

Control Response: Policies, Procedures, Plans, RoB, and Guides

Most FedRAMP-required attachments derive their requirement from one or more NIST SP 800-53 controls. With an OSCAL SSP, the attachment is linked directly from the control. This is how tools know which attachment satisfies each requirement.

Control ID	Artifact to Link	Expected
Each <code>-1</code>	Policy	1
Each <code>-1</code>	Procedure(s)	1+
SA-5 (<code>id=sa-5</code>)	Appendix D: User Guide	1
PL-4 (<code>id=pl-4</code>)	Rules of Behavior	1
CP-2 (<code>id=cp-2</code>)	Information System Contingency Plan (ISCP)	1
CM-9 (<code>id=cm-9</code>)	Configuration Management Plan (CMP)	1
IR-8 (<code>id=ir-8</code>)	Incident Response Plan (IRP)	1
CA-7 (<code>id=ca-7</code>)	Continuous Monitoring Plan	1
SR-2 (<code>id=sr-2</code>)	Supply Chain Risk Management Plan (SCRMP)	1

Retrofit MVP

For Retrofit MVP, simply use a `links` array in the `implemented-requirements` entry for each "-1" control.

```
system-security-plan:
  control-implementation:
    description: There is one control in this example. Follow this pattern for each
      additional control.
    implemented-requirements:
      - uuid: 11111111-2222-4000-8000-012000010000
        control-id: ac-1
        links:
          - href: ./AC_Policy.docx
            rel: policy
            media-type: application/docx
```

```
- href: ./AC_Procedure.docx
  rel: procedure
  media-type: application/docx
```

Normalized

For Retrofit Advanced, and all New adoption:

- Attach the document as a back-matter resource.
- Create a component that represents the document
- Specify the component in the control response

Attach Document

[Attach each document](#) as `back-matter` / `resources` entries and include a `props` array with:

- `name` set to `type`
- `value` set to `policy`, `procedure`, `plan`, `users-guide` or `rules-of-behavior`

```
system-security-plan:
```

```
  back-matter:
```

```
    resources:
```

```
      - uuid: 11111111-2222-4000-8000-001000000005
```

```
        title: Access Control and Identity Management Policy
```

```
        description: A single policy that addresses both the AC and IA families.
```

```
        props:
```

```
          - name: type
```

```
            value: policy
```

```
          - name: published
```

```
            value: '2023-01-01T00:00:00Z'
```

```
          - name: version
```

```
            value: '1.2'
```

```
        rlinks:
```

```
          - href: ./attachments/policies/sample_AC_and_IA_policy.pdf
```

```
            media-type: application/pdf
```

Create Component

[Create a component](#) for each document in `system-implementation` / `components` and include:

- a `props` array with one entry:
 - `name` set to `implementation-point`
 - `value` set to `internal` if the document is system-specific; or
 - `value` set to `external` and `class` set to `corporate` if the document is Corporate
- a `links` array with one entry:
 - `href` contains a URI fragment that cites the back-matter resource
 - a hashtag (`#`) followed by the UUID of the back-matter resource.
 - `rel` contains `attachment`

All other fields depicted in the example are required by OSCAL to be present.

```
system-security-plan:  
  
  system-implementation:  
    components:  
      - uuid: 11111111-2222-4000-8000-009000600001  
        type: policy  
        title: Access Control and Identity Management Policy  
        description: 'This is a corporate AC policy used for the system.'  
        props:  
          - name: implementation-point  
            value: external  
            class: corporate  
        links:  
          - href: '#11111111-2222-4000-8000-001000000005'  
            rel: attachment  
        status:  
          state: operational
```

Control Response

Use `implemented-requirements` / `statements` / `by-components` entries in every control response that cites the document.

```
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: 11111111-2222-4000-8000-0090000600001

uuid: 11111111-2222-4000-8000-012000010102

description: Describe how this policy satisfies part a.

implementation-status:

state: implemented

Revision #4

Created 2026-02-12 00:28:03 UTC by Brian Ruf

Updated 2026-04-09 02:33:25 UTC by Brian Ruf