

FedRAMP Training - How to Write a Control

1. FedRAMP_Training_HTWAC_v5_508

1.1 FedRAMP HTWAC Online Training Splash Screen



Notes:

Transcript

Title:

How to Write a Control

Image

Image of FedRAMP logo.

Text

FedRAMP Online Training; How to Write a Control. Presented by: FedRAMP PMO.

Select the Next button to begin.

1.2 Course Navigation



Notes:

Transcript

Title

Course Features and Functions

Text

<N/A>

Image

Screen capture of the course including the FedRAMP logo, Description 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 Description 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.

When you are finished, click the Next arrow to continue.

Menu (Slide Layer)

Menu tab: Displays a list of the course screens you may click to view.

Image: Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Closed Captions Course Audio Script: To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes** tab in the upper-left hand corner of the slide.

FedRAMP
Federal Risk and Authorization Management Program

FedRAMP Online Training
Security Assessment Plan (SAP) Overview
12/9/2015
Presented by: FedRAMP PMO

Navigation buttons: < BACK, NEXT >, < PREV, NEXT >

Transcript (Slide Layer)

Transcript tab: Click to see the Audio Transcript.

Transcript
Title
Review of the Security Assessment Report (SAR) Tables
Text <N/A>

Image: Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.

Closed Captions Course Audio Script: To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes** tab in the upper-left hand corner of the slide.

FedRAMP
Federal Risk and Authorization Management Program

FedRAMP Online Training
Security Assessment Plan (SAP) Overview
12/9/2015
Presented by: FedRAMP PMO

Navigation buttons: < BACK, NEXT >, < PREV, NEXT >

Resources (Slide Layer)

The screenshot shows a slide from a FedRAMP training course. On the left is a sidebar with a 'Transcript' section containing text about SAR Tables, FedRAMP logs, and closed captions. The main slide area features the FedRAMP logo (a circle with 'FR' and 'FedRAMP Federal Risk and Authorization Management Program') and the title 'FedRAMP Online Training Security Assessment Plan (SAP) Overview'. A callout box points to a 'Resources' button in the top right corner, with the text: 'Resources button: Click to view files available to view and/or print for this course.' At the bottom, there are navigation controls including a play/pause button, a progress bar, and 'PREV' and 'NEXT' buttons.

Play/Pause (Slide Layer)

This screenshot is identical to the one above, but the callout box now points to the play/pause button in the bottom navigation bar. The callout text reads: 'Play/Pause button: Click to play or pause the course.'

Replay (Slide Layer)



The screenshot shows a training slide titled "FedRAMP Online Training Security Assessment Plan (SAP) Overview". The slide features the FedRAMP logo (a blue square with "FR" inside a circle) and the text "Federal Risk and Authorization Management Program". Below the logo, it says "FedRAMP Online Training Security Assessment Plan (SAP) Overview" and "Presented by: FedRAMP PMO". A dark blue box with white text is overlaid on the slide, pointing to a circular "Replay" button in the bottom navigation bar. The text in the box reads: "Replay button: Click to replay the screen." The left sidebar contains a "Transcript" section with the following text: "Title: Review of the Security Assessment Report (SAR) Tables", "Text <N/A>", "Image: Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.", and "Closed Captions Course Audio Script: To view Closed Captions of the Security Assessment Report (SAR) Tables, select the Notes tab in the upper-left hand corner of the slide." The bottom navigation bar includes buttons for "PREV" and "NEXT", and a "Replay" button.

Back/Next (Slide Layer)



This screenshot is identical to the one above, showing the same FedRAMP training slide. However, a dark blue box with white text is overlaid on the slide, pointing to the "Back" and "Next" buttons in the bottom navigation bar. The text in the box reads: "Back/Next arrows: Click to return to previous screen or continue to the next screen." The "Back" and "Next" buttons in the navigation bar are highlighted with a yellow border.

Volume Control (Slide Layer)



The screenshot shows a training slide with a blue header and footer. The main content area is white and features the FedRAMP logo (a blue square with 'FR' in white) inside a black circle. Below the logo, the text reads 'FedRAMP Online Training' and 'Security Assessment Plan (SAP) Overview'. A date '12/9/2015' and 'Presented by: FedRAMP PMO' are also visible. On the left side, there is a 'Transcript' panel with a 'Notes' tab selected. A dark blue callout box with white text says 'Volume Control: Use your mouse button to adjust the volume of audio.' The bottom of the slide has navigation buttons: 'PREV' and 'NEXT' on the left, and 'BACK' and 'NEXT' on the right.

Transcript
Title
Review of the Security Assessment Report (SAR) Tables
Text -N/A-
Image
Screen capture of the course including the FedRAMP logo, Description and Menu tabs, navigation buttons, and Resources button.
Closed Captions Course Audio Script. To view Closed Captions of the Security Assessment Report (SAR) Tables, select the **Notes** tab in the upper-left hand corner of the slide.

Volume Control: Use your mouse button to adjust the volume of audio.

FedRAMP Online Training
Security Assessment Plan (SAP) Overview
12/9/2015
Presented by: FedRAMP PMO

1.3 Today's Training



The screenshot shows a slide with a blue header containing the FedRAMP logo and the title 'Today's Training'. The main content area is white and contains a bulleted list of training topics. The fifth item, 'How to Write to a Control - 201B', is highlighted with a grey background. The footer of the slide contains the website 'www.fedramp.gov' and 'PAGE | 3'.

Today's Training

- Welcome to Part Six of the FedRAMP Training Series:
 1. Introduction to the Federal Risk and Authorization Program (FedRAMP) – 100A
 2. FedRAMP System Security Plan (SSP) Required Documents – 200A
 3. Security Assessment Plan (SAP) Overview – 200B
 4. Security Assessment Report (SAR) Overview – 200C
 - 5. How to Write to a Control – 201B**
 6. Continuous Monitoring Overview – 200D
- This course aims to assist CSPs in writing compliant control implementation descriptions in the SSP.

www.fedramp.gov PAGE | 3

Notes:

Transcript Title

Today's Training

Image

Video covering Today's Training

Text

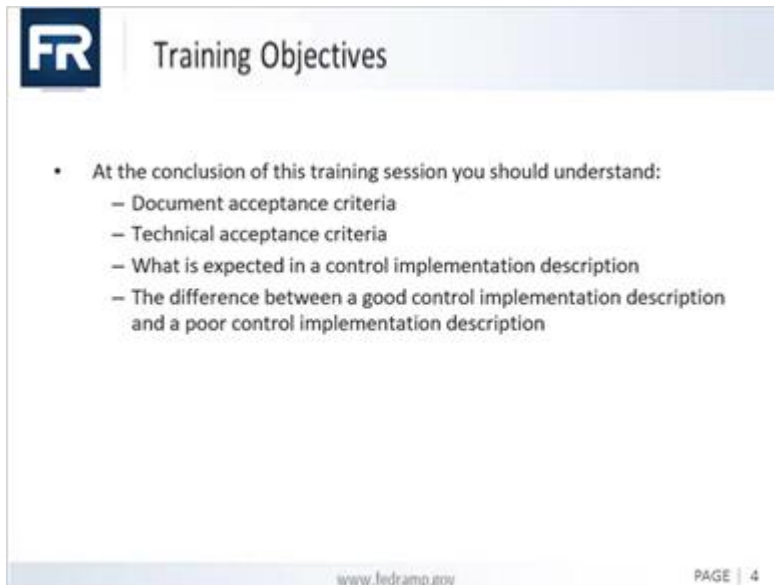
Welcome to Part Four of the FedRAMP Training Series:

1. Introduction to the Federal Risk and Authorization Program (FedRAMP) - 100A
2. FedRAMP System Security Plan (SSP) Required Documents - 200A
3. Security Assessment Plan (SAP) Overview - 200B
4. Security Assessment Report (SAR) Overview - 200C
- 5. How to Write a Control - 201B**
6. Continuous Monitoring (ConMon) Overview - 200D

Audio

Welcome to the FedRAMP online training series. I am <name> your instructor for this training. In this course, we're going to talk about how to write a control. The FedRAMP PMO developed this training series to help FedRAMP CSP applicants properly prepare for a FedRAMP assessment by providing a detailed understanding of the program and the level of effort required to satisfactorily complete a FedRAMP assessment. This training module is tailored to a CSP that is documenting the security of the Cloud System and will assist with writing compliant control implementation descriptions in the System Security Plan or SSP. By providing insight into what to expect when going through the FedRAMP assessment process, we want to ensure CSPs have the knowledge and resources to successfully achieve FedRAMP authorization.

1.4 Training Objectives

A slide titled "Training Objectives" with the FedRAMP logo (FR) in the top left corner. The slide lists the following objectives:

- At the conclusion of this training session you should understand:
 - Document acceptance criteria
 - Technical acceptance criteria
 - What is expected in a control implementation description
 - The difference between a good control implementation description and a poor control implementation description

The slide footer contains the website address "www.fedramp.gov" and the page number "PAGE | 4".

Notes:

Transcript Title

Training Objectives

Image

Video covering Training Objectives

At the conclusion of this training session, you should understand:

- Document acceptance criteria
- Technical acceptance criteria
- What is expected in a control implementation description
- The difference between a good control implementation and a poor control implementation

Text

At the conclusion of this training session, you should understand:

- Document acceptance criteria
- Technical acceptance criteria
- What is expected in a control implementation description
- The difference between a good control implementation and a poor control implementation

We are going to review specific tips for writing the SSP; however, the majority of these principles can be applied Document acceptance criteria to all documentation submitted to the FedRAMP PMO for review.

1.5 FedRAMP Mindset for SSP Development



Notes:

Transcript Title

FedRAMP Mindset for SSP Development

Image

FedRAMP Mindset for SSP Development

1. Allocate Sufficient Time and Effort for Writing
2. Strongly and Clearly Articulate Security Architecture and Implementations
3. Tell a Story
4. Answer Who, What, When, Where, Why, and How
5. Answer 100 percent of the Controls
6. Be Clear, Concise, Consistent, and Complete
7. Adequately Reference all Documentation
8. Ensure Compliance with FedRAMP Policy

Text

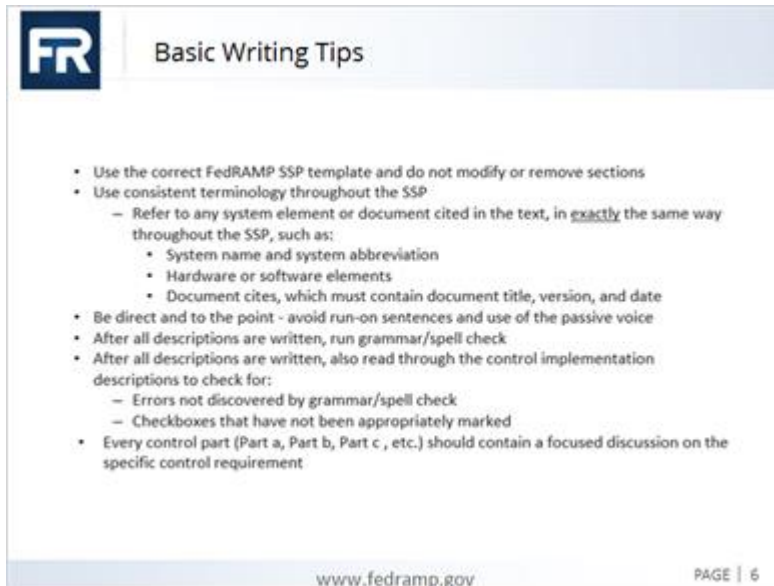
The System Security Plan is a document that requires an eye for detail. A few small mistakes can create a lot of questions following the review by the FedRAMP PMO, Agency, or JAB and slow down the assessment process. Before beginning documentation, it is important to understand the full scope of creating the SSP and level of effort required to make it good.

It is important to understand writing the SSP takes time, effort, careful thinking, and strong, clear articulation of your system's functionality. The SSP is required to be complete and well-structured,

- Make sure that you have the required expertise and knowledge of NIST and FedRAMP security controls.
- Make sure you have enough resources - often one writer is not enough and you may have to allocate additional resources and subject matter experts to complete the SSP (or System Security Plan).
- Make sure that the writers have technical knowledge of the system or can obtain the information from the System Owners.
- For the writers, we want you to tell your story and present the who, what, when, where, why and how of the system.
- When filling out the SSP, be sure to answer 100% of the controls but, keep in mind that a strong SSP is tailored to fit the mission and system environment. If a specific control is inherited or not applicable provide a risk based justification as to why.

We will touch more on these next points in a later slide but be clear, concise, consistent, and complete when writing and make sure you adequately reference all documentation and that your system is compliant with FedRAMP Requirements.

1.6 Basic Writing Tips



The image is a screenshot of a presentation slide titled "Basic Writing Tips". The slide features a blue header with the "FR" logo on the left and the title "Basic Writing Tips" on the right. The main content is a bulleted list of writing guidelines. At the bottom of the slide, there is a footer with the website "www.fedramp.gov" on the left and "PAGE | 6" on the right.

- Use the correct FedRAMP SSP template and do not modify or remove sections
- Use consistent terminology throughout the SSP
 - Refer to any system element or document cited in the text, in exactly the same way throughout the SSP, such as:
 - System name and system abbreviation
 - Hardware or software elements
 - Document cites, which must contain document title, version, and date
- Be direct and to the point - avoid run-on sentences and use of the passive voice
- After all descriptions are written, run grammar/spell check
- After all descriptions are written, also read through the control implementation descriptions to check for:
 - Errors not discovered by grammar/spell check
 - Checkboxes that have not been appropriately marked
- Every control part (Part a, Part b, Part c , etc.) should contain a focused discussion on the specific control requirement

www.fedramp.gov PAGE | 6

Notes:

Transcript Title

Basic Writing Tips

Image

Video covering Basic Writing Tips

Text

- Use the correct FedRAMP SSP template and do not modify or remove sections
- Use consistent terminology throughout the SSP
 - Refer to any system element or document cited in the text, in exactly the same way throughout the SSP, such as:
 - System name and system abbreviation
 - Hardware or software elements
 - Document cites, which must contain document title, version, and date
- Be direct and to the point - avoid run-on sentences and use of the passive voice
- After all descriptions are written; run grammar/spell check
- After all descriptions are written, also read through the control implementation descriptions to check for:
 - Errors not discovered by grammar/spell check
 - Checkboxes that have not been appropriately marked
- Every control part (Part a, Part b, Part c , etc.) should contain a focused discussion on the specific control requirement

Audio

- Use the correct FedRAMP SSP template and do not modify or remove sections. However, you may add sections if relevant to addressing the full scope of the System Security Implementations. The latest version

of the SSP template and all required attachments can be found at FedRAMP.gov.

- Use consistent terminology throughout the SSP.
 - Refer to any system element, or document cited in the text, in exactly the same way throughout the SSP, such as:
 - System Name and System Abbreviation
 - Hardware or software elements
 - Document cites, which must contain document title, version, and date:
 - When citing other sections of the SSP document, use MS Word cross references. That way, as the document changes, any section references can be updated automatically (much like how the SSP author can generate the table of contents automatically as the document changes). This will ensure that, if sections change, references stays relevant with a minimal level of effort.
 - <https://blogs.office.com/2011/09/16/use-cross-references-to-link-to-other-parts-of-a-document/>
- Be direct and to the point. Avoid run-on sentences and use of the passive voice.
- After all descriptions are written, run grammar/spell check.
- After all descriptions are written, also read through the control implementation descriptions to check for:
 - Errors not discovered by grammar/spell check

That all appropriate checkboxes have been marked

Focus discussion: Every control part (e.g., Part a, Part b, Part c etc.) should contain a focused discussion on the specific control requirement. Avoid information that is not directly relevant to the control requirement as this can "muddy the water". Overviews of control families can and are recommended for inclusion in the beginning parts of the SSP.

1.7 Document Acceptance Criteria

The graphic titled "Document Acceptance Criteria" features the FR logo in the top left. It lists four criteria in blue boxes, each with a list of bullet points:

- Clear**
 - Material is unambiguous, clear, and comprehensive
 - Written in correct and consistent format
 - Logical presentation of material
- Concise**
 - Content and complexity are relevant to the audience
 - No superfluous words or phrases
 - Omit words that don't add meaning
- Consistent**
 - Terms have the same meaning throughout the document
 - Items are referred to by the same name or description throughout the document
 - The level of detail and presentation style are the same throughout the document
- Complete**
 - Responsive to all applicable FedRAMP requirements
 - The Security Package includes all appropriate sections of the FedRAMP template
 - The Security Package includes all attachments and appendices

At the bottom, it includes the website www.fedramp.gov and the page number "PAGE | 7".

Notes:

Transcript Title

Document Acceptance Criteria

Image

Video covering Document Acceptance Criteria

- Clear; Concise; Consistent, and Complete

Text

Many of the general principles in writing a quality control implementation for document acceptance criteria are centered around the 4C's... Clear, Concise, Consistent, and Complete. These will be the key points that the FedRAMP PMO will look for when you submit your Security Package. If these points are not met, then the documents will not be accepted and the CSP will be asked to make updates.

- Clear - straightforward, avoiding convoluted phrases or over-long phrases;
- Concise - pack the most meaning into your words;
- Consistent - ensure terms have the same meaning throughout the document and items are referred to by the same name or description. The level of detail and presentation style should also remain the same throughout the document; and finally,
- Complete - be responsive to all applicable FedRAMP requirements and include all appropriate sections of the FedRAMP templates.

1.8 Technical Acceptance Criteria

Criterion	Description
Readable	<ul style="list-style-type: none"> • Refers to the Four Cs for text – Clear, Concise, Complete, and Consistent • Is there a clear understanding of what was written?
Relevant	<ul style="list-style-type: none"> • Refers to the control implementation description addressing the specific control requirement(s) including any parameters • Did the statement address the control requirement?
Sufficient	<ul style="list-style-type: none"> • Refers to the detail and thoroughness contained in the control implementation description - it should be sufficient to allow a reader to understand what is done and how it is done • Is there enough detail to fully address all portions of the requirement?
Complete	<ul style="list-style-type: none"> • Refers both to the control implementation description's agreement with the marked control template checkboxes and its consistency with other SSP text • Do the implementation statements and the control template checkboxes match?

www.fedramp.gov PAGE | 8

Notes:

Transcript Title

Document Acceptance Criteria

Image

Readable, Relevant, Sufficient; Complete

Text

Readable

- Refers to the *Four Cs* for text - *Clear, Concise, Complete, and Consistent*.
- Is there a clear understanding of what was written?

Relevant

- Refers to the control implementation description addressing the specific control requirement(s), including any parameters.
- Did the statement address the control requirement?

Sufficient

- Refers to the detail and thoroughness contained in the control implementation description; it should be sufficient to allow a reader to understand what is done and how it is done. (Build out talking point of HOW)
- Is there enough detail to fully address all portions of the requirement, and to meet any security related needs?

Complete

- Refers to both the control implementation description's agreement with the marked control template checkboxes and its consistency with other SSP text.
- Do the implementation statements and the control template checkboxes match?

1.9 A Poor Control Implementation Description

The slide features a blue header with the 'FR' logo and the title 'A Poor Control Implementation Description'. Below the header is a list of five bullet points. At the bottom, there is a footer with the website 'www.fedramp.gov' and the page number 'PAGE | 9'.

- Inappropriately cites a document or does not contain sufficient detail to demonstrate that the control is implemented and compliant
- Does not identify all persons responsible (by role) for implementing/enforcing the solution to the security control
- Does not describe all possible places where a control is implemented
- Where a single control contains multiple requirements, does not address all requirements
- The wrong Implementation status is checked

www.fedramp.gov PAGE | 9

Notes:

Transcript Title

A Poor Control Implementation Description

Image

Video covering A Poor Control Implementation Description

- Repeats or rephrases the control requirement instead of describing how it is addressed in the system
- Uses "boilerplate" text copied and pasted over and over again
- Contains text not directly relevant to describing how the control is implemented
- Is left blank for example no control implementation description has been written
- Is marked N/A when it is not, or is marked N/A without a risk based justification of why it is considered N/A

Text

The following points are common mistakes and need to be addressed to effectively address Control Implementation statements

Customer Responsibility

The customer specific responsibility should be addressed explicitly and consistently (e.g. addressed under a "Customer Responsibility" heading). This is so that customers know exactly what their responsibilities are with regard to meeting the control requirement exclusively or in partnership with the CSP.

Control Scope

There are multiple platforms in a system identified by the inventory. At minimum each device category has access controls and likely audit logging, sometimes session lock etc. Platforms may have those controls configured uniquely for each device type. It is expected that unique implementations would be addressed by platform for the following controls/control families where applicable: AC, IA, AU, CM, SI-2, SI-3, SI-5, SI-11. Recommend using a standard format for addressing controls by platform (e.g., have a sub header within the control part/parts for "Cisco", "Brocade", "Windows", "Linux", "Oracle" etc).

Where applicable each facility should be addressed including alternate, backup and operational facilities.

Document References

Policies and procedures as well as supporting documents should be explicitly referenced (Title, date and version) so it is clear which is active.

If the entire referenced document does not apply, specific sections references should be provided so the applicable sections can be located easily.

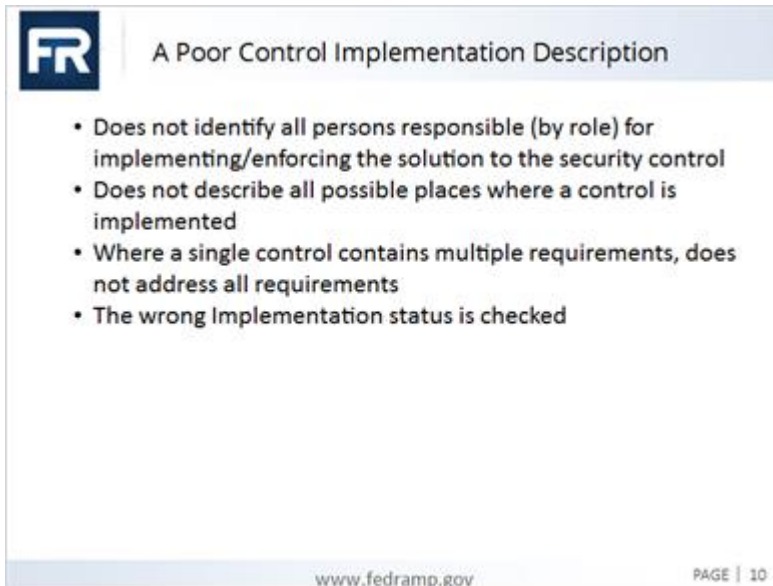
Reviewers should not have to rely solely on following the references to understand the control implementation. An overview of what the referenced document addresses and direct relevancy to the control requirement should be provided so the SSP can stand on its own.

You can have a table at the end of the SSP that specifies all referenced documents, their title, date, and

version. Then reference that table when a document is cited. That way you only have to maintain date and version in one place.

- Repeats or rephrases the control requirement instead of describing how it is addressed in the system.
- Uses “boilerplate” text, copied and pasted over and over again
- Contains text not directly relevant to describing how the control is implemented
- Is left blank for example no control implementation description has been written
- Is marked N/A when it is not, or is marked N/A without a risk based justification of why it is considered N/A
- Inappropriately cites a document or does not contain details and specifics that demonstrate to a limited extent that the control is implemented and compliant. Where a document cite is appropriate to indicate some part of implementation, give title, version, date (and section or page of the document containing the specifics).
- Does not identify all persons responsible (by role) for implementing/enforcing the solution to the security control. A role defined for a control should also be included in the Roles and Privileges table of the SSP.
- Does not describe all possible places where a control is implemented (e.g., only discusses access for non-privileged users and excludes privileged users; only discusses access control for some platforms and not others; only discusses audit logging, maintenance, flaw remediation, configuration management etc for some platforms and not others; only discusses physical controls at one facility.)
- Where a single control contains multiple requirements, does not address all requirements.
- The wrong Implementation Status is checked. For example, Is marked Planned but does not identify planned date or where it is marked Alternative Implementation it does not clearly describe the alternative. As general guidance If all or part of the control is an alternative implementation then the status "Partially Implemented" and "Alternative Implementation" are both checked. If all or part of the control is planned then the status "Partially Implemented" and "Planned" are both checked. If selecting a status of Planned, Alternative Implementation, and/or Not Applicable, the aspects of the control that are Planned, Alternative, and/or Not Applicable should be clearly explained in the implementation description. If the control is solely a customer responsibility and the CSP has no responsibility for the implementation of the control, then "Implemented" is checked and the appropriate customer related control origination is checked.

1.10 A Poor Control Implementation Description



Notes:

Transcript Title

A Poor Control Implementation Description

Image

Video covering A Poor Control Implementation Description

- Does not identify all persons responsible (by role) for implementing/enforcing the solution to the security control
- Does not describe all possible places where a control is implemented
- Where a single control contains multiple requirements, does not address all requirements
- The wrong Implementation status is checked

Text

The following points are common mistakes and need to be addressed to effectively address Control Implementation statements

Customer Responsibility

The customer specific responsibility should be addressed explicitly and consistently (e.g. addressed under a "Customer Responsibility" heading). This is so that customers know exactly what their responsibilities are with regard to meeting the control requirement exclusively or in partnership with the CSP.

Control Scope

There are multiple platforms in a system identified by the inventory. At minimum each device category has access controls and likely audit logging, sometimes session lock etc. Platforms may have those controls configured uniquely for each device type. It is expected that unique implementations would be addressed by platform for the following controls/control families where applicable: AC, IA, AU, CM, SI-2, SI-3, SI-5, SI-11. Recommend using a standard format for addressing controls by platform (e.g. have a sub header within the control part/parts for "Cisco", "Brocade", "Windows", "Linux", "Oracle" etc).

Where applicable each facility should be addressed including alternate, backup and operational facilities.

Document References

Policies and procedures as well as supporting documents should be explicitly referenced (Title, date and version) so it is clear which is active.

If the entire referenced document does not apply, specific sections references should be provided so the applicable sections can be located easily.

Reviewer should not have to rely solely on following the references to understand the control implementation. An overview of what the referenced document addresses and direct relevancy to the control requirement should be provided so the SSP can stand on its own.

You can have a table at the end of the SSP that specifies all referenced documents, their title, date, and version. Then reference that table when a document is cited. That way you only have to maintain date and version in one place.

- Repeats or rephrases the control requirement instead of describing how it is addressed in the system
- Uses "boilerplate" text, copied and pasted over and over again
- Contains text not directly relevant to describing how the control is implemented
 - Is left blank for example no control implementation description has been written
 - Is marked N/A when it is not, or is marked N/A without a risk based justification of why it is considered N/A
 - Inappropriately cites a document or Does not contain details and specifics that demonstrate to a limited extent that the control is implemented and compliant.
-

Where a document cite is appropriate to indicate some part of implementation, give title, version, date (and section or page of the document containing the specifics). Does not identify all persons responsible (by role) for implementing/enforcing the solution to the security control. A role defined for a control should also be included in the Roles and Privileges table of the SSP.

- Does not describe all possible places where a control is implemented (e.g. Only discusses access for non-privileged users and excludes privileged users; only discusses access control for some platforms and not others; only discusses audit logging, maintenance, flaw remediation, configuration management etc for some platforms and not others; only discusses physical controls at one facility.)
- Where a single control contains multiple requirements, does not address all requirements.
- The wrong Implementation Status is checked
 - For example, Is marked Planned but does not identify planned date or where it is marked Alternative Implementation it does not clearly describe the alternative.
 - As general guidance If all or part of the control is an alternative implementation then the status "Partially Implemented" and "Alternative Implementation" are both checked. If all or part of the control is planned then the status "Partially Implemented" and "Planned" are both checked. If selecting a status of Planned, Alternative Implementation, and/or Not Applicable, the aspects of the control that are Planned, Alternative, and/or Not Applicable should be clearly explained in the implementation description. If the control is solely a customer responsibility and the CSP has no responsibility for the implementation of the control, then "Implemented" is checked and the

appropriate customer related control origination is checked.

1.11 Readability Example

FR | Readability Example

AC-17, Part a

- Asks for establishment and documentation of usage restrictions, configuration/ connection requirements, and implementation guidance for each type of remote access allowed

Poor Example - AC-17, Part a:

Remote access for privileged functions be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by <role named> . . . The number of users who can access <system name> remotely is limited and approval for such access is documented.

The example above is difficult to read and understand because:

- The text “meanders” around the point of what the control requires, is off-topic, and is non-specific; this makes it difficult for a reviewer to understand what was meant.
- Insufficient because it does not address all of the specific requirements of the control.

www.fedramp.gov PAGE | 11

Notes:

Transcript Title

Readability Example

Image

Video covering Readability Example

AC-17, Part a

- Asks for establishment and documentation of usage restrictions, configuration/ connection requirements, and implementation guidance for each type of remote access allowed

- Poor Example - AC-17, Part a:

Remote access for privileged functions be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by <role named> . . . The number of users who can access <system name> remotely is limited and approval for such access is documented.

- The example above is difficult to read and understand because:

- The text “meanders” around the point of what the control requires, is off-topic, and is non-specific; this makes it difficult for a reviewer to understand what was meant.
- Insufficient because it does not address all of the specific requirements of the control.

Text

Point out that there is a grammar error (or you correct it) in the first sentence (use "is", not "be").

You can point out that there is heavy use of passive voice (four times).

- The heavy use of passive voice fails to give specific information. So "what" and "how" are not answered.
- Not all the requirements are addressed.

Save words, and omit "this makes it difficult for a reviewer to understand what was meant." You are explaining that concept with your detailed comments.

1.12 Relevancy Example

The slide, titled "Relevancy Example" with the FR logo, is divided into two main sections. On the left, under "CA-1 Requires:", there are two bullet points: "The policy is reviewed and updated [every three years] and" and "The procedures are reviewed and updated [at least annually]". On the right, there are two bullet points. The first is "Poor Example – CA-1, Part b" followed by the text: "Certification, authorization, and security assessment procedures address all areas in the policy and policy-compliant implementations of related security controls." The second bullet point states: "The example is not relevant because it does not address the specifics of CA-1, Part b; a better example might be:" followed by a template sentence: "<System Name> certification, authorization, and security assessment policies are reviewed and updated by <role(s)> at least every three years using <describe process>; the associated procedures are reviewed and updated by <role(s)> at least annually using <describe process>." The slide footer includes "www.fedramp.gov" and "PAGE | 12".

Notes:

Transcript Title

Relevancy Example

Image

Video covering Relevancy Example

CA-1

Requires:

- The policy is reviewed and updated [every three years] and
- The procedures are reviewed and updated [at least annually]
- Poor Example - CA-1, Part b

Certification, authorization, and security assessment procedures address all areas in the policy and policy-compliant implementations of related security controls.

- The example is not relevant because it does not address the specifics of CA-1, Part b; a better example might be:

<System Name> certification, authorization, and security assessment policies are reviewed and updated by <role(s)> at least every three years using <describe process>; the associated procedures are reviewed and updated by <role(s)> at least annually using <describe process>.

Text

"This example does not provide the required relevant information. No policy review and update period is stated. No review and update period for procedures is stated."

1.13 Sufficiency Example

FR | Sufficiency Example

CP-9: Part c

- Requirements include backup of system documentation (daily incremental, weekly full), and at least three backup copies

Poor Example – CP-9, Part c

- The XYZ system has data backup procedures in accordance with control requirements. Daily incremental and weekly full backups are performed (sufficient technical details about which backup procedures are then provided in the control implementation description).
- This example control implementation description is insufficient because it does not specifically mention backup of system documentation, and does not address the FedRAMP requirement for at least three backup copies at all.

www.fedramp.gov | PAGE | 13

Notes:

Transcript Title

Sufficiency Example

Image

Video covering Sufficiency Example

CP-9: Part c:

- Requirements include backup of system documentation (daily incremental, weekly full), and at least three backup copies

Poor Example - CP-9, Part c

The XYZ system has data backup procedures in accordance with control requirements. Daily incremental and weekly full backups are performed . . . (sufficient technical details about which backup procedures are then provided in the control implementation description).

- This example control implementation description is insufficient because it does not specifically mention backup of system documentation, and does not address the FedRAMP requirement for at least three backup copies at all.

Text

First, understand exactly what information the control is asking you to provide before you start writing it.

- Tip #1: If you experience difficulty understanding the requirement, NIST supplemental guidance for the control may help.
- Tip #2: If you find the control text itself difficult to parse, just pick out the subject-verb-object of each sentence; this should make the control specifics clearer.

Keep all of the review parameters in mind when writing (Readability, Relevancy, Sufficiency, and Consistency).

- Sufficiency is the “how” of the writing process (as appropriate, consider “who, what, when, where, why, how” for each control element to assure sufficiency is addressed in your writing).

1.14 Consistency Example

The slide, titled "Consistency Example", features the FR logo in the top left. It is divided into two main sections. The left section, titled "SA-11 (1)", contains a bullet point: "Includes requirements that the developer (of the IS, component, or service) employ static code analysis tools to identify common flaws, and documents analysis results". The right section, titled "Poor Example – SA-11 (1)", contains two bullet points: "Implemented is checked." and "The control implementation description text states: *XYZ system does not develop or code applications which would require such analysis . . .*". Below these sections, a larger bullet point states: "The example above is inconsistent because the control implementation text appears to imply the CSP deems this requirement not applicable, but the control is marked as implemented." The slide footer includes "www.fedramp.gov" and "PAGE | 14".

Notes:

Transcript Title

Consistency Example

Image

Video covering Consistency Example

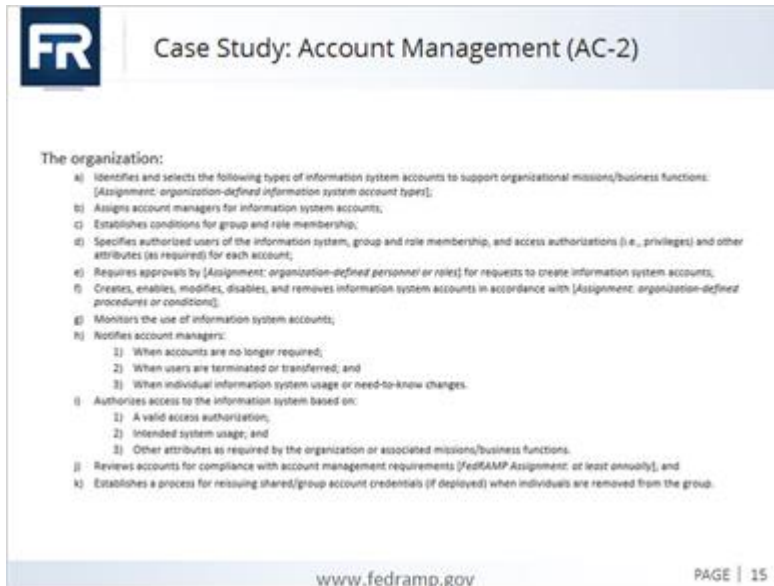
SA-11 (1)

- Includes requirements that the developer (of the IS, component, or service) employ static code analysis tools to identify common flaws, and documents analysis results
- Poor Example - SA-11 (1)
 - Implemented is checked.
 - The control implementation description text states: XYZ system does not develop or code applications which would require such analysis . . .
 - The example above is inconsistent because the control implementation text appears to imply the CSP deems this requirement not applicable, but the control is marked as implemented.

Text

- Includes requirements that the developer (of the IS, component, or service) employ static code analysis tools to identify common flaws, and documents analysis results

1.15 Case Study: Account Management (AC-2)



The organization:

- Identifies and selects the following types of information system accounts to support organizational missions/business functions:
[Assignment: organization-defined information system account types];
- Assigns account managers for information system accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
- Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- Monitors the use of information system accounts;
- Notifies account managers:
 - When accounts are no longer required;
 - When users are terminated or transferred; and
 - When individual information system usage or need-to-know changes.
- Authorizes access to the information system based on:
 - A valid access authorization;
 - Intended system usage; and
 - Other attributes as required by the organization or associated missions/business functions.
- Reviews accounts for compliance with account management requirements [FedRAMP Assignment: at least annually], and
- Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

www.fedramp.gov PAGE | 15

Notes:

Transcript Title

Case Study: Account Management (AC-2)

Image

Video of Case Study: Account Management (AC - 2)

Text

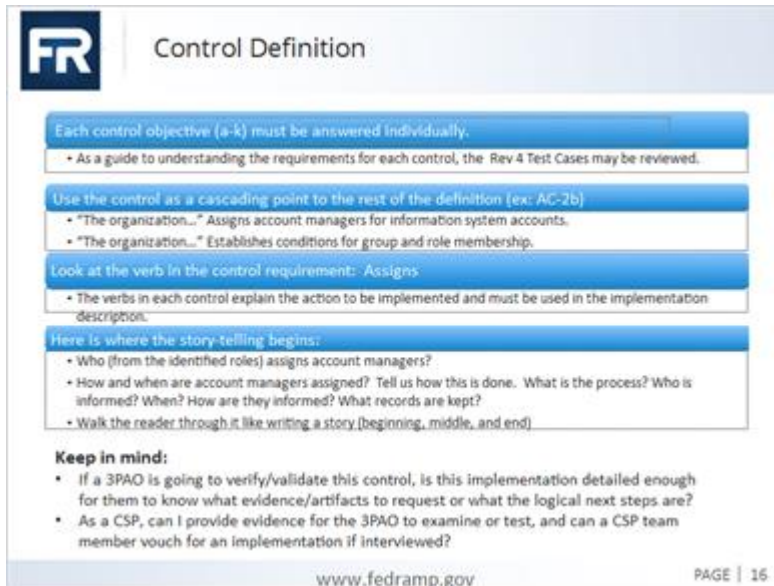
The organization:

- a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];
 - b) Assigns account managers for information system accounts;
 - c) Establishes conditions for group and role membership;
 - d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
- Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
- Monitors the use of information system accounts;
- Notifies account managers:
- When accounts are no longer required;
 - When users are terminated or transferred; and
 - When individual information system usage or need-to-know changes.
- Authorizes access to the information system based on:
 - A valid access authorization;
 - Intended system usage; and
 - Other attributes as required by the organization or associated missions/business functions.
 - Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: at least annually*]; and
 - Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

In analyzing a proper response to a control, let's look at a control in the Access Control family. AC 2 addresses Account Management. It is the CSP's responsibility to describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage, and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer.

With regards to Account Management specifically, Information system account types include, for example, individual, shared, group, system, temporary, and service. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. So let's look further at how to specifically write to this control.

1.16 Control Definition



The slide features a blue header with the 'FR' logo and the title 'Control Definition'. Below the header, there are four blue-bordered boxes containing text and bullet points. The first box states that each control objective (a-k) must be answered individually and provides a guide to understanding requirements. The second box explains how to use the control as a cascading point with an example. The third box focuses on the verb in the control requirement. The fourth box discusses where the story-telling begins. A 'Keep in mind' section follows with two bullet points. At the bottom, the website 'www.fedramp.gov' and 'PAGE | 15' are displayed.

FR Control Definition

Each control objective (a-k) must be answered individually.

- As a guide to understanding the requirements for each control, the Rev 4 Test Cases may be reviewed.

Use the control as a cascading point to the rest of the definition (ex: AC-2b)

- "The organization..." Assigns account managers for information system accounts.
- "The organization..." Establishes conditions for group and role membership.

Look at the verb in the control requirement: Assigns

- The verbs in each control explain the action to be implemented and must be used in the implementation description.

Here is where the story-telling begins:

- Who (from the identified roles) assigns account managers?
- How and when are account managers assigned? Tell us how this is done. What is the process? Who is informed? When? How are they informed? What records are kept?
- Walk the reader through it like writing a story (beginning, middle, and end)

Keep in mind:

- If a 3PAO is going to verify/validate this control, is this implementation detailed enough for them to know what evidence/artifacts to request or what the logical next steps are?
- As a CSP, can I provide evidence for the 3PAO to examine or test, and can a CSP team member vouch for an implementation if interviewed?

www.fedramp.gov PAGE | 15

Notes:

Transcript Title

Control Definition

Image

<N/A>

Text

Let's break the example of AC-2 down to a basic form.

First, each control objective (a-k) will need to be answered individually.

- As a guide to understanding the requirements for each control, the NIST SP 800-53 Rev 4 Test Cases may be reviewed. The Test Case workbook provides a standard risk and controls template for assessing baseline controls and helps to drive consistency in the annual assessment testing performed by Third Party Assessor Organizations (3PAOs). 3PAOs use this workbook to test selected baseline controls per required test procedures and document any control deficiencies and findings.

Use the control as a cascading point to the rest of the definition

- "The organization..." Assigns account managers for information system accounts.
- "The organization..." Establishes conditions for group and role membership.

Look at the verb in the control requirement: **Assigns**

- The verbs in each control explain the action to be implemented and must be used in the description.

Here is where the story-telling begins:

- Who (from your types of user list) assigns account managers?
- How and when are account managers assigned? Tell us how this is done. What is the process? Who is informed? When? How are they informed? What records are kept?

- Walk the reader through it like writing a story (beginning, middle, and end)

Keep in Mind

- A 3PAO must be able to test this control and examine the evidence provided by the CSP.

1.17 Control Writing Tips

FR Control Writing Tips

Organization Defined

- Organization-defined assignments must be defined and documented by a CSP
- Acceptable references may come from Standard Operating Procedures, Security Policy, or Concept of Operations guides

Staying with AC-2, let's look at assessment objective (a):

Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]:

- The control is asking the CSP to **identify** and **select** the types of information system accounts to support organizational missions/business functions
- The CSP can choose to include a reference to the policies where these accounts are identified, as long as the reference includes the **name**, **date**, and **version** of the policies, and the **section number** or **page number** where these accounts can be located

www.fedramp.gov PAGE | 17

Notes:

Transcript Title

Control Writing Tips

Image

<N/A>

Text

- Let's review what is meant by Organization defined assignments and use AC-2 objective (a) as an example. In this case the control is asking the CSP to Identifies and selects the following types of information system accounts to support organizational missions/business functions.
- This definition and assignment may come from SOPs, Policy Documents, or ConOps guides.
- From the requirement, the control is asking the CSP to **identify** and **select** the following types of information system accounts to support organizational missions/business functions.
- The CSP can choose to include a reference to the policies where these accounts are identified, as long as the reference includes the **name**, **date**, and **version** of the policies, and the **section number** where these accounts can be located.

1.18 Control Writing Tips

FR Control Writing Tips

FedRAMP Assignments

- These follow the same logic as organization-defined assignments and must be treated as such
- The assignments are also documented in the “Parameter” sections of the Control Summary Information following the requirements

Requirements with multiple items (AC-2f)

The organization: *Creates, enables, modifies, disables, and removes* information system accounts in accordance with [Assignment: *organization-defined procedures or conditions*];

- Each action must be addressed individually with the same level of detail to satisfy the control, so that it is testable

www.fedramp.gov PAGE | 18

Notes:

Transcript Title

Control Writing Tips

Image

Video of Control Writing Tips

FedRAMP Assignments

- These follow the same logic as organization-defined assignments and must be treated as such
- The assignments are also documented in the “Parameter” sections of the Control Summary Information following the requirements
-

Requirements with multiple items (AC-2f)

The organization: *Creates, enables, modifies, disables, and removes* information system accounts in accordance with [Assignment: *organization-defined procedures or conditions*];

- Each action must be addressed individually with the same level of detail to satisfy the control, so that it is testable

Text

- FedRAMP Assignments follow the same logic as organization-defined assignments. The assignments are also documented in the “Parameter” sections of the Control Summary Information following the requirements.
- When multiple requirements are presented as in the case with AC-2 objective (f) each action needs to be addressed individually with the same level of detail to satisfy the control, so that it is testable.

- Make sure that you write to the how and why for how your organization Creates System Accounts, Enables System Accounts, Modifies System Accounts, Disables System Accounts and Removes System Accounts.

1.19 Information that Can Help You



Notes:

Transcript Title

Information That Can Help You

Image

Video of Information that Can Help You

Use the FedRAMP website, www.fedramp.gov, to:

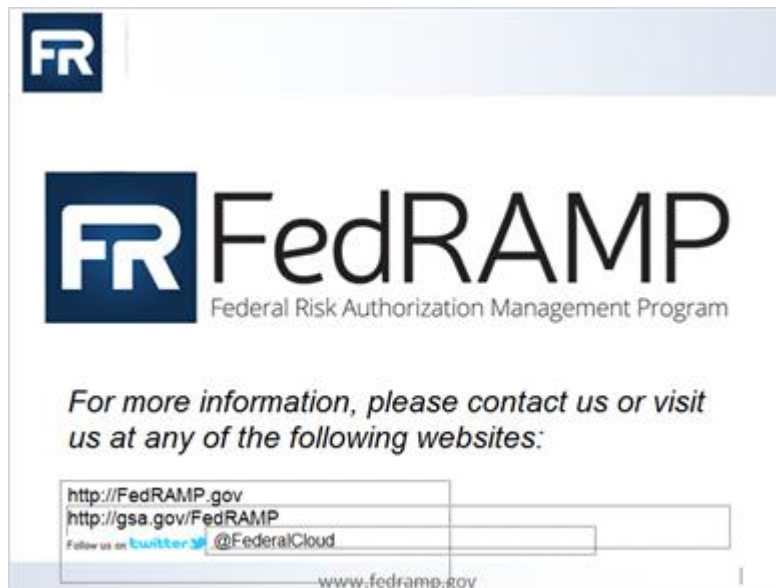
- Obtain the SSP template
- Read "Tips and Cues"
- Read the FedRAMP Newsletter
- Access FedRAMP reference and training materials

- Reference NIST Special Publication 800-53, Revision 4, which contains supplemental guidance for each NIST control
-
- For questions about FedRAMP, email info@fedramp.gov

Text

- Additional information and guidance documents can be found on FedRAMP.gov:
 - FedRAMP Continuous Monitoring Strategy and Guide
 - Vulnerability Scanning Requirements
 - ATO Management and Revocation Guide
 - FedRAMP Plan of Action & Milestones (POA&M) Template Completion Guide
- NIST SP 800-137 - *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
- For questions about FedRAMP, email info@fedramp.gov

1.20 Untitled Slide



Notes:

Transcript

Title <N/A>

Image

Image of FedRAMP logo.

Text

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

<http://FedRAMP.gov>

<http://gsa.gov/FedRAMP>

[@FederalCloud](https://twitter.com/FederalCloud)

References

- Penetration Guidance
- NIST 800 53
- A2LA Website
- SAP Template
- Rev 4 Test Case Workbook