Roles

Every FedRAMP assessment package must identify the party (individual, team or organization) responsible for pre-defined roles, such as system owner and information system security officer (ISSO).

Representing this information in OSCAL requires four important elements:

- `roles` to define the roles
- `parties` to represent individuals, teams or organizations
- `responsible-parties` linking `roles` to `parties`
- Canonical role ID values for required roles ensure consistency for tool processing

This is represented in OSCAL `metadata`.

- A `roles` entry must exist that includes:
  - `id` with an canonical role ID value
  - `title` with a human-readable name for the role as it appears in the FedRAMP authorization package
- One or more `parties` entries must exist that includes:
  - `uuid` with a unique value
  - `type` with a value of `individual` for people or `organization` for teams and organizations
  - `name` with the name of the person, team or organization.
  - other fields as needed, such as `email-addresses`, `telephone numbers`, `addresses` or `location-uuid`.
- A `responsible-parties` entry must exist that includes:
  - `role-id` with the same value as in `roles`/`id` above.
  - `party-uuids` array with one or more UUIDs that reference `parties` entries above.
- Optional `locations` entries that can be linked from party entries

Representation

```
metadata:
  roles:
  - id: system-owner
    title: System Owner
  - id: authorizing-official
    title: Authorizing Official

  locations:
  - uuid: 11111111-2222-4000-8000-003000000001
    title: CSP HQ
```

```
    address:
      type: work
      addr-lines:
      - Suite 0000
      - 1234 Some Street
      city: Haven
      state: ME
      postal-code: '00000'

parties:
- uuid: 11111111-2222-4000-8000-004000000003
  type: individual
  name: A. Person
  email-addresses:
  - a.person@example.com
  location-uuids:
  - 11111111-2222-4000-8000-003000000001

responsible-parties:
- role-id: authorizing-official
  party-uuids:
  - 11111111-2222-4000-8000-004000000003
```

Canonical Role ID Values

The following values are canonical for roles and must be used for `id` in `roles` and `role-id` in `responsible-parties` to ensure consistent tool processing:

Roles for All FedRAMP Artifacts

This role ID	identifies
`prepared-by`	who prepared the FedRAMP artifact
`prepared-for`	for whom the artifact was prepared
`content-approver`	the individual(s) who approve the content in the FedRAMP artifact as accurate and complete.

Roles for System Security Plan (SSP)

This role ID	identifies
`cloud-service-provider`	the Cloud Service Provider's organization
`system-owner`	the CSP officer legally responsible for system
`system-poc-management`	the system's prmariy management contact
`system-poc-technical`	the system's primary technical contact
`authorizing-official`	an Agency's authorizing official (AO)
`authorizing-official-poc`	an Agency's primary point of contact on behalf of the AO.
`system-poc-other`	additional points of contact for the system
`information-system-security-officer`	the individual responsible for the the secure operation of the system
`privacy-poc`	the individual responsible for ensuring appropriate protection of privacy information within the system

For Retrofit MVP, start with just `cloud-service-provider` and `information-system-security-officer`.

Roles for Plan of Action and Milestones (POA&M)

> To be added in Phase 2

Roles for Security Assessment Plan (SAP)

> To be added in Phase 3

Roles for Security Assessment Report (SAR)

> To be added in Phase 3

Revision #7
Created 2026-03-11 21:07:11 UTC by Brian Ruf
Updated 2026-04-15 03:28:08 UTC by Brian Ruf