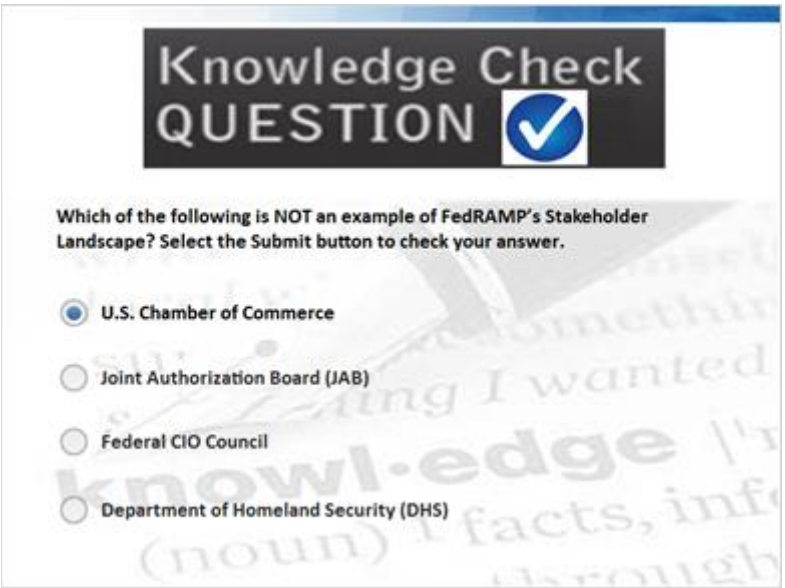


Incorrect (Slide Layer)



1.8 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)



Correct	Choice
X	U.S. Chamber of Commerce
	Joint Authorization Board (JAB)
	Federal CIO Council
	Department of Homeland Security (DHS)

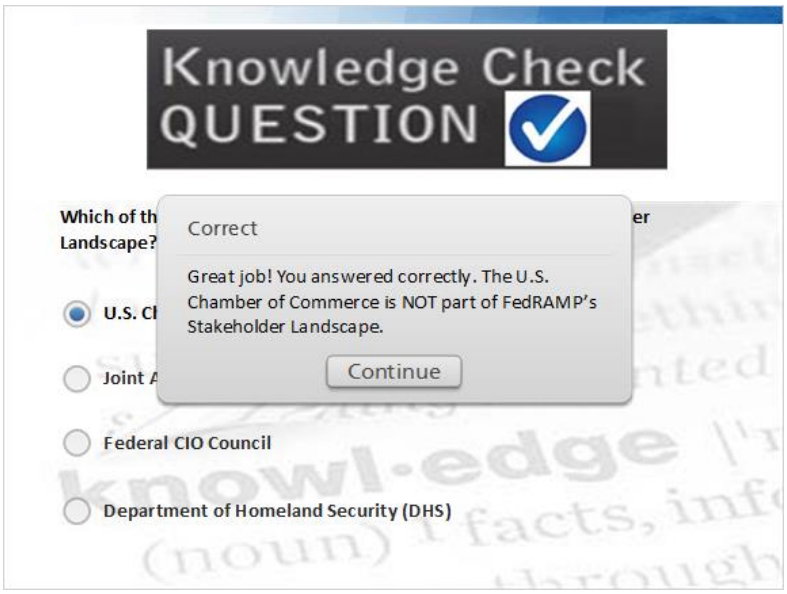
Feedback when correct:

Great job! You answered correctly. The U.S. Chamber of Commerce is NOT part of FedRAMP's Stakeholder Landscape.

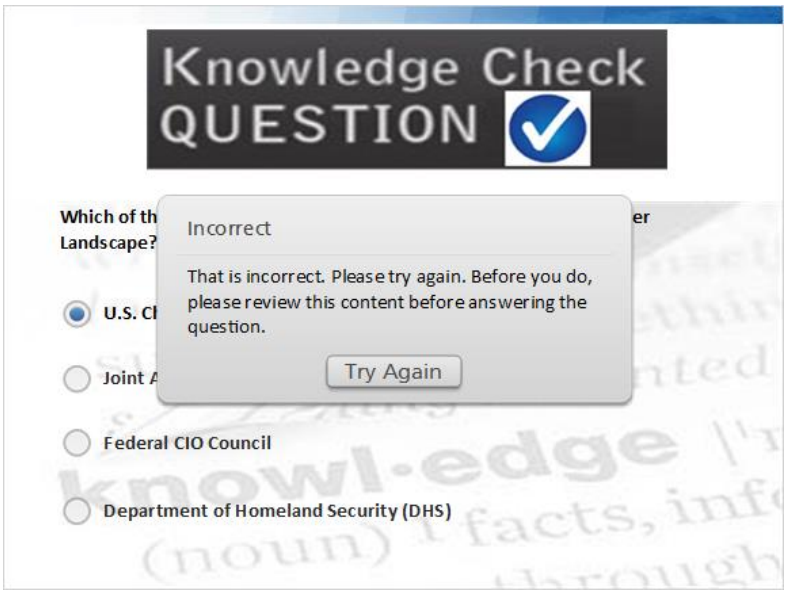
Feedback when incorrect:

Incorrect! You should have known that the U.S. Chamber of Commerce is NOT part of FedRAMP's Stakeholder Landscape.

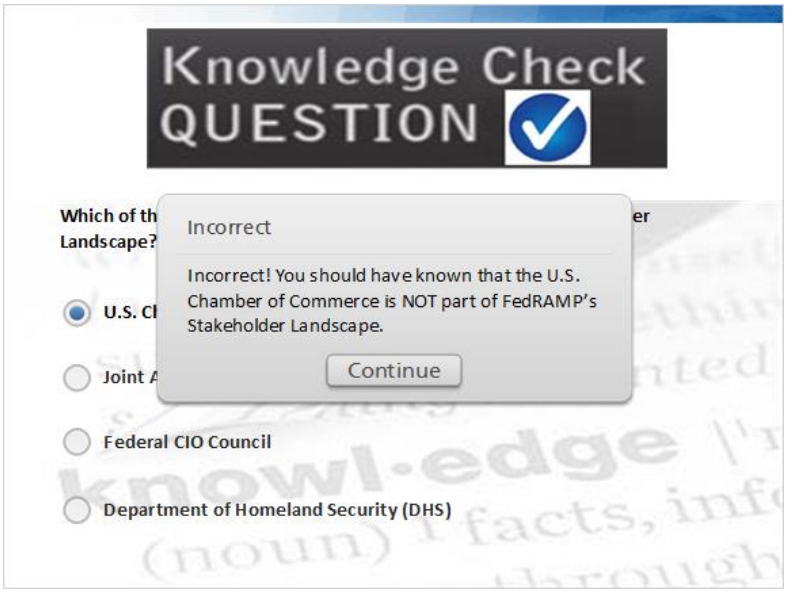
Correct (Slide Layer)



Try Again (Slide Layer)



Incorrect (Slide Layer)



1.9 Goals and Benefits of FedRAMP

Notes:

Transcript

Title

FedRAMP Training - Welcome to FedRAMP

Goals and Benefits of FedRAMP

Text

The Goals of FedRAMP are to

1. Ensure use of cloud services adequately protects and secures federal information

2. Enable cloud services' reuse across the federal government wherever possible to save money and time

Sliding text:

- FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- FedRAMP uses FISMA and NIST defined guidance and frameworks for assessing security in the cloud.
- FedRAMP supports consistent application of best practices and an uniformed approach to assessing cloud services.
- FedRAMP assessment and continuous monitoring processes ensure transparency and trust between the federal government and industry.
- FedRAMP is designed to help accelerate the adoption of cloud computing in the federal government by offering a centralized repository to facilitate
  re-use.

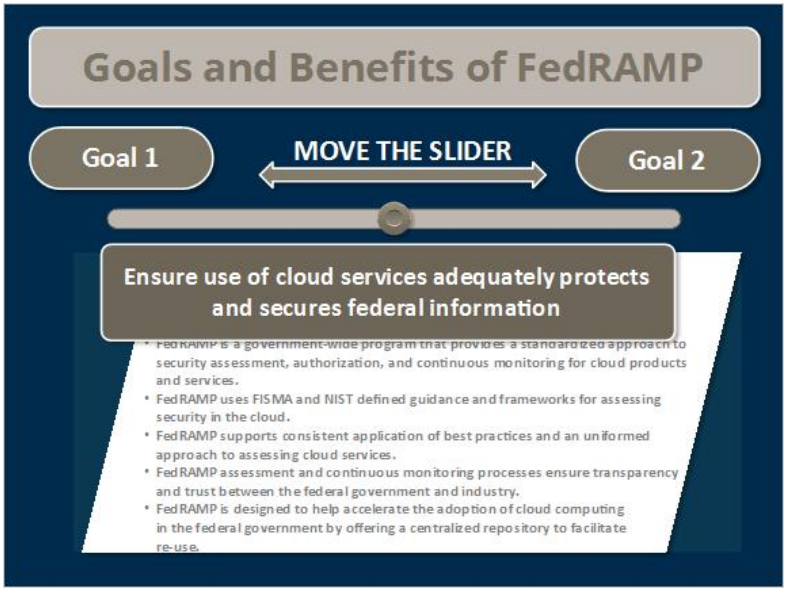
Image

Image of FedRAMP Goals displayed in a circular format

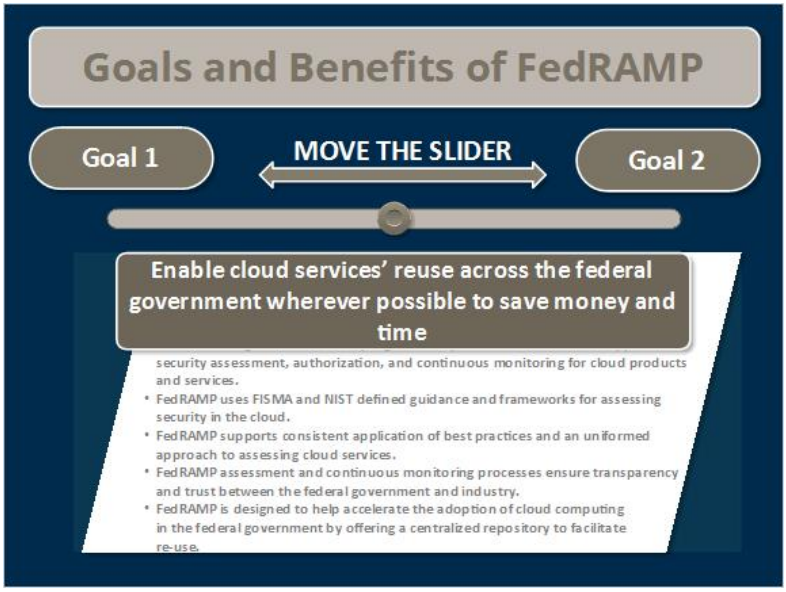
Audio

- FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- FedRAMP uses FISMA and NIST defined guidance and frameworks for assessing security in the cloud.
- FedRAMP supports consistent application of best practices and an uniformed approach to assessing cloud services.
- FedRAMP assessment and continuous monitoring processes ensure transparency and trust between the federal government and industry.
- FedRAMP is designed to help accelerate the adoption of cloud computing in the federal government by offering a centralized repository to facilitate re-use.

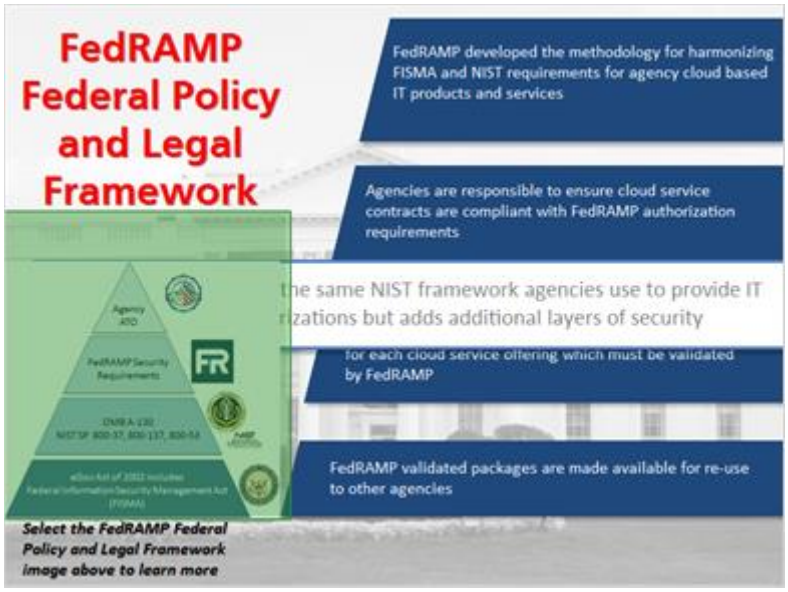
Goal 1 (Slide Layer)



Goal 2 (Slide Layer)



1.10 FedRAMP Federal Policy and Legal Framework



Notes:

Transcript

Title

FedRAMP Federal Policy and Legal Framework

Text

Main slide text: FedRAMP fits within the same NIST framework agencies use to provide IT security authorizations but adds additional layers of security.

Slide text 1: FedRAMP developed the methodology for harmonizing FISMA and NIST requirements for agency cloud based IT products and services.

Slide text 2: Agencies are responsible to ensure cloud service contracts are compliant with FedRAMP authorization requirements.

Slide text 3: Agencies are required to grant individual authorizations for each cloud service offering which must be validated by FedRAMP.

Slide text 4: FedRAMP validated packages are made available for re-use to other agencies.

Image text: Select the FedRAMP Federal Policy and Legal Framework image above to learn more.

FedRAMP Training - Welcome to FedRAMP

Image

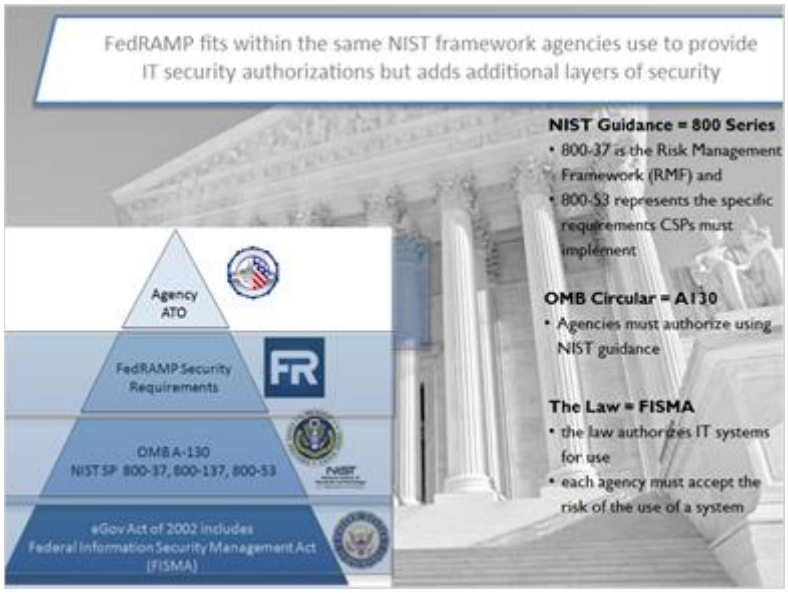
Pyramid showing agency ATO; FedRAMP Security Requirements; OMB A-130 (including NIST SP 800-37; 800-137; 800-53; and eGov Act of 2002 which includes FISMA)

Audio

- FedRAMP fits within the same NIST framework agencies had been using to provide security authorizations of IT services but adds additional layers of security.
- FedRAMP does not replace FISMA - FedRAMP builds upon FISMA.
- FedRAMP developed the methodology for harmonizing FISMA and NIST for FedRAMP security authorization requirements for use with cloud based service offerings
- Agencies are required to use FedRAMP when conducting security authorizations and granting ATOs for all executive department or agency use of cloud services.
- Agencies must ensure cloud IT service contracts comply with FedRAMP security authorization requirements.
- Agencies are responsible to grant individual authorizations.
- FedRAMP validated packages are made available for re-use to other agencies.

The FedRAMP Legal Framework link

The FedRAMP Federal Policy and Legal Framework



Notes:

Transcript

Title

The FedRAMP Legal Framework

Text

In the hierarchy:

- FISMA is the law
- OMB A-130 is the mandate establishing the NIST framework for agencies to implement FISMA
- FedRAMP is the policy based upon OMB A-130 and builds upon NIST security guidance specifically for cloud solutions
- Agencies use FedRAMP requirements to authorize a system for use

FedRAMP fits within the same NIST framework agencies use to provide IT security authorizations but adds additional layers of security.

Image

Image of Court

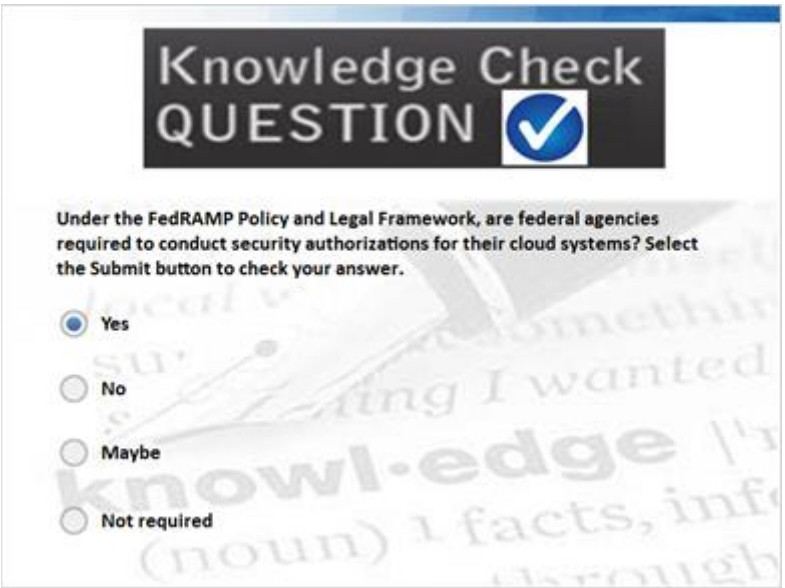
Audio
With the FedRAMP Legal Framework, you will notice the following:

- FISMA is the law
- OMB A-130 is the mandate establishing the NIST framework for agencies to implement FISMA
- FedRAMP is the policy based upon OMB A-130 and builds upon NIST security guidance specifically for cloud solutions

Agencies use FedRAMP requirements to authorize a system for use

1.11 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)



Correct	Choice
X	Yes
	No
	Maybe
	Not required

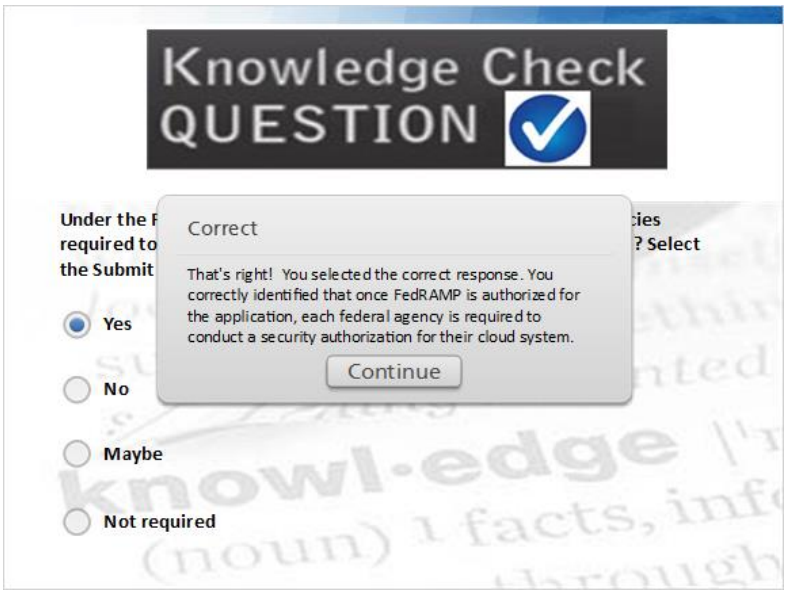
Feedback when correct:

That's right! You selected the correct response. You correctly identified that once FedRAMP is authorized for the application, each federal agency is required to conduct a security authorization for their cloud system.

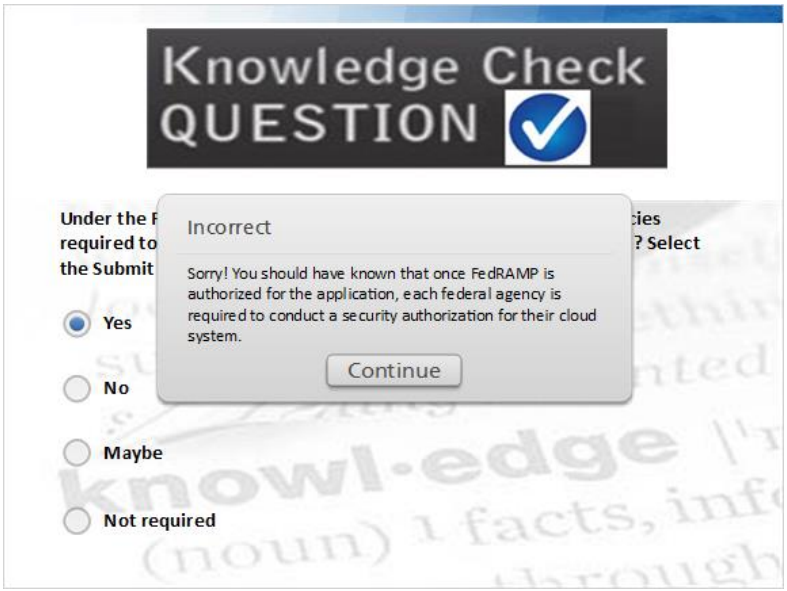
Feedback when incorrect:

Sorry! You should have known that once FedRAMP is authorized for the application, each federal agency is required to conduct a security authorization for their cloud system.

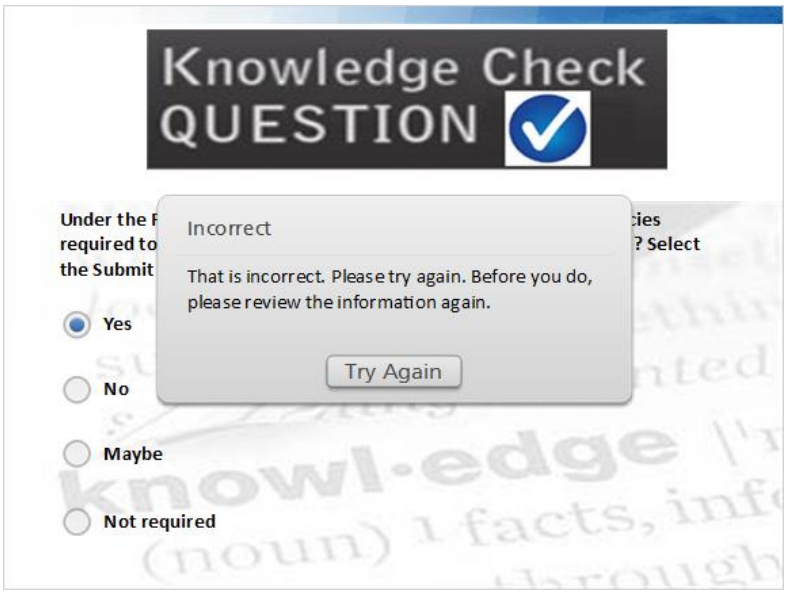
Correct (Slide Layer)



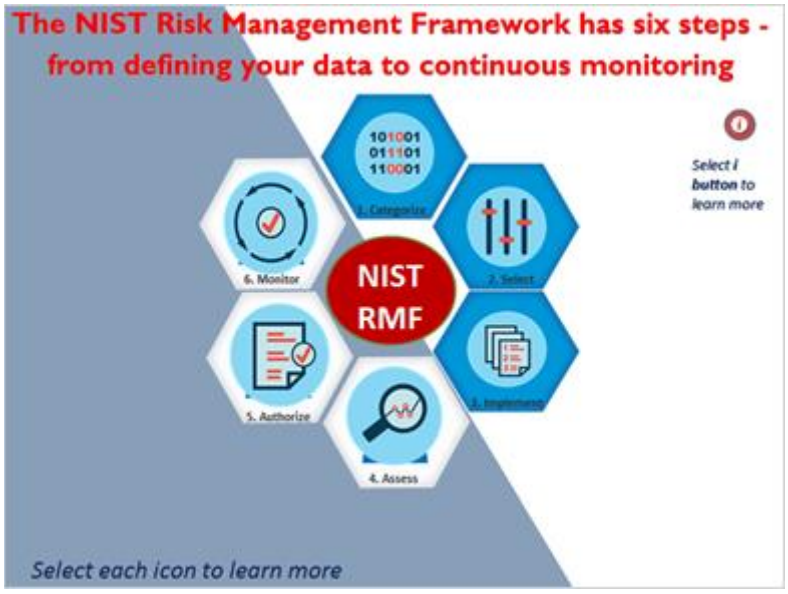
Incorrect (Slide Layer)



Try Again (Slide Layer)



1.12 FedRAMP Relationship to NIST Risk Management Framework (RMF)



Notes:

Transcript

Title

FedRAMP Training - Welcome to FedRAMP

FedRAMP Relationship to NIST RMF

Text
The NIST Risk Management Framework has six steps - from defining your data to continuous monitoring. Select i button to learn more: Did you know that FedRAMP was built on the NIST Risk Management Framework? The NIST Risk Management Framework (RMF) is known as Special Publication (SP) 800-37 (as revised) and is available through the NIST website, which you can find by selecting the Resources tab at the top right portion of this training course.

The purpose of the Risk Management Framework is:

- To ensure that managing risk from the operation and use of federal systems is consistent with the organization's mission, business objectives and overall risk strategy;
- To ensure that information security requirements are integrated into the enterprise architecture;
- To support consistent, well informed, and ongoing security authorization decisions; and
- To achieve more secure information and systems.

Image

Image of NIST RMF surrounded 1. Categorize the Information System; 2. Select the Controls; 3. Implement Security Controls; 4. Assess the Security Controls; 5. Authorize Information System; 6. Monitor Security Controls

Audio
These are the 6 steps in NIST's Risk Management Framework. Select each step to learn more:
1. Categorize the Information System - CSPs define the criticality/sensitivity of the information system data and information according to potential worst-case, adverse impact to mission/business. In order to accurately define the criticality/sensitivity of the system, the system data types must be defined and understood. Many government systems are intended to provide administrative or business services to support mission accomplishment. Each data type stored, processed, and transmitted must be cross-referenced to the "Recommended Provisional Impact Levels for Management and Support Information Types" in NIST Special Publication (SP) 800-60 Volumes 1 and 2. The provisional levels for Confidentiality, Integrity, and Availability (CIA) are listed for each data type. The provisional levels may be adjusted based upon the specific system requirements. All security categorizations and related adjustments are recorded in the FIPS 199 document for the system. The High water mark for CIA is the highest level attained by the aggregation of levels applied to data types, either Low, Moderate, or High.

2. Select Security Controls - CSPs select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment. Once the System Owner and the Authorizing Official have agreed upon the security categorization of the data and information as captured in the FIPS 199, then the security control baseline can be determined. The FedRAMP set of Low, Moderate, and High baselines are rooted in NIST SP 800-53 (as revised) and further enhanced for use by FedRAMP.

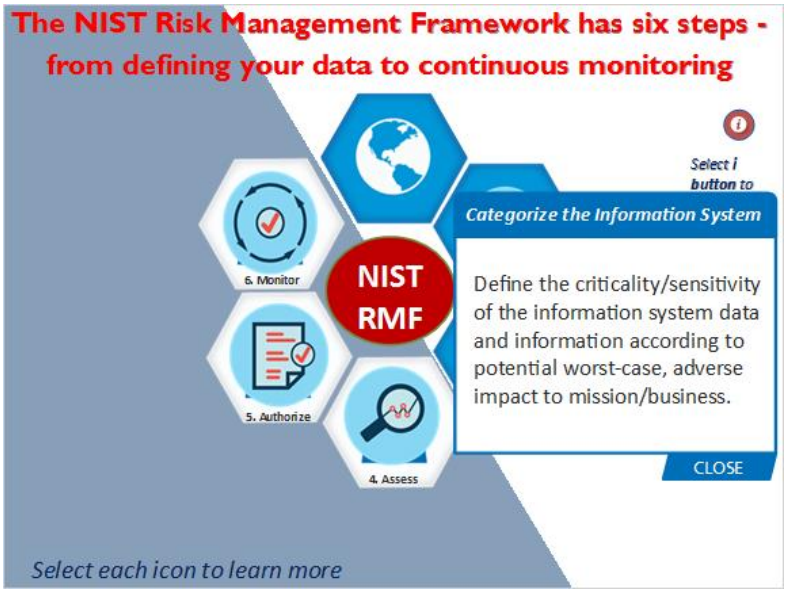
3. Implement Security Controls - CSPs implement security controls consistent with the organization's enterprise architecture and information security architecture using sound systems engineering practices to ensure minimum information assurance methodologies; apply security configuration settings; document the implementation details. The objective is to ensure that the security controls are implemented correctly, so they operate as intended, and meet the organization's security requirements.

4. Assess Security Controls - Third Party Assessment Organizations (3PAOs) determine security control effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements for information system). Ensure that the Assessor chosen has the required amount of technical expertise and independence to conduct an effective assessment. Ensure that the results of the assessment are captured in the security assessment report. This document provides the Authorizing Official with the determination of risk posed by the system.

5. Authorize Information System - Agencies determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation. The Plan of Actions and Milestones (POA&M) identifies tasks planned to remediate and/or mitigate weaknesses and deficiencies identified during the security assessment. If the risk determination based upon the residual risks is beyond the threshold acceptable to the Authorizing Official, the Authorizing Official may not authorize the operation of the system.

6. Monitor Security Controls - Continuously track changes to the information system that may affect security controls and continuously reassess control effectiveness. The ongoing monitoring activities provide near real time risk management. Reports generated are provided to all stakeholders.

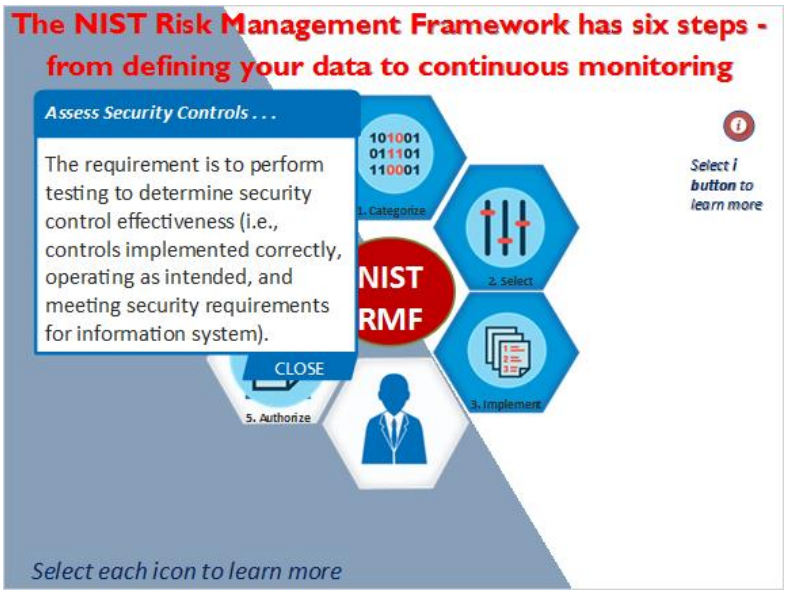
Categorize the Information System (Slide Layer)



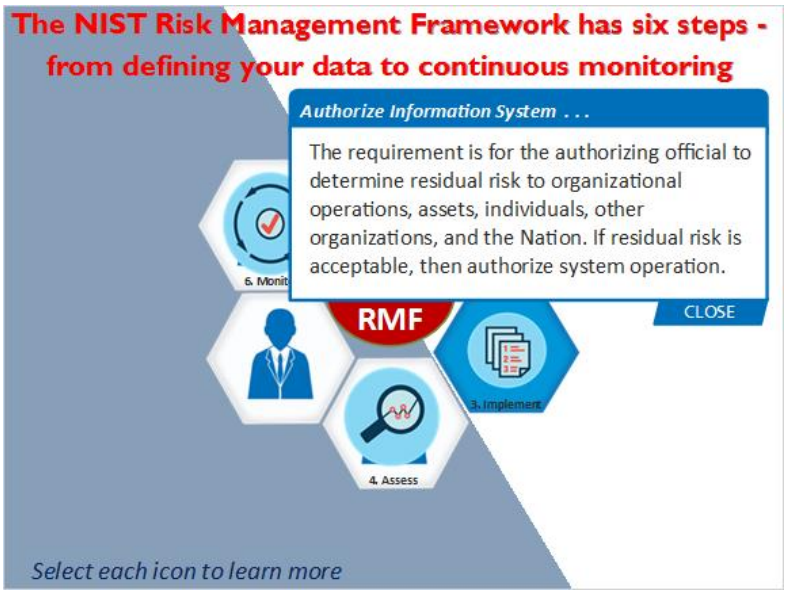
Select the Controls . . . (Slide Layer)

Implement Security Controls (Slide Layer)

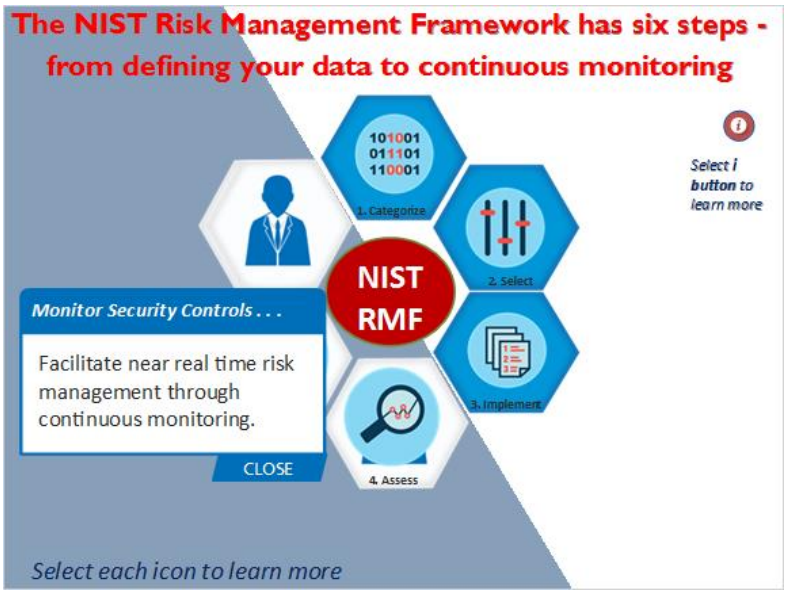
Assess Security Controls . . . (Slide Layer)



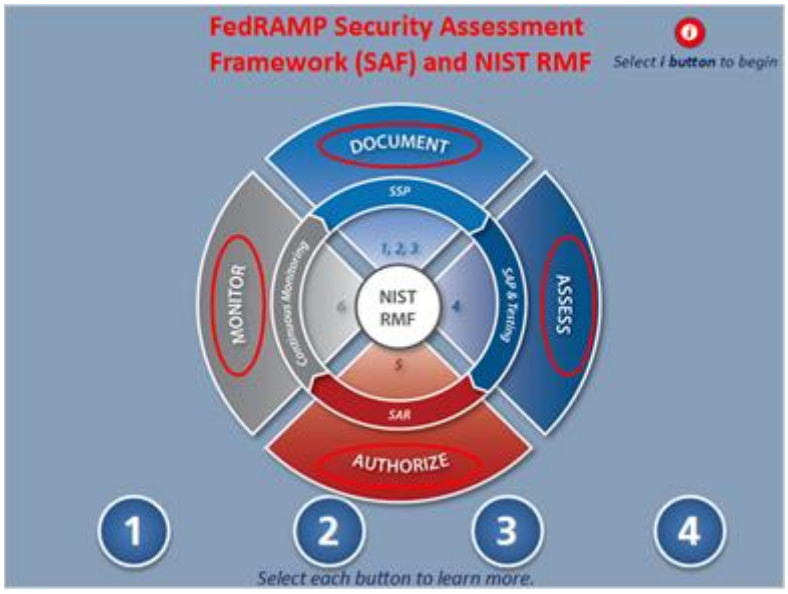
Authorize Information System . . . (Slide Layer)



Monitor Security Controls . . . (Slide Layer)



1.13 FedRAMP Security Assessment Framework (SAF) and NIST RMF



Notes:

Transcript

Title

FedRAMP Training - Welcome to FedRAMP

FedRAMP Security Assessment Framework (SAF) and NIST RMF

Text

NIST RMF surrounded 1. Document (with SSP); 2. Assess (SAP and Testing); 3. Authorize (SAR); 4. Monitor (Continuous Monitoring). Select i button to learn more. Federal Agencies are required to assess and authorize information systems in accordance with FISMA. The FedRAMP Security Assessment Framework (SAF) is compliant with FISMA and is based on the NIST RMF. The FedRAMP SAF methodology utilizes the same processes for creating the documents and deliverables that NIST has always required agencies to use. However, FedRAMP simplifies the NIST RMF by creating four process areas that encompass the 6 steps within 800-37: Document, Assess, Authorize, and Monitor.

Image

Image of NIST RMF surrounded 1. Document; 2. Assess; 3. Authorize; 4. Monitor.

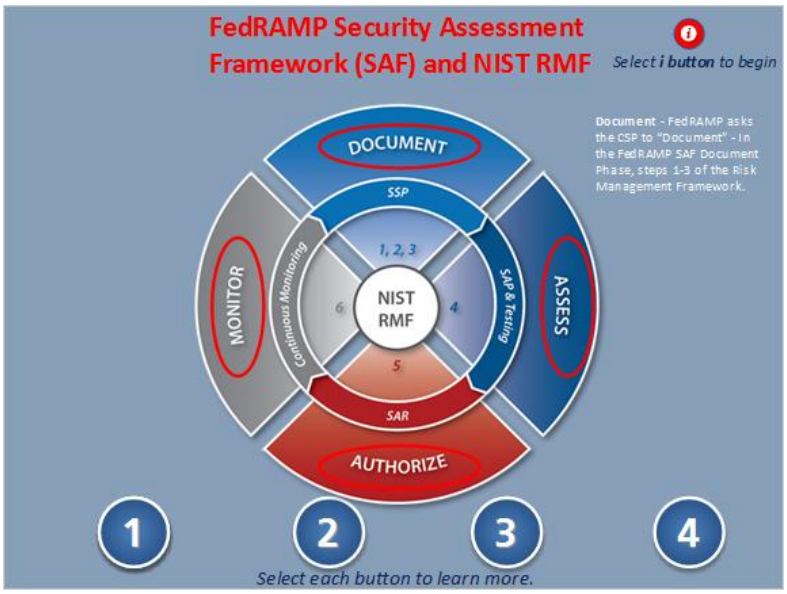
Audio

Federal Agencies are required to assess and authorize information systems in accordance with FISMA. The FedRAMP Security Assessment Framework (SAF) is compliant with FISMA and is based on the NIST RMF.

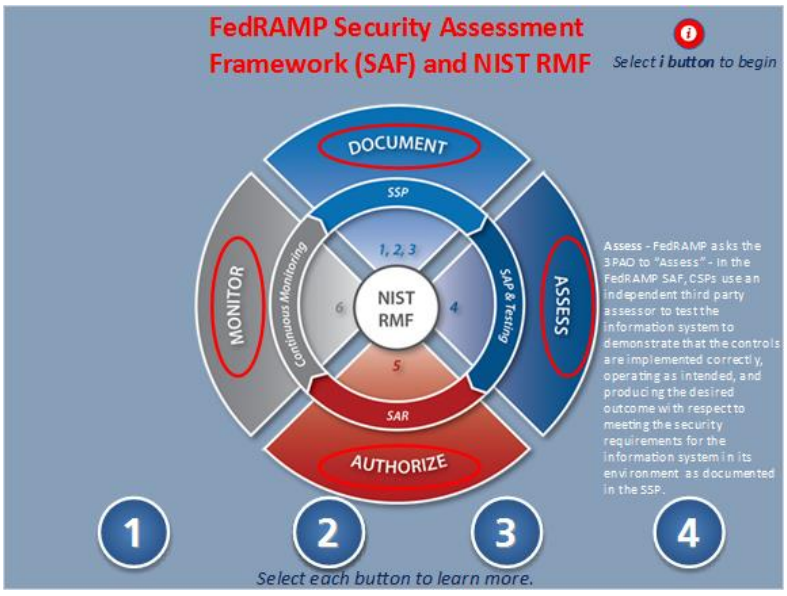
The FedRAMP SAF methodology utilizes the same processes for creating the documents and deliverables that NIST has always required agencies to use. However, FedRAMP simplifies the NIST RMF by creating four process areas that encompass the 6 steps within 800-37: Document, Assess, Authorize, and Monitor.

- FedRAMP asks the CSP to "Document" - In the FedRAMP SAF Document Phase, steps 1-3 of the Risk Management Framework, (i) Categorize, (ii) Select, (iii) Implement are covered by categorizing the information system, selecting the security controls, and implementing and documenting the security controls and implementations in the SSP and supporting documents.
- FedRAMP asks the 3PAO to "Assess" - In the FedRAMP SAF, CSPs use an independent third party assessor to test the information system to demonstrate that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment as documented in the SSP. The assessment starts with documenting the security assessment testing methodology and processes for testing the system environment in the Security Assessment Plan (SAP).
- FedRAMP asks the Authorizing Official to "Authorize" - In the FedRAMP SAF, once testing is completed, the authorizing official(s) make a system authorization decision based on the security system package of documents and the residual risk identified in the Security Assessment Report (SAR).
- FedRAMP asks the CSP and the 3PAO to "Monitor" - In the FedRAMP SAF, ongoing authorization is based upon continuous monitoring of the system environment. Once an information system is authorized, continuous monitoring is the most important safeguard against threats and vulnerabilities and prevents greater than acceptable residual risk within the environment. Ideally, the CSP works to reduce residual risk in an ongoing manner. Continuous Monitoring, when done effectively, determines whether the set of deployed security controls in an information system remain effective in light of planned and unplanned changes that occur in the system and its environment, over time. Continuous monitoring results in greater transparency of the security posture of the CSP cloud service offering and enables timely risk-management decisions.

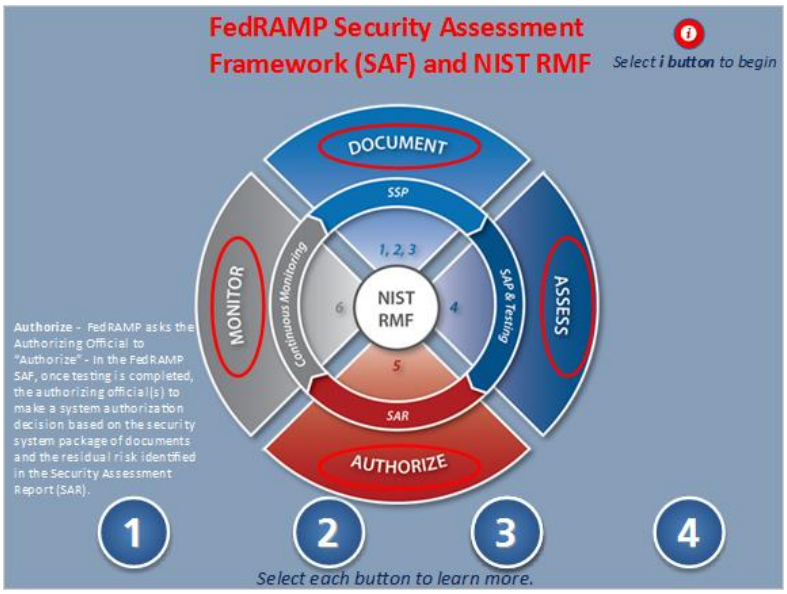
Document (Slide Layer)



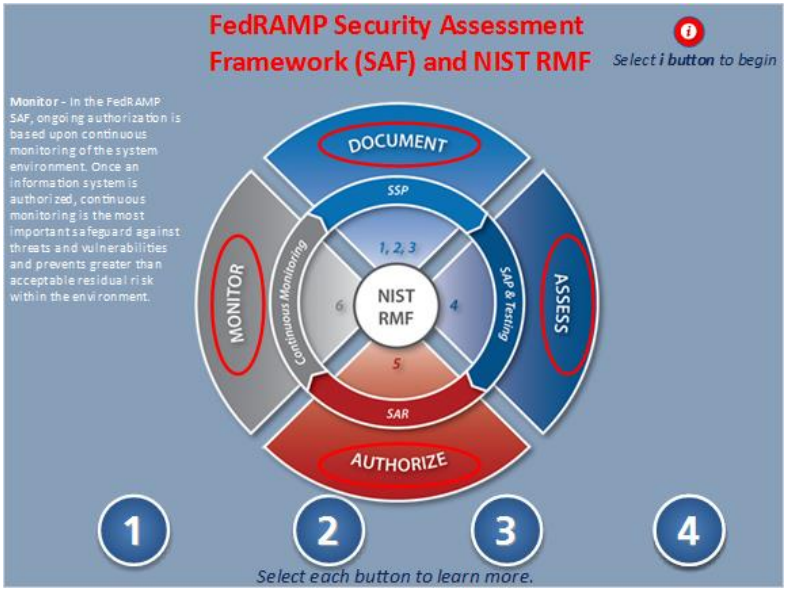
Assess (Slide Layer)



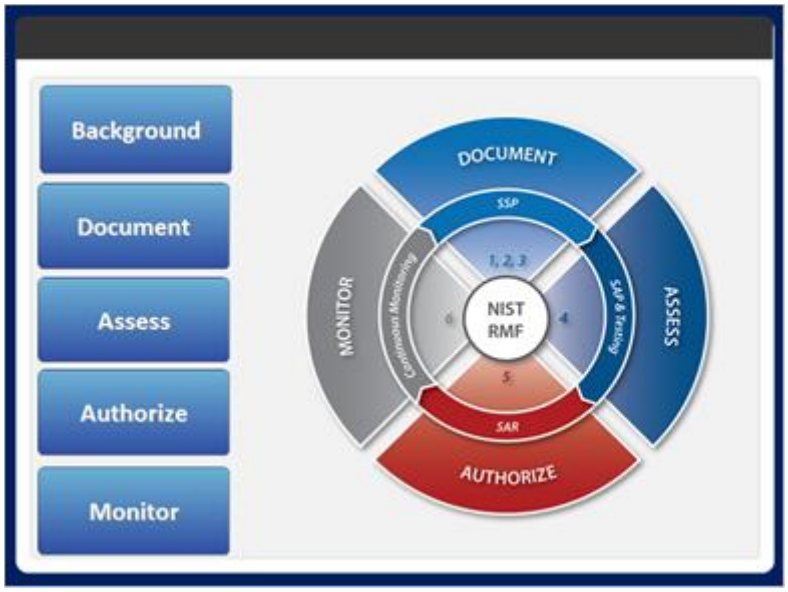
Authorize (Slide Layer)



Monitor (Slide Layer)



1.14 FedRAMP SAF/NIST RMF Comparison



Notes:

Transcript

Title

FedRAMP SAF/NIST RMF Comparison

Text

Buttons listing Background, Document, Assess, Authorize, Monitor

Image

FedRAMP SAF Process aligned to Background, Document, Assess, Authorize, Monitor

Audio

For Risk Management to succeed at all levels of the organization, the organization must have a consistent and effective approach to risk management that is applied to all risk management process and procedures. In comparing the SAF and RMF, we see how the FedRAMP methodologies are integrated and aligned to NIST. FedRAMP provides a standardized approach to a security authorization by applying the SAF across authorizations and continuous monitoring of cloud based services.

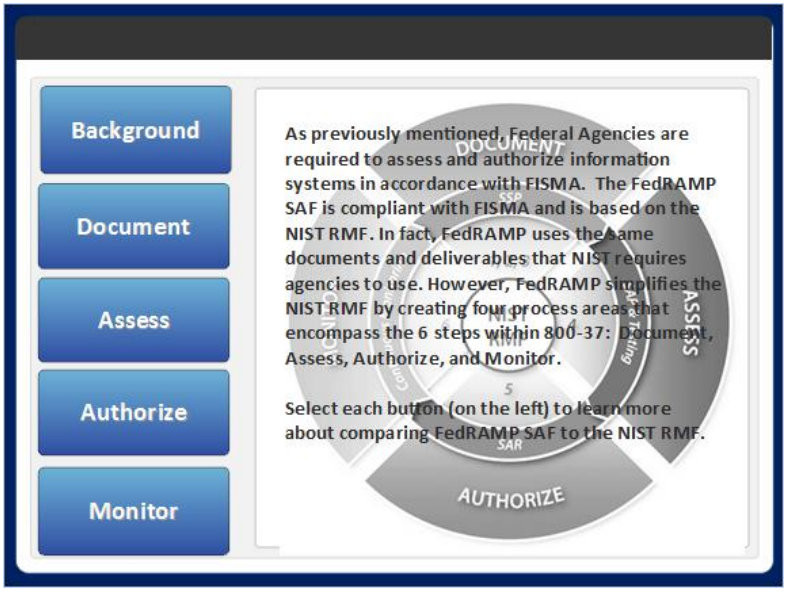
Specifically, FedRAMP looks for:

- System Categorization aligned with appropriate control baselines and impact levels
- High quality documentation of how security controls are implemented across the organization
- Assessment of security controls, by a 3PAO, to ensure that the controls are implemented correctly, operating as intended, and providing the desired outcomes
- Coordinated authorizations with either the JAB or Authorizing Agency to determine the acceptable risk levels for cloud systems

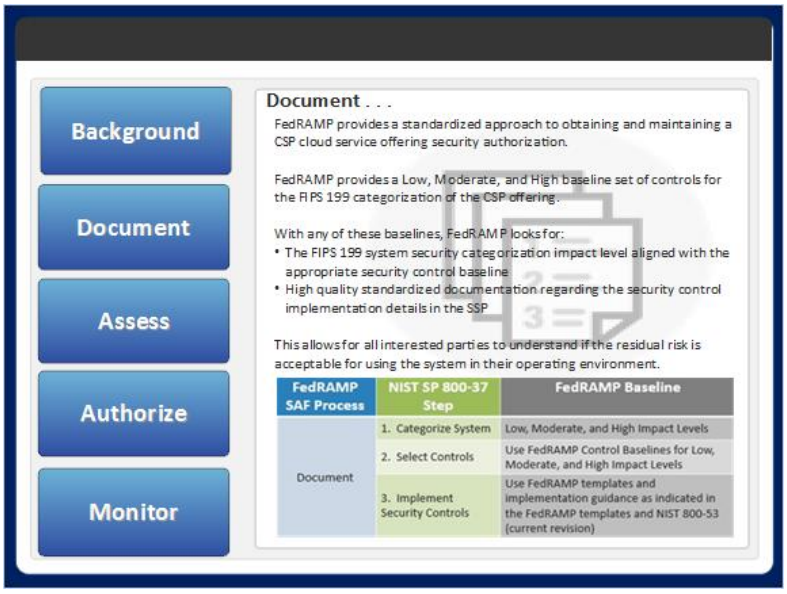
- Assurances captured in the ongoing Continuous Monitoring Strategy to improve or maintain the approved risk posture.

Select each button on the left to learn more.

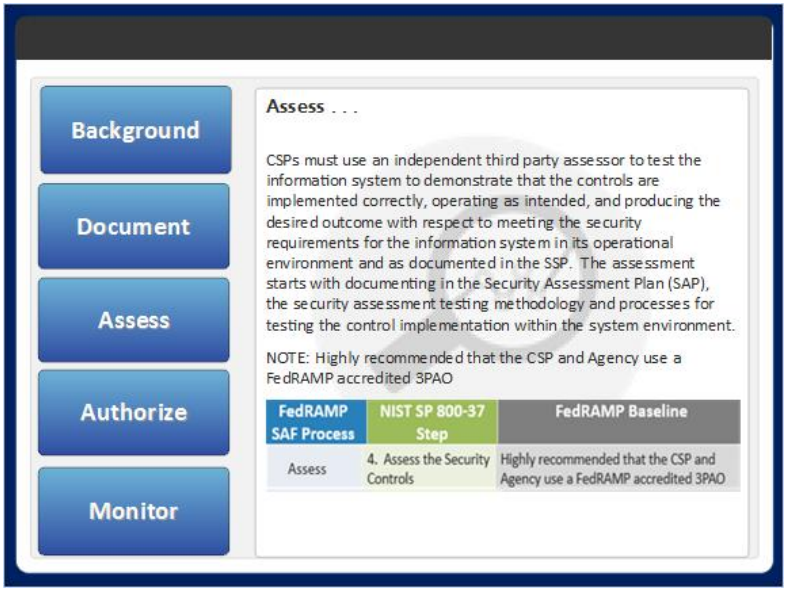
Background (Slide Layer)



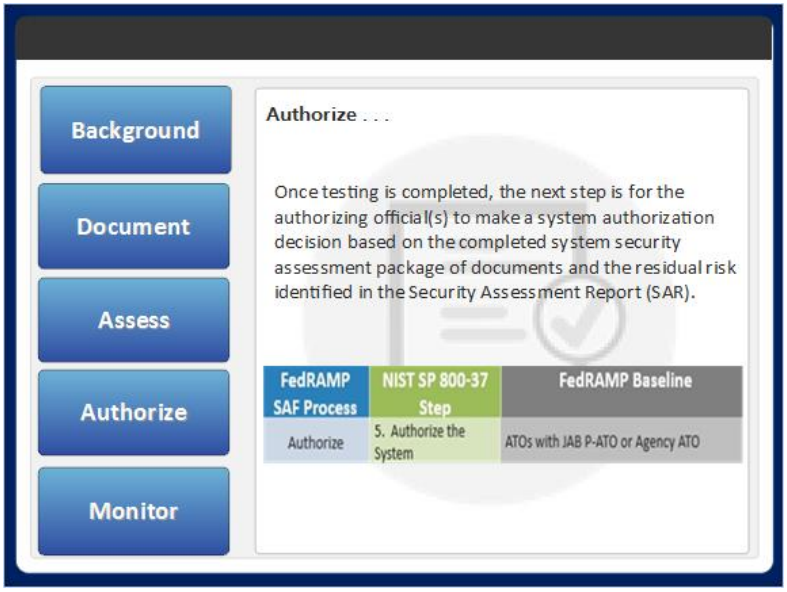
Document (Slide Layer)



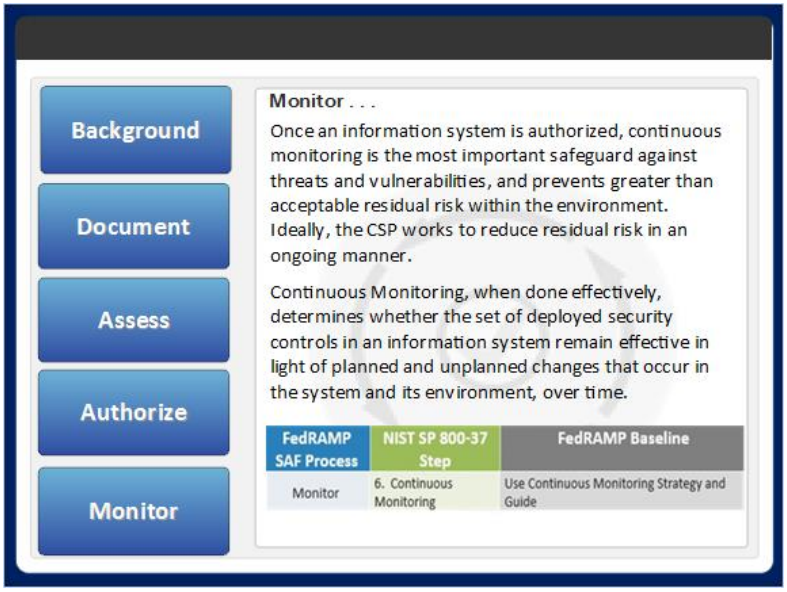
Assess (Slide Layer)



Authorize (Slide Layer)



Monitor (Slide Layer)



1.15 Knowledge Check

(True/False, 10 points, 1 attempt permitted)

Correct	Choice
X	True
	False

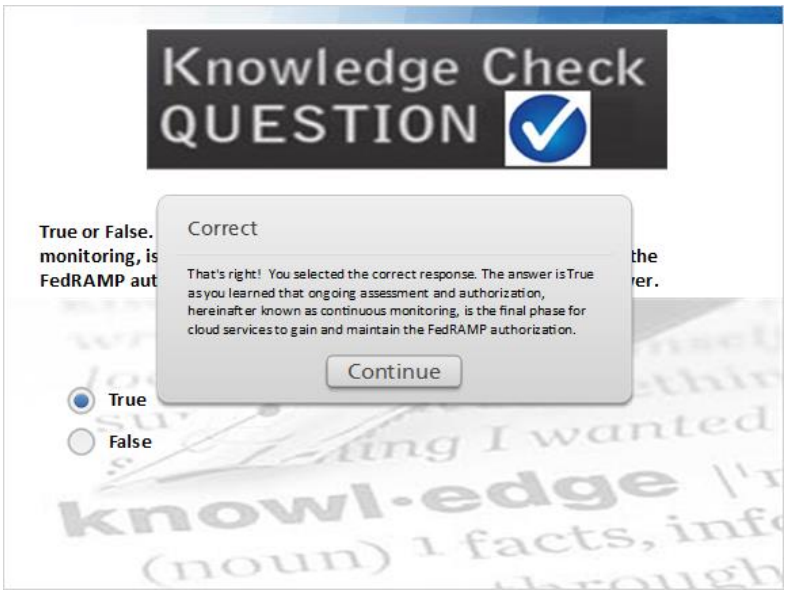
Feedback when correct:

That's right! You selected the correct response. The answer is True as you learned that ongoing assessment and authorization, hereinafter known as continuous monitoring, is the final phase for cloud services to gain and maintain the FedRAMP authorization.

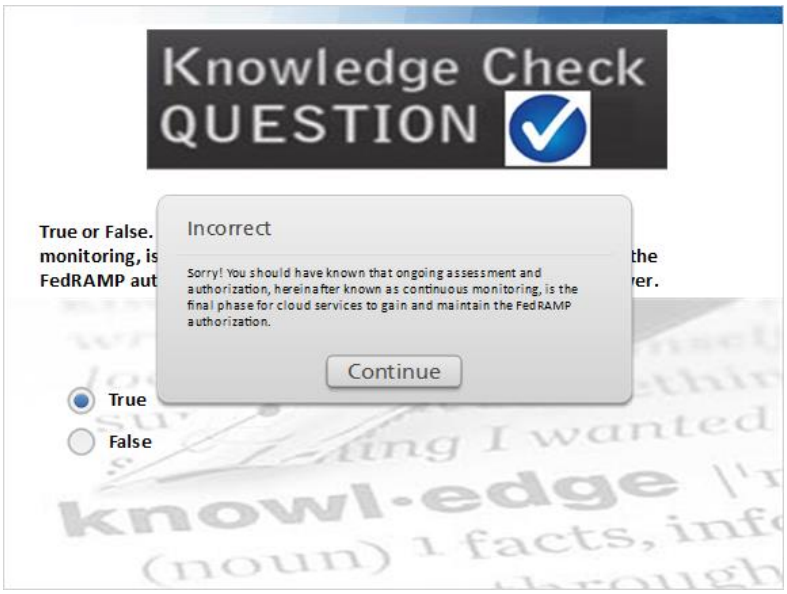
Feedback when incorrect:

Sorry! You should have known that ongoing assessment and authorization, hereinafter known as continuous monitoring, is the final phase for cloud services to gain and maintain the FedRAMP authorization.

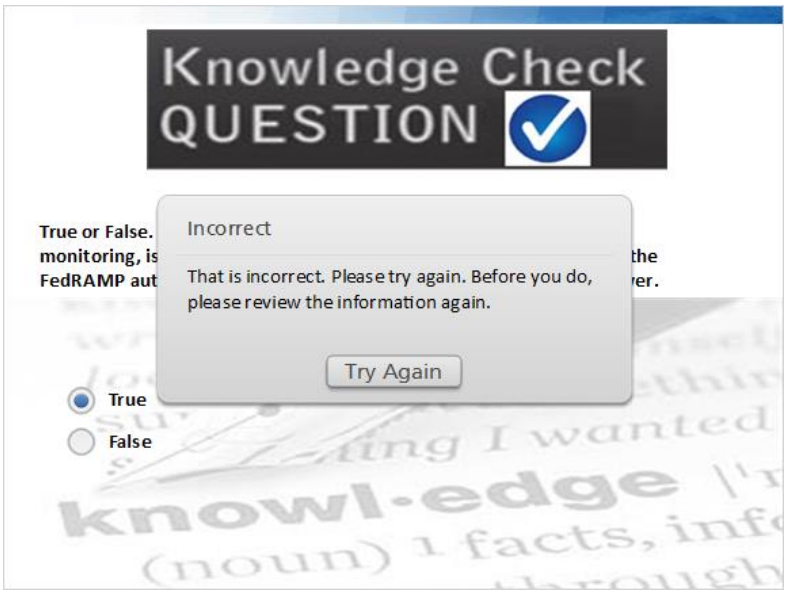
Correct (Slide Layer)



Incorrect (Slide Layer)



Try Again (Slide Layer)



1.16 FedRAMP Stakeholder Landscape

Notes:

Transcript

Title

FedRAMP Stakeholder Landscape

Text

FedRAMP is governed by a Joint Authorization Board (JAB) that acts as the primary governance and decision-making body for FedRAMP. The JAB is comprised of the Chief Information Officers from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD). NIST and OMB provide ongoing support for the FedRAMP Program. FedRAMP collaborates with other stakeholders to identify security initiatives and develop recommendations for policies, procedures, and standards. The governance of FedRAMP is comprised of different executive branch entities that work in a collaborative manner to develop, manage, and operate the program.

Joint Authorization Board (JAB):

- Defines requirements baselines
- Establishes 3PAO standards
- Authorizes a limited number of cloud services

NIST:

- Provides basic technical guidance for 3PAOs
- Establishes basic FISMA technical standards that FedRAMP builds upon

DHS:

- Monitors and reports on security incidents and provides appropriate assistance
- Updates Federal standards for FISMA reporting
- Develops continuous monitoring standards for ongoing cybersecurity

Federal CIO Council:

- Coordinates cross Agency communications

Office of Management and Budget (OMB):

- Governing body that issued the FedRAMP policy memo which defines the key requirements and capabilities of the program

GSA FedRAMP Program Management Office (PMO):

- Provides a unified process for all agencies to follow
- Works with the JAB to prioritize vendors to achieve authorizations
- Supports CSPs and agencies through the FedRAMP process

Image

Image of FedRAMP Governance map showing JAB; NIST; Federal CIO Council, GSA FedRAMP Program Management Office, and DHS

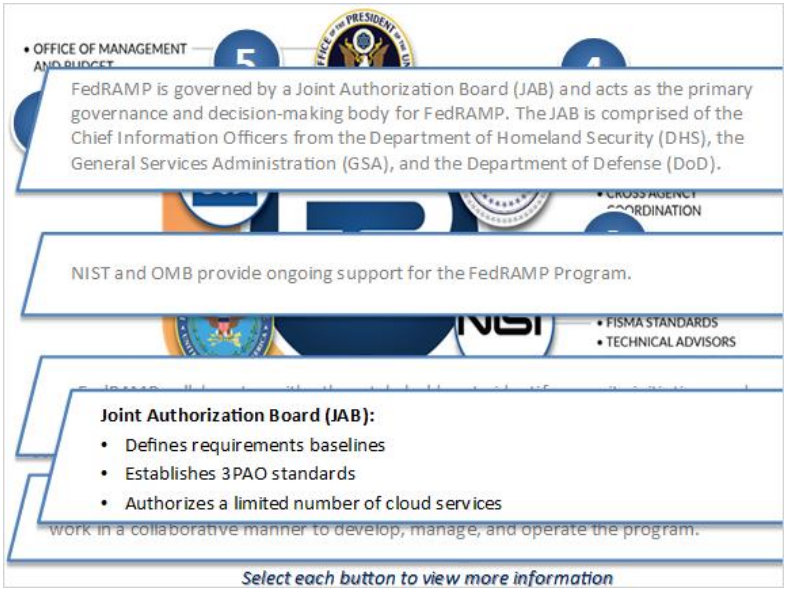
Audio

FedRAMP is governed by the Joint Authorization Board (JAB) that acts as the primary governance and decision-making body for FedRAMP. The JAB is comprised of the Chief Information Officers from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD). NIST and OMB provide ongoing support for the FedRAMP Program. FedRAMP collaborates with other stakeholders to identify security initiatives and develop recommendations for policies, procedures, and standards. The governance of FedRAMP is comprised of different executive branch entities that work in a collaborative manner to develop, manage, and operate the program.

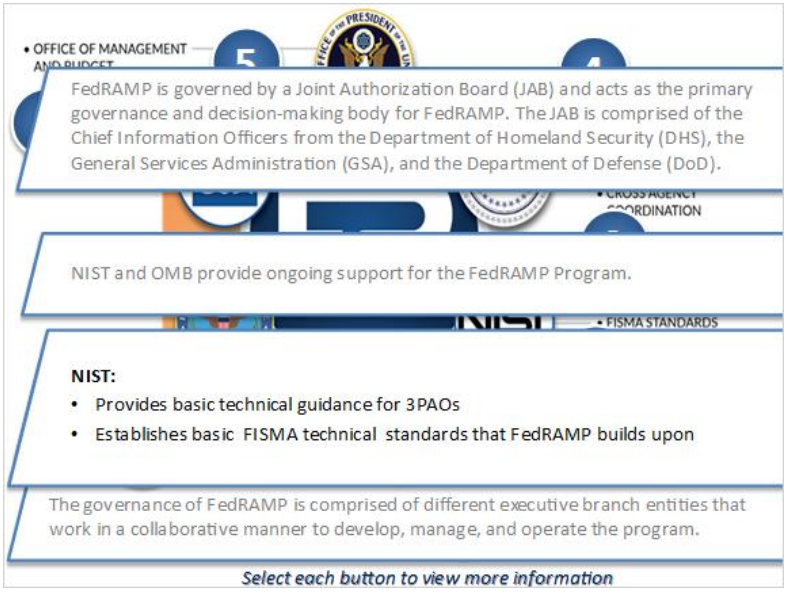
Other governing bodies of FedRAMP include:

- **National Institute for Standards and Technology (NIST):** NIST is the Federal government's leading body for the establishment of standards. As required by FISMA, NIST's security standards (SP 800-53, FIPS-199, FIPS-200, and risk management framework (SP 800-37)) serve as the foundation for FedRAMP. NIST advises FedRAMP on FISMA compliance requirements and also assists in developing standards for the accreditation of independent 3PAOs
- **Federal CIO Council:** Disseminates FedRAMP information to Federal CIOs and other representatives through cross agency communications and events
- **Department of Homeland Security (DHS):** Manages the FedRAMP continuous monitoring strategy including data feed criteria, reporting structure, threat notification coordination, and incident response
- **Office of Management and Budget Policy (OMB):** The governing body that issued the FedRAMP policy memo which defines the key requirements and capabilities of the program
- **FedRAMP Program Management Office:** Established within the GSA and responsible for the development of the FedRAMP program including the management of day-to-day operations

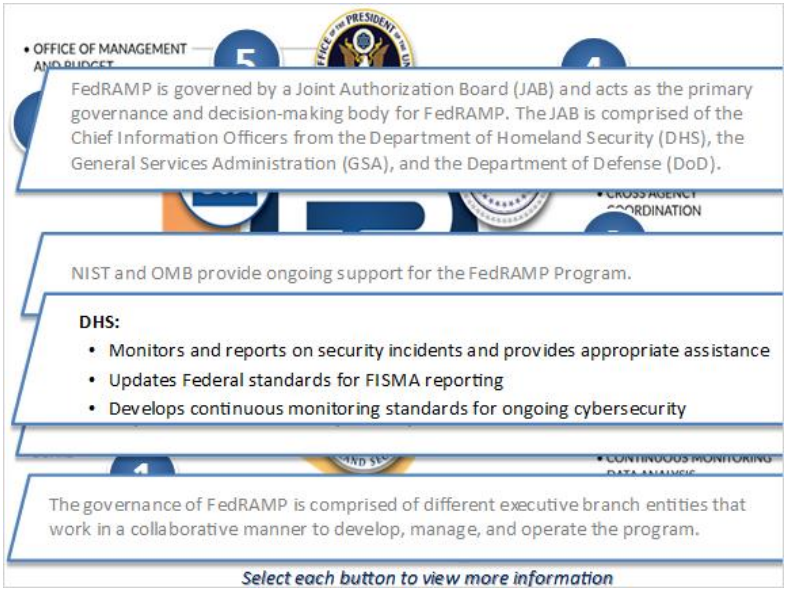
Joint Authorization Board (JAB) (Slide Layer)



NIST (Slide Layer)



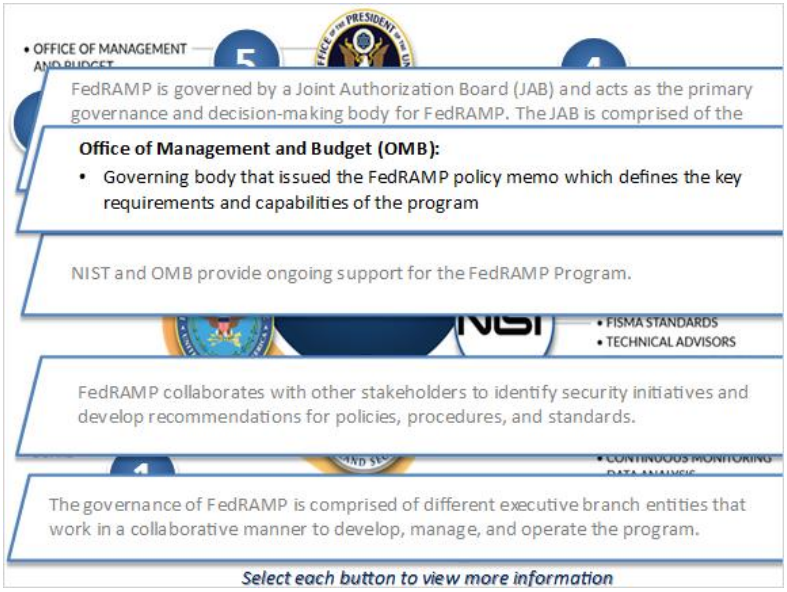
DHS (Slide Layer)



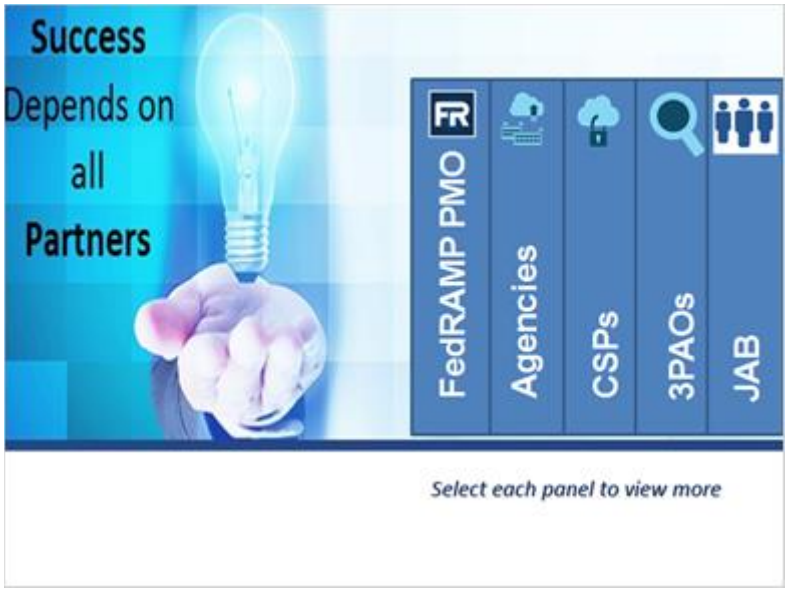
Federal CIO Council (Slide Layer)

GSA FedRAMP PMO (Slide Layer)

Office of Management and Budget (OMB) (Slide Layer)



1.17 Partnerships



Notes:

Transcript

Title

Success Depends on all Partners

Text

1. FedRAMP PMO:
- Provides a standardized process for all agencies to follow
- Works with the JAB for prioritized vendors to achieve authorizations with an efficient review schedule
- Supports CSPs and agencies through the authorization process - regardless of which path they choose
- Maintains a secure repository of FedRAMP ATOs to enable authorization reuse

2. Agencies:
- Integrate the FedRAMP requirements into agency specific policies/procedures
- Contract with CSPs
- Authorize cloud services following FedRAMP requirements

3. CSPs:
- Contract with the 3PAOs to perform consulting and assessment activities
- Provide secure cloud services to the Federal Government
- Maintain a sound security posture in adherence with NIST/FedRAMP requirements

4. 3PAOs:
- Contract in good faith with the CSPs to provide consulting and assessment activities
- Maintain independence from CSPs - in accordance with International Standards Organization (ISO) standards
- Provide consulting and assessment services for CSP environments according the FedRAMP requirements

5. JAB:

- Defines FedRAMP requirements baselines
- Establishes FedRAMP standards for all stakeholders
- Authorizes a limited number of cloud services

Image

Image of FedRAMP PMO; Agencies; CSPs; 3PAOs; JAB tabs

Audio

When we look at the FedRAMP Partnerships with both industry and agencies, we see that the success of this program is dependent on strong relationships.

The day-to day-operations of FedRAMP is coordinated through the PMO at GSA. The PMO provides a standardized process for all agencies to follow and works closely with the JAB for prioritized vendors to achieve authorizations.

The PMO supports CSPs and agencies through the authorization process - regardless of which path they go, and maintains the secure repository of FedRAMP ATOs to enable authorization reuse.

Agencies are responsible for:

- Integrating the FedRAMP requirements into agency specific policies/procedures
- Contracting with CSPs
- Authorizing cloud services following FedRAMP requirements

A CSP can be a commercial or government entity that has a cloud offering or service saleable to the federal government and that will transmit or store federal data and information via the "Cloud". The CSP is responsible for:

- Contracting with the 3PAOs who then perform consulting and assessment activities
- Providing secure cloud services to the federal government
- Maintaining a sound security posture in adherence to NIST/FedRAMP requirements

The CSP is also responsible for:

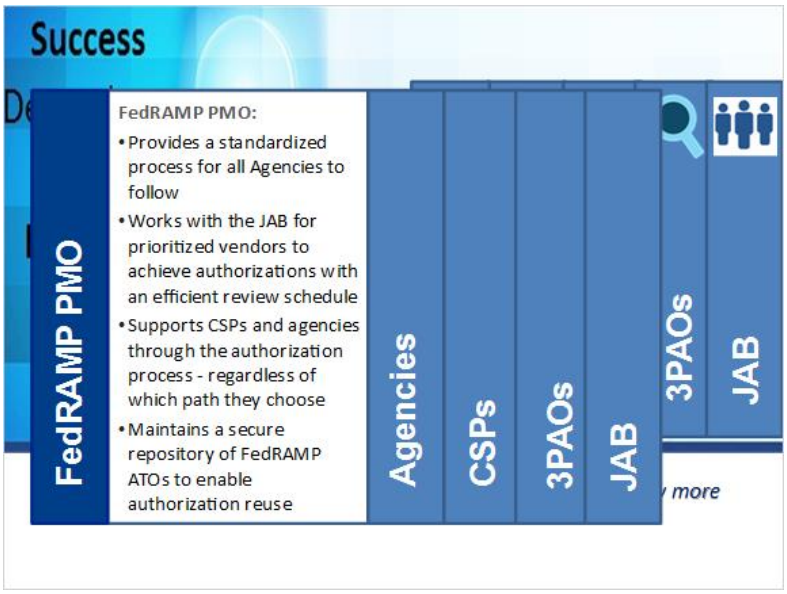
- Submitting quality documentation in support of their FedRAMP application,
- Implementing FedRAMP security controls,
- Working closely with an independent third party assessor to perform initial and annual assessments, and,
- Maintaining its authorization by complying with continuous monitoring requirements.

3PAOs are independent entities that perform initial and periodic security assessments of cloud systems.

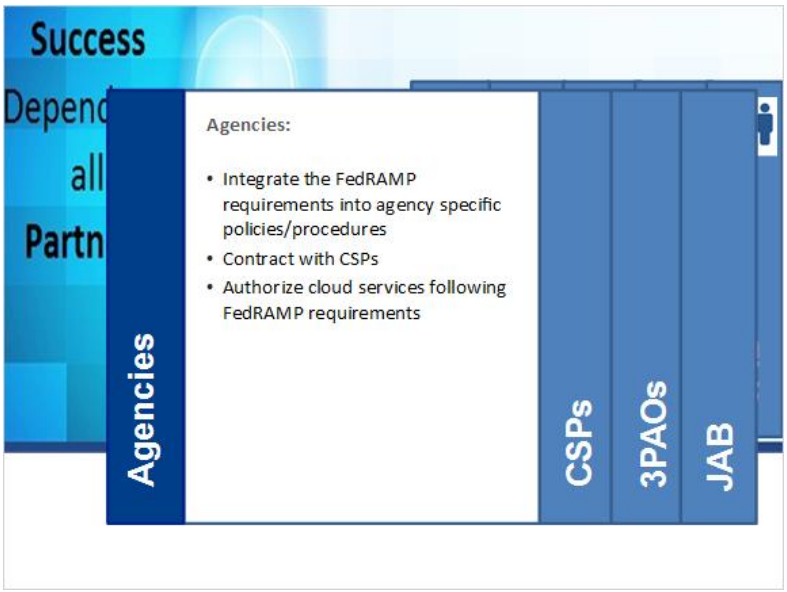
1. The 3PAOs contract in good faith with the CSPs to provide consulting and assessment activities
2. The 3PAOs assess the CSPs security control implementation, and generate Security Assessment Reports and associated evidence of test results
3. The independence of the 3PAOs plays a critical role in the FedRAMP security assessment process. The independent 3PAOs verify cloud providers' security implementations and provide the overall risk posture of a cloud environment for a security authorization decision. 3PAOS:
    - Must be independent of CSPs - in accordance with ISO standards, and
    - Provide consulting and assessment services of CSP environments according the FedRAMP requirements.

The JAB defines requirements baselines; establishes 3PAO standards for all stakeholders; and authorizes a limited number of cloud services based upon a prioritization process.

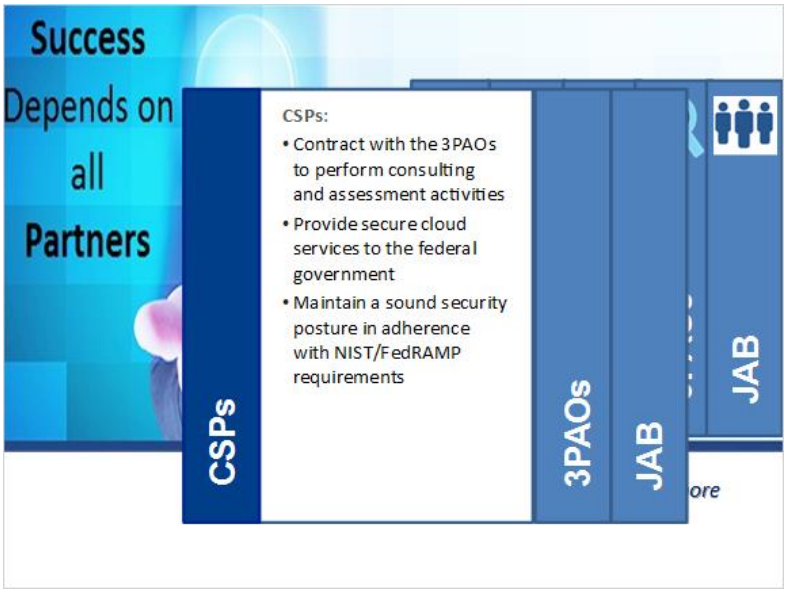
FedRAMP PMO (Slide Layer)



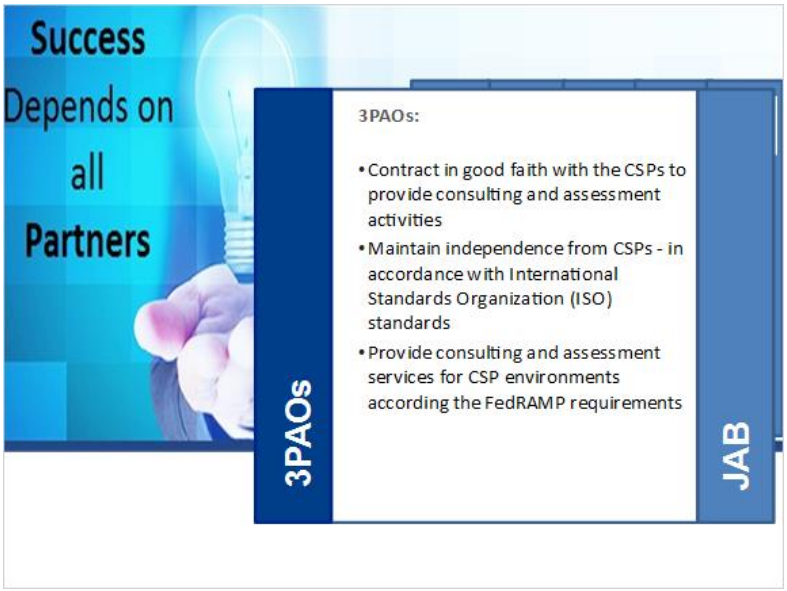
Agencies (Slide Layer)



CSPs (Slide Layer)



3PAOS (Slide Layer)



JAB (Slide Layer)

1.18 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)

Correct	Choice
X	Maintain independence when performing quality risk assessments
	Integrate FedRAMP requirements into Agency specific policies/procedures
	Encourage customers to reuse existing ATOs for their products
	Conduct single-use quality risk assessments

Feedback when correct:

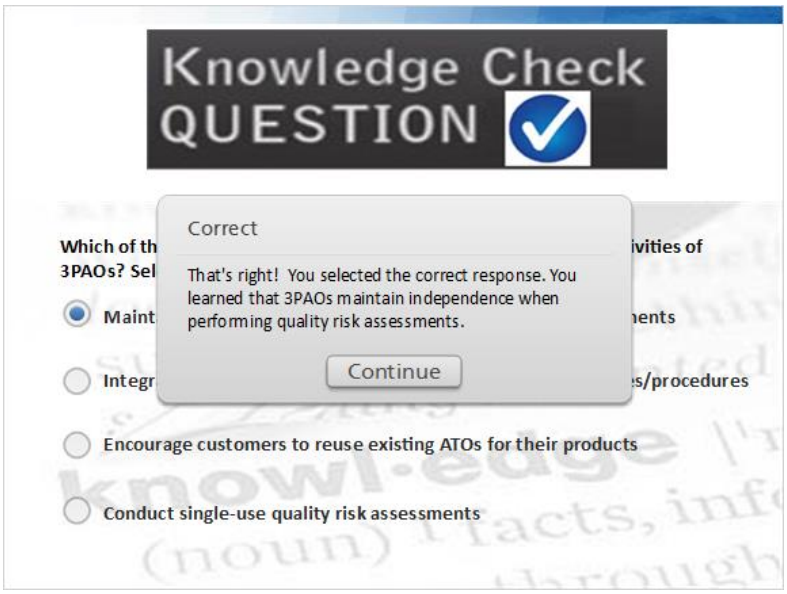
That's right! You selected the correct response. You learned that 3PAOs maintain independence when performing quality risk assessments.

Feedback when incorrect:

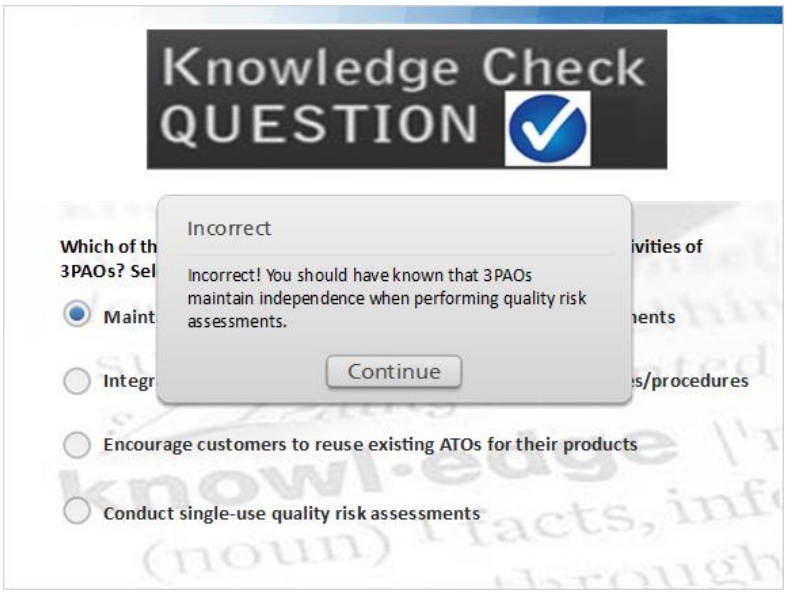
Incorrect! You should have known that 3PAOs maintain independence when performing quality risk assessments.

Notes:

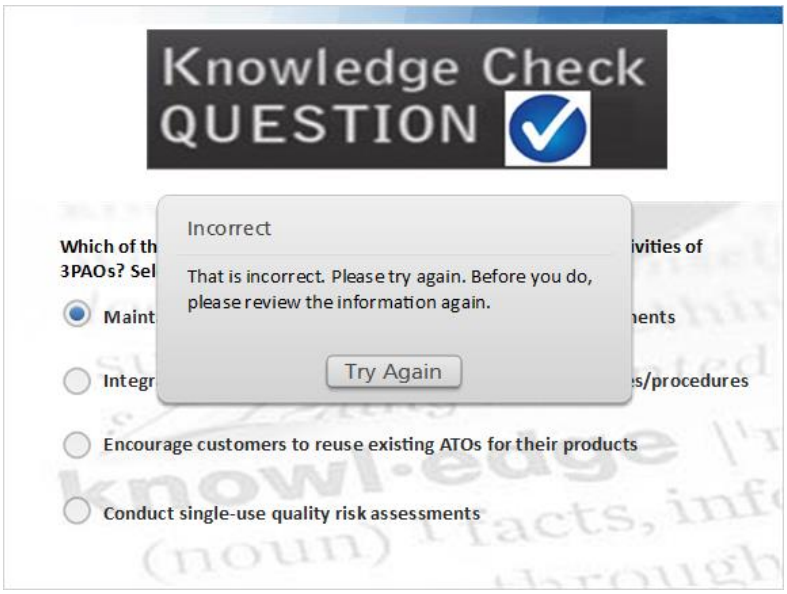
Correct (Slide Layer)



Incorrect (Slide Layer)

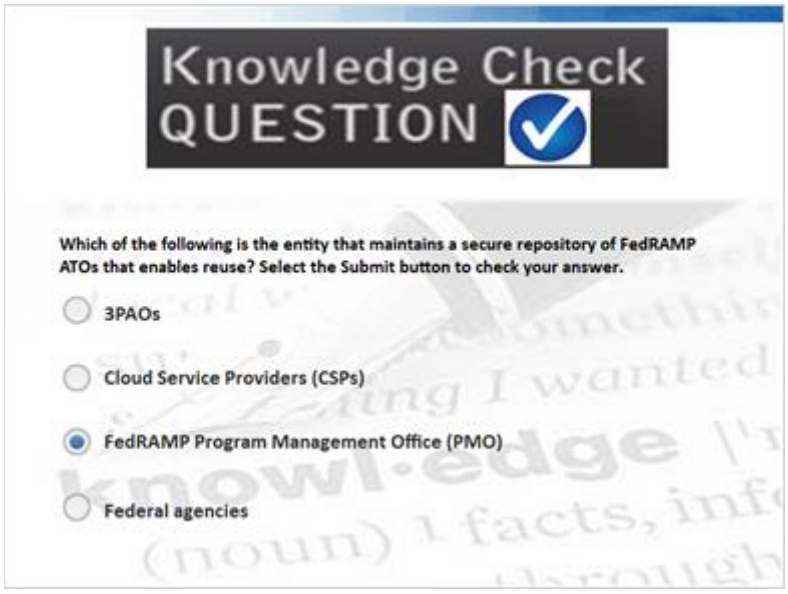


Try Again (Slide Layer)



1.19 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)



Correct	Choice
	3PAOs
	Cloud Service Providers (CSPs)
X	FedRAMP Program Management Office (PMO)
	Federal agencies

Feedback when correct:

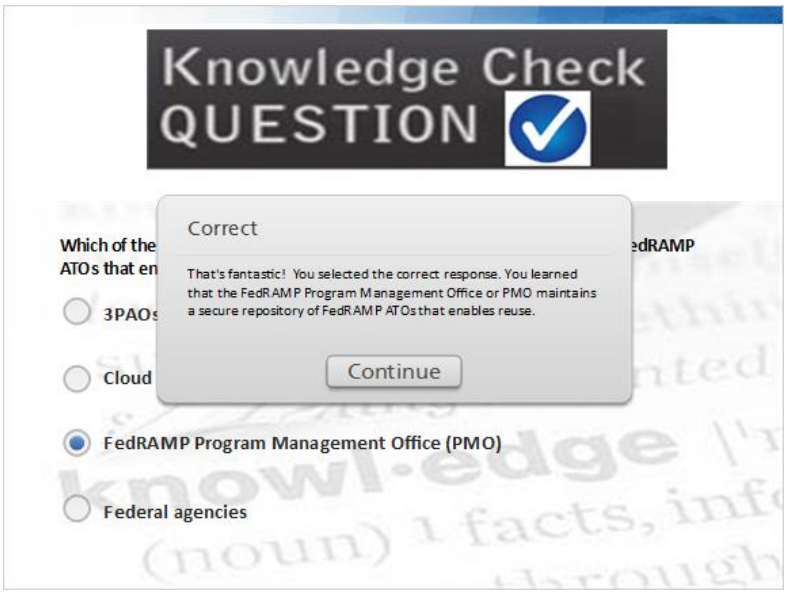
That's fantastic! You selected the correct response. You learned that the FedRAMP Program Management Office or PMO maintains a secure repository of FedRAMP ATOs that enables reuse.

Feedback when incorrect:

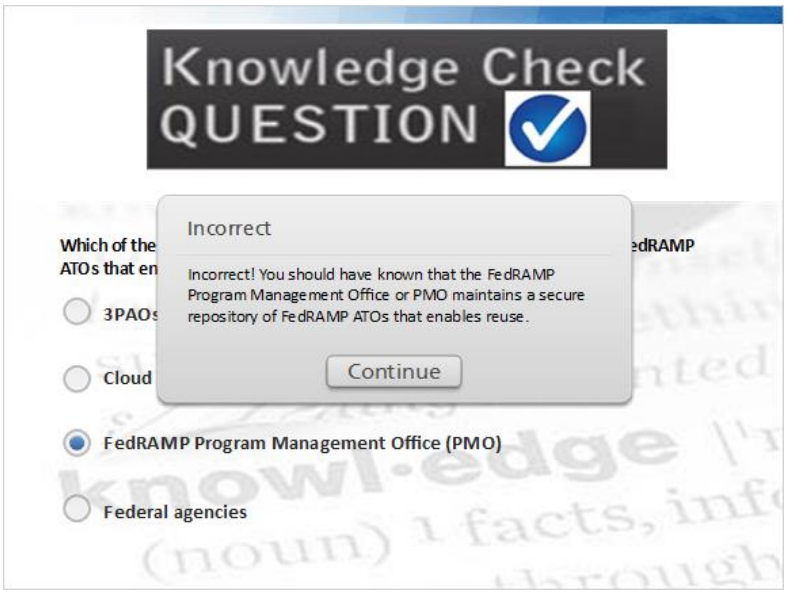
Incorrect! You should have known that the FedRAMP Program Management Office or PMO maintains a secure repository of FedRAMP ATOs that enables reuse.

Notes:

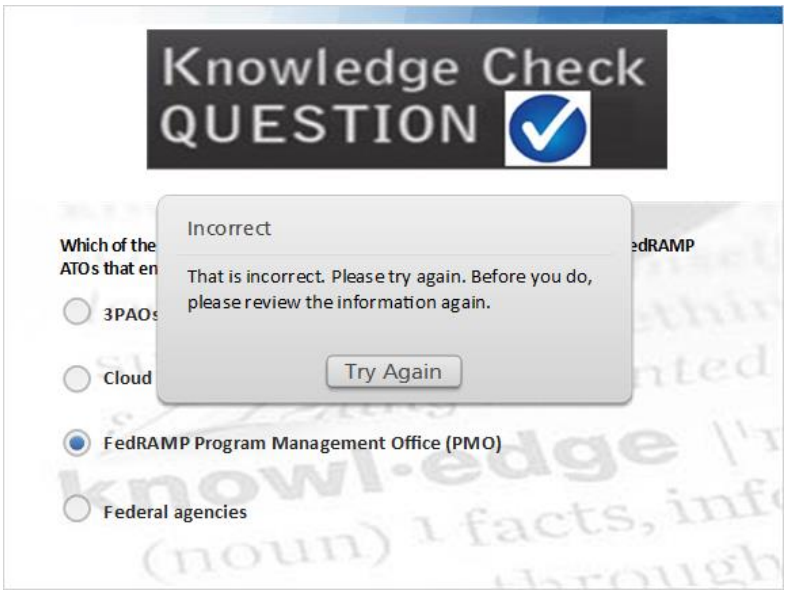
Correct (Slide Layer)



Incorrect (Slide Layer)



Try Again (Slide Layer)



1.20 FedRAMP Authorization Paths

Notes:

Transcript

Title

FedRAMP Training - Welcome to FedRAMP

FedRAMP Authorization Paths

Text

JAB Provisional Authorization to Operate (P-ATO):

- DHS, DoD, and GSA reviewers analyze CSP security assessment packages to determine if the cloud service offering provides an acceptable security posture for system use within the Federal government
- A FedRAMP P-ATO is an initial approval of the CSP authorization package by the JAB that an executive department or agency can leverage to grant a security authorization and an accompanying ATO for the acquisition and use of the cloud service within their agency.

Agency Authorization to Operate (ATO):

1. Initial:

- CSP submits the security assessment package documentation to an agency
- Agency reviews the CSP security assessment package to ensure that the security posture is acceptable for use within the agency
- Agency partners with the CSP and issues the Agency Authorization
- Agency submits the complete package to the FedRAMP PMO so that the package can be reused by other agencies

2. Reuse:

- Agency requests access to secure repository to view package for reuse
- Agency makes an authorization decision
- Agency grants authorization letter and submits letter to be uploaded to secure repository
- All agencies forming a partnership with the CSP should collaborate to manage the CSP continuous monitoring
-

Image

Image showing JAB Provisional Authorization to Operate (P-ATO); Agency Authorization to Operate (ATO)

Audio

Next, we will discuss the two potential paths for a CSP to obtain FedRAMP Authorization. FedRAMP streamlines the federal agencies' ability to make use of cloud services. FedRAMP accomplishes this by providing two paths for a CSP to obtain an authorization. It is important to understand that packages must go through either of these paths to be re-used by a Federal Agency.

The JAB consists of a group of CIOs from the DoD, the DHS, and the GSA and is the primary governance and decision making body for FedRAMP. For the JAB P-ATO, JAB reviewers conduct a rigorous technical review of each CSP package to ensure that the CSP meets all controls, as defined by NIST 800-53 (current revision), and present an acceptable security posture for use across the federal government.

CSPs that opt to apply for a JAB P-ATO are required to go through the FedRAMP review and approval process and submit appropriate documentation, in a timely manner to the FedRAMP PMO. The key benefit for a CSP achieving a JAB P-ATO is that the rigor of the JAB review gives Agencies a very high confidence that the package does not present any unidentified or unanticipated risks.

Currently, FedRAMP has three CSP designations on the FedRAMP Marketplace:
1.) "FedRAMP Ready Products" means that a CSP, through the attestation of a FedRAMP certified 3PAO, has submitted a Readiness Assessment Report (RAR) to the FedRAMP PMO. If the package is within the acceptable FedRAMP compliance limits, the CSP package is posted to the FedRAMP secure repository and the CSP is listed on the Marketplace as being "FedRAMP Ready".

2.) "FedRAMP In Process Products" are CSP cloud service offerings that have a partnering agency and are proceeding with the agency authorization.
3.) "FedRAMP Authorized Products" have received the initial Agency Authorization to Operate and have also been reviewed and deemed compliant by the FedRAMP PMO.

Once a CSP cloud service offering is "FedRAMP Authorized", the offering is ready to be re-used by other agencies. First, the agencies will need to conduct a review process of the CSP package located in the FedRAMP secure repository to determine whether the package presents an acceptable level of risk to the agency. In accordance with FISMA, only the head of an agency or his appointed designee, the Authorizing Official, can make a risk-based determination to use IT systems. All agencies using a cloud offering share responsibility for the continuous monitoring of the system.

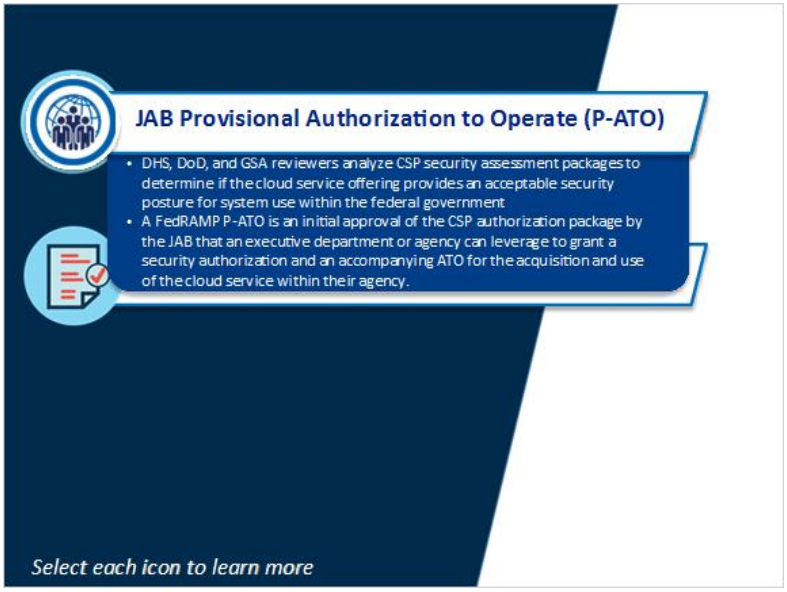
FedRAMP's primary goal is to bring as many secure, multi-tenant, and unique cloud tools to the FedRAMP Marketplace <https://marketplace.fedramp.gov/index.html>. Both JAB and initial agency authorizations must pass a security assessment based upon a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls. This means JAB and agency authorizations are secure and compliant for use with federal data and information. Currently, FedRAMP classifies authorizations based on "necessary" and "unique".

A "necessary" cloud system that is multi-tenant in nature and has a broad use case of capabilities is exactly the kind of cloud that should pursue JAB authorization. The JAB reviews clouds that can and are being used government-wide. So, if a CSP is considering JAB authorization, they should definitely take into consideration the amount of federal interest in their service and the depth of use cases across the government.

If only one or two agencies are interested in a CSP's cloud product or the cloud was designed specifically for a particular agency, then a "unique" agency authorization is a better fit. Agency authorizations are targeted for niche cloud services that may only be used by a singular agency. Clouds that are unique to a particular agency provide a great benefit to that agency, but is not a good option for JAB authorization.

The decision to pursue JAB or agency authorization depends on if the cloud is multi-tenant and has broad use across many agencies or if it is unique to a few. While there are two routes to authorization, the end goal of JAB and agency authorizations are the same - increasing the amount of secure and diverse cloud products that are available to the federal government.

JAB Provisional Authorization to Operate (P-ATO) (Slide Layer)



Agency Authorization to Operate (ATO) (Slide Layer)

1.21 FedRAMP Authorization Requirements

Notes:

Transcript

Title

FedRAMP Authorization Requirements

Text
A cloud system is authorized with FedRAMP if it meets the following requirements:

Slide text 1: The system security package has been created using the required FedRAMP templates

Slide text 2: The system meets the FedRAMP security control requirements

Slide text 3: The system has been assessed by an independent assessor (3PAO or Agency designated assessor). The agency package is validated by the PMO. The P-ATO package is reviewed and validated by the JAB.

Slide text 4: A Provisional Authorization, and/or an Agency ATO, has been granted for the system
Slide text 5: An agency authorization letter for the system is on file with the GSA FedRAMP Program Management Office (PMO)
Slide text 6: The CSP and agency maintain the continuous monitoring requirements of FedRAMP

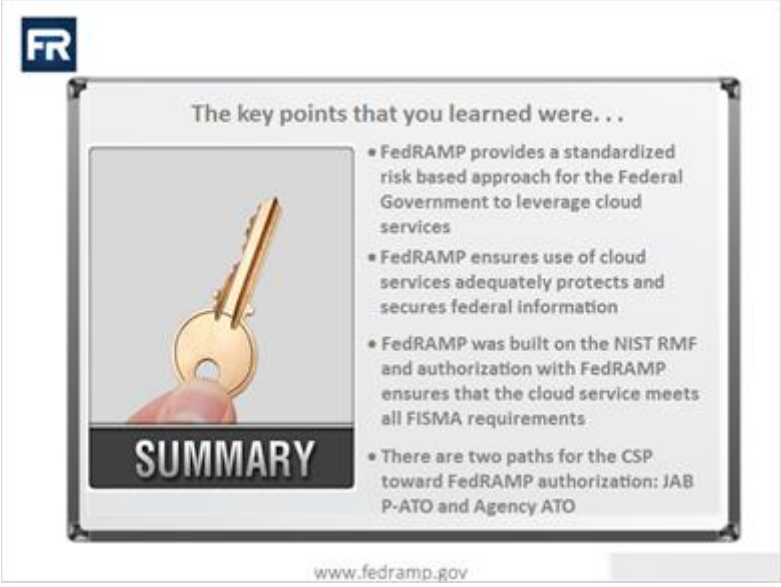
Image
A sliding image showing six different requirements:
1. The system security package has been created using the required FedRAMP templates
2. The system meets the FedRAMP security control requirements
3. The system has been assessed by an independent assessor (3PAO or Agency designated assessor). The agency package is validated by the PMO. The P-ATO package is reviewed and validated by the JAB
4. A Provisional Authorization, and/or an Agency ATO, has been granted for the system
5. An agency authorization letter for the system is on file with the GSA PMO
6. The CSP and agency maintain the continuous monitoring requirements of FedRAMP

Au**dio**
FedRAMP Authorized is a designation for cloud systems that demonstrate the following requirements:

1. The system security package has been created using the required FedRAMP templates;
2. The system meets the FedRAMP security control requirements
3. The system has been assessed by an independent assessor (3PAO or agency designated assessor) and the agency package is validated by the PMO. The P-ATO package is reviewed and validated by the JAB.

A CSP must obtain either:
4. A Provisional Authorization from the JAB;
An Agency ATO that meets FedRAMP Security Assessment Authorization Package standards;
5. An authorization letter for the system is on file with the GSA FedRAMP Program Management Office (PMO)
6. And, the CSP and agency maintain the continuous monitoring requirements of FedRAMP

1.22 Summary



Notes:

Transcript

Title

Summary

Text
The key points you learned were . . .
- FedRAMP provides a standardized risk based approach for the Federal Government to leverage cloud services.
- FedRAMP ensures use of cloud services adequately protects and secures federal information.
- FedRAMP is built upon the NIST RMF and authorization with FedRAMP ensures that the cloud service meets all FISMA

requirements
- There are two paths for the CSP towards FedRAMP authorization: JAB P-ATO and Agency ATO

Image

Gold key with the word, SUMMARY, on the lower portion

Audio

We have come to the conclusion of this course. The key points that you learned were. . .

- FedRAMP provides a standardized risk based approach for the Federal Government to leverage cloud services
- FedRAMP accelerates the adoption of secure cloud solutions through reuse of assessments and authorizations
- FedRAMP was built on the NIST RMF and authorization with FedRAMP ensures that the cloud service meets all FISMA requirements
- There are two paths for the CSP toward FedRAMP authorization: JAB P-ATO and Agency ATO

1.23 What's Next?

Notes:

Transcript

Title

What's Next?

Text

FedRAMP Training - Welcome to FedRAMP

You've now completed this course and are now eligible to enroll in other available courses. Please visit the GSA Blackboard Learn Portal for more information or for additional information on FedRAMP Training, send us an email to info@fedramp.gov.

Image

Image of FedRAMP logo.

Audio

You've now completed this course and are now eligible to enroll in other available courses. Please visit the GSA Blackboard Learn Portal for more information or contact us at http://gsa.gov/FedRAMP.

For more information, please contact us or visit us at any of the following websites:

http://FedRAMP.gov

http://gsa.gov/FedRAMP

@FederalCloud