

Inheritance and Customer Responsibilities

For systems that may be leveraged, OSCAL enables a robust mechanism for providing both inheritance details as well as customer responsibilities (referred to as consumer responsibilities by NIST). OSCAL is designed to enable leveraged and leveraging system SSP details to be linked by tools for validation.

Within the appropriate `by-component` assembly, include an export assembly. Use `provided` to identify a capability that may be inherited by a leveraging system. Use `responsibility` to identify a `customer responsibility`. If a `responsibility` must be satisfied to achieve inheritance, add the `provided-uuid` flag to the `responsibility` field.

Representation

```
system-security-plan:
  control-implementation:
    implemented-requirements:
      - uuid: 11111111-2222-4000-8000-012000020000
        control-id: ac-2

    statements:
      - statement-id: ac-2_smt.a
        uuid: 11111111-2222-4000-8000-012000020100
        by-components:
          - component-uuid: 11111111-2222-4000-8000-009000000000
            uuid: 11111111-2222-4000-8000-012000020102
            description: 'Confidential control response.'
            implementation-status:
              state: implemented

        export:
          provided:
            - uuid: 11111111-2222-4000-8000-015000000001
              description: This system's statement of capabilities which may be inherited
                by a customer's leveraging systems toward satisfaction of AC-2, part a.

          responsibilities:
            - uuid: 11111111-2222-4000-8000-016000000001
```

```
provided-uuid: 11111111-2222-4000-8000-015000000001
description: 'Leveraged system''s statement of a leveraging system''s
  responsibilities in satisfaction of AC-2, part a.'
responsible-roles:
- role-id: cloud-service-provider
party-uuids:
- 11111111-2222-4000-8000-004000000001
```

See the [NIST OSCAL Leveraged Authorization Presentation](#) for more information.

Leveraged Authorization Response: Inheriting Controls, Satisfying Responsibilities

When the current system is inheriting a control from or meeting customer responsibilities defined by an underlying authorization, the leveraged system must first be defined as described in the [Response: Identifying Inheritable Controls and Customer Responsibilities](#) section, and documented a `component` in the leveraging system SSP before it may be referenced in a control response. The `by-component` assembly references these components.

IMPORTANT: The leveraged system may provide a single `component` representing the entire leveraged system or may provide individual system components as well. In either case, the `inherited-uuid` property in the `component` must have the `value` flag set to the UUID of the leveraged system or component.

```
The organization:
  (a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or
    roles]:
    (1) An access control policy that addresses purpose, scope, roles, responsibilities,
    management commitment, coordination among organizational entities, and
    compliance; and
    (2) Procedures to facilitate the implementation of the access control policy and
    associated access controls; and
  (b) Reviews and updates the current:
    (1) Access control policy [FedRAMP Assignment: at least annually]; and
    (2) Access control procedures [FedRAMP Assignment: at least annually or whenever a
    significant change occurs].
```

Representation

```
system-security-plan:
  system-implementation:
    components:
      - uuid: 11111111-2222-4000-8000-009000100004
        type: system
        title: Leveraged Authorized System
        description: Briefly describe the leveraged system.
        status:
          state: operational

control-implementation:
  implemented-requirements:
    statements:
      by-components:
        - component-uuid: 11111111-2222-4000-8000-009000000004
          uuid: 11111111-2222-4000-8000-012000020104
          description: For the portion inherited from an underlying FedRAMP-authorized
            provider, describe what is inherited.
          implementation-status:
            state: implemented
          inherited:
            - uuid: 11111111-2222-4000-8000-017000000001
              provided-uuid: 11111111-0000-4000-9009-002001002001
              description: 'Optional description.'
          satisfied:
            - uuid: 11111111-2222-4000-8000-018000000001
              responsibility-uuid: 11111111-0000-4000-9009-002001002002
              description: 'Description of how the responsibility was satisfied.'
```

See the [NIST OSCAL Leveraged Authorization Presentation](#) for more information.

Revision #3

Created 2026-02-12 00:42:29 UTC by Brian Ruf

Updated 2026-04-15 03:20:33 UTC by Brian Ruf