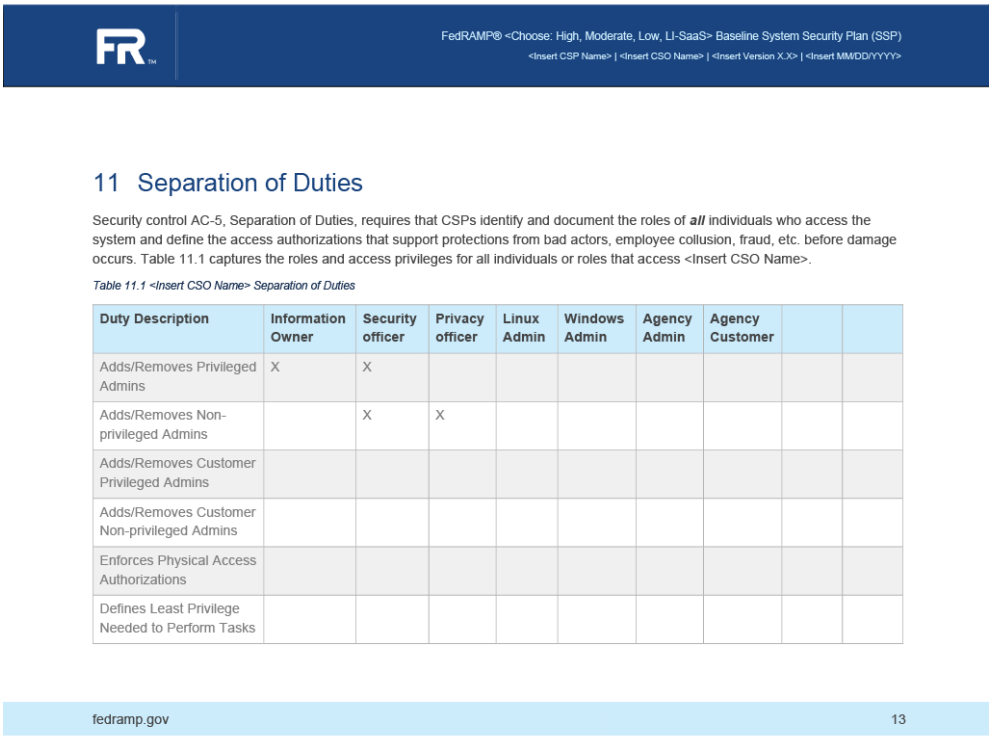
11. Seperation of Duties Matrix



FedRAMP® <Choose: High, Moderate, Low, LI-SaaS> Baseline System Security Plan (SSP)

<Insert CSP Name> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>

11 Separation of Duties

Security control AC-5, Separation of Duties, requires that CSPs identify and document the roles of ***all*** individuals who access the system and define the access authorizations that support protections from bad actors, employee collusion, fraud, etc. before damage occurs. Table 11.1 captures the roles and access privileges for all individuals or roles that access <Insert CSO Name>.

Table 11.1 <Insert CSO Name> Separation of Duties

Duty Description	Information Owner	Security officer	Privacy officer	Linux Admin	Windows Admin	Agency Admin	Agency Customer		
Adds/Removes Privileged Admins	X	X							
Adds/Removes Non-privileged Admins		X	X						
Adds/Removes Customer Privileged Admins									
Adds/Removes Customer Non-privileged Admins									
Enforces Physical Access Authorizations									
Defines Least Privilege Needed to Perform Tasks									

fedramp.gov 13

The `metadata` / `roles` array must have one entry for each column

- an `id` with a token (use pre-defined ID values whenever possible)
- a `title` with a human-readable role name

The `system-implementation` / `users` array must have one entry for each row:

- a `uuid` (required)
- a `props` array with the following entry:
  - a `name` with `separation-of-duties-matrix`
  - a `ns` with `http://fedramp.gov/ns/oscal`
  - a `value` with `yes`
- a `role-ids` array with each entry:
  - the role ID token defined in `metadata` / `roles`
  - Only for roles where an "X" would appear in the table
- an `authorized-privileges` array with one or more entries:
  - a `title` with the text from the "Duty Description" column
  - a `functions-performed` array with at least one string entry describing the function. (This is an OSCAL required field that is not required by FedRAMP.)

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

```
  roles:
  - id: asset-administrator
    title: Asset Administrator
  - id: admin-client
    title: Customer-Designated Administrator
  - id: admin-unix
    title: Unix Administrator

system-implementation:
  users:
  - uuid: 11111111-2222-4000-8000-008000000002
    props:
    - name: separation-of-duties-matrix
      ns: http://fedramp.gov/ns/oscal
      value: 'yes'
    role-ids:
    - asset-administrator
    authorized-privileges:
    - title: Add/Remove Admins
      functions-performed:
      - This can add and remove admins.
  - uuid: 11111111-2222-4000-8000-008000000003
    props:
    - name: separation-of-duties-matrix
      ns: http://fedramp.gov/ns/oscal
      value: 'yes'
    role-ids:
    - asset-administrator
    - admin-client
    authorized-privileges:
    - title: Add/Remove Users
      functions-performed:
      - add/remove non-privliged users
  - uuid: 11111111-2222-4000-8000-008000000004
    props:
    - name: separation-of-duties-matrix
      ns: http://fedramp.gov/ns/oscal
      value: 'yes'
    role-ids:
```

```
    - asset-administrator
    authorized-privileges:
    - title: Cloud-Native Service Deployment
      functions-performed:
      - Manage services and components within the virtual cloud environment.
  - uuid: 11111111-2222-4000-8000-008000000005
    props:
    - name: separation-of-duties-matrix
      ns: http://fedramp.gov/ns/oscal
      value: 'yes'
    role-ids:
    - admin-client
    authorized-privileges:
    - title: Application User Admin
      functions-performed:
      - Add and remove users from the virtual cloud environment.
```

> **The `props` entry is required in each `users` entry.** It identifies which `users` array entries are intended to represent the Separation of Duties Matrix. Tools processing OSCAL SSPs only for FedRAMP should ignore any `users` entry that does not include this `props` entry.

Revision #5
Created 2026-02-25 13:21:30 UTC by Brian Ruf
Updated 2026-04-09 01:32:52 UTC by Brian Ruf