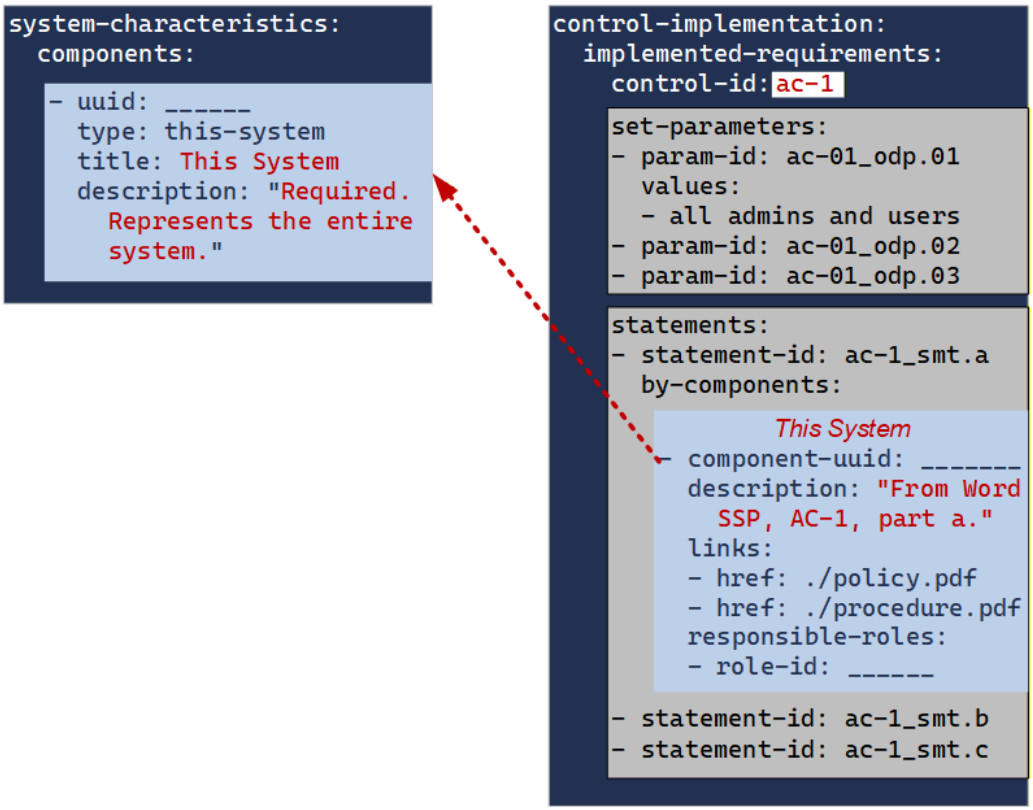
Control Response: Flat Approach

The flat approach to control responses is only intended as a starting point for service providers converting from a legacy FedRAMP SSP Word template.

If you are not converting a legacy SSP, use the Control Response: Normalized Approach.

With the flat approach, the entire statement-level response from a FedRAMP Word-based SSP is represented "as-is" in a single `by-component` entry in OSCAL.



Retrofit Adoption Path: MVP

With OSCAL SSPs, all control responses must be assocaited with a component. To ensure this is always possible, OSCAL SSPs also require the existence of a `this system` component, which represents the entire system.

When converting from a legacy Word-based SSP, the simpelest form of OSCAL adoption is to move the text from each control statement response into the "this system" component response.

Transition to Normalized

Over time, components can be added to the `components` array in `system-characteristics`. Some components will be added in order to represent SSP tables, such as leveraged authorizations, external services and cryptographic modules. Others may be added to support inventory normalization. Add any additional components you need to support or control responses.

At any time, additional `by-components` entries can be added to a `statements` entry, and linked to a component. This may occur one component at a time.

Example Transition

The legacy Word-Based SSP, response to AC-1, Statement a is:

> *The Trust an Compliance Team developed, maintains and disseminates the XYZ Corp Access Control Policy, v2.3 dated January 5th 2024 to all management, administrators and users of the PDQ Cloud System.*
>
> *Chapters 1 and 2 define purpose and scope, while chapter 3 defines roles. Chapters 4 - 8 define responsibilities and coordination, and chapter 9 confirms maangement commitment and potential penalties.*
>
> *The PDQ Information System Security Officer developed, maintains and disseminates the PDQ Access Control Procedure, v 1.1 dated March 1, 2026, which defines access control operations for the system. The ISSO ensures all PDQ Cloud System managers and administrators receive a copy of this docuemnt*

MVP OSCAL Representation

The entire statement above is represented as follows:

- `metadata/roles` entries for the ISSO and Trust and Compliance Team.
- a `this-system` entry in the `components` array
- an `implemented-requirements` entry for AC-1 (`ac-1`)
  - a `statements` entry for AC-1, part a (`ac-1_smt.a`)
    - a `by-components` entry with the `component-uuid` value of the `this-system` entry in the `components` array
      - a `description` field with the statement from the Word-based SSP.

```
system-security-plan:
  metadata:
    roles:
    - role-id: information-system-security-officer
      title: ISSO
    - role-id: trust-and-compliance
      title: Corporate Trust and Compliance Team
  system-implementation:
    components:
    - uuid: 11111111-2222-4000-8000-009000000000
      type: this-system
      title: This System
      description: 'This component represents the entire system or authorization boundary.'

  control-implementation:
    description: 'OSCAL-required field.'
    implemented-requirements:
    - uuid: 11111111-2222-4000-8000-012000010000
      control-id: ac-1

      statements:
      - statement-id: ac-1_smt.a
        uuid: 11111111-2222-4000-8000-012000010100
        by-components:
        - component-uuid: 11111111-2222-4000-8000-009000000000
          uuid: 11111111-2222-4000-8000-012000010101

          description: 'The Trust an Compliance Team developed, maintains and disseminates the
XYZ Corp Access Control Policy, v2.3 dated January 5th 2024 to all management, administrators
and users of the PDQ Cloud System.

Chapters 1 and 2 define purpose and scope, while chapter 3 defines roles. Chapters 4 - 8
define responsibilities and coordination, and chapter 9 confirms maangement commitment and
potential penalties.

The PDQ Information System Security Officer developed, maintains and disseminates the PDQ
Access Control Procedure, v 1.1 dated March 1, 2026, which defines access control operations
for the system. The ISSO ensures all PDQ Cloud System managers and administrators receive a
```

```
copy of this docuemnt.'

          implementation-status:
            state: implemented
          responsible-roles:
          - role-id: information-system-security-officer
          - role-id: trust-and-compliance
```

Transition

In moving to the *normalized* approach, OSCAL components must eventually be defined for required documents. This will result in additional entries to the `components` array as follows:

- Additional entries to the `components` array
  - a `type` set to `policy` or `process-procedure`
  - a `title` with the title of the policy or procedure
  - a `responsible-roles` array with the appropraite role-id cited.

```
system-security-plan:
  system-implementation:
    components:
    - uuid: 11111111-2222-4000-8000-009000000001
      type: policy
      title: XYZ Access Control Policy
      description: 'This is the corporate AC Policy.'
      responsible-roles:
      - role-id: trust-and-compliance

    - uuid: 11111111-2222-4000-8000-009000000003
      type: policy
      title: PDQ Access Control Procedure
      description: 'This is the system-specific AC Procedure.'
      responsible-roles:
      - role-id: information-system-security-officer
```

Once defined, additional by-component entries may be added to the AC-1, part a atatement; however they do not need to be added all at once. For example, the policy may be addressed in one pass and the procedures deferred.

- add one additional `by-components` entry for the policy
- move only the policy portion of the control response
- drop the `trust-and-compliance` role
  - It is not necessary to move the `trust-and-compliance` role as it is defined for the component above.

```
system-security-plan:
  control-implementation:
    implemented-requirements:
    - uuid: 11111111-2222-4000-8000-012000010000
      control-id: ac-1
      statements:
      - statement-id: ac-1_smt.a
        uuid: 11111111-2222-4000-8000-012000010100
        by-components:

        - component-uuid: 11111111-2222-4000-8000-009000000000
          uuid: 11111111-2222-4000-8000-012000010101

          description: 'The PDQ Information System Security Officer developed, maintains and
disseminates the PDQ Access Control Procedure, v 1.1 dated March 1, 2026, which defines access
control operations for the system. The ISSO ensures all PDQ Cloud System managers and
administrators receive a copy of this docuemnt.'

          implementation-status:
            state: implemented
          responsible-roles:
          - role-id: information-system-security-officer

        - component-uuid: 11111111-2222-4000-8000-009000000001
          uuid: 11111111-2222-4000-8000-012000010102

          description: 'The Trust an Compliance Team developed, maintans and disseminates the
XYZ Corp Access Control Policy, v2.3 dated January 5th 2024 to all management, administrators
and users of the PDQ Cloud System.

Chapters 1 and 2 define purpose and scope, while chapter 3 defines roles. Chapters 4 - 8
define responsibilities and coordination, and chapter 9 confirms maangement commitment and
potential penalties.'
```

```
          implementation-status:
            state: implemented
```

When all components have been added, the original `by-components` entry for `this-system` may still be used for providing information (control responses, status differences or additional roles) that do not fit specific component responses.

Revision #9
Created 2026-04-02 16:57:12 UTC by Brian Ruf
Updated 2026-04-07 15:09:07 UTC by Brian Ruf