Sections 1 - 11

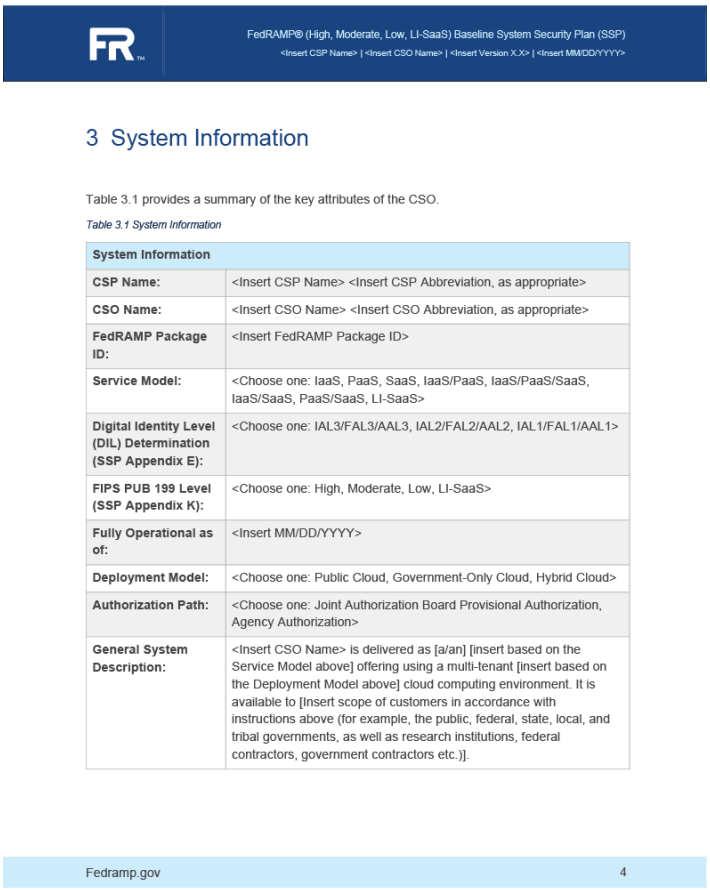
1. Introduction

This entire chapter is FedRAMP PMO boilerplate and does not need to be represented in OSCAL content.

2. Purpose

This entire chapter is FedRAMP PMO boilerplate and does not need to be represented in OSCAL content.

3. System Information



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

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

3 System Information

Table 3.1 provides a summary of the key attributes of the CSO.

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

Fedramp.gov 4

System Information

CSP Name

The cloud service provider (CSP) name and abbreviation are represented in the SSP `metadata`.

- A `roles` extry must exist with `id` = `cloud-service-provider`
- A `parties` entry must exist with the CSP's `name` and `short-name`.
- A `responsible-parties` entry must exist to link the `parties` UUID value to the `cloud-service-provider` role.

OSCAL Representation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000
  metadata:
    roles:
    - id: cloud-service-provider
```

```
      title: Cloud Service Provider
      short-name: CSP

  parties:
    - uuid: 11111111-2222-4000-8000-004000000001
      type: organization
      name: Cloud Service Provider (CSP) Name
      short-name: CSP Acronym/Short Name

  responsible-parties:
    - role-id: cloud-service-provider
      party-uuids:
      - 11111111-2222-4000-8000-004000000001
```

CSO Name

The CSO name and abbreviation are represented in `system-characteristics`.

- The `system-name` field contains the CSO Name
- The `system-name-short` field contains the CSO abbreviation.

OSCAL Representation

```
system-security-plan:
  system-characteristics:
    system-name: System's Full Name
    system-name-short: System's Short Name or Acronym
    system-ids:
    - identifier-type: http://fedramp.gov/ns/oscal
      id: F00000000
```

FedRAMP Package ID

The FedRAMP Package ID is represented in `system-characteristics`.

- A `system-ids` entry must exist that includes:
  - `identifier-type` set to `http://fedramp.gov/ns/oscal`
  - `id` set to the FedRAMP Package ID

OSCAL Representation

```
system-security-plan:
  system-characteristics:
    system-ids:
    - identifier-type: http://fedramp.gov/ns/oscal
      id: F00000000
```

> **FedRAMP Allowed Value**
>
> Required Identifier Type:
>
> - identifier-type="https://fedramp.gov"

Service Model

The Service Model is represented in `system-characteristics`.

- A `system-characteristics` property (`prop`) entry must exist that includes:
  - A `name` set to `cloud-service-model`
  - A `value` set to one of the allowed service model values below.
  - If the `value` is set to `other`, `remarks` is used to explain.

If more than one service model type is applicable (IaaS and PaaS; IaaS and PaaS and SaaS; PaaS and SaaS), use one "cloud-service-model" prop for *each* applicable cloud service model.

OSCAL Representation

```
system-security-plan:
  system-characteristics:
    props:
    - name: cloud-service-model
      value: iaas
    - name: cloud-service-model
```

```
    value: paas
  - name: cloud-service-model
    value: other
    remarks: Remarks are required if service model is "other". Optional otherwise.
```

> **OSCAL Allowed Values**
>
> Valid `cloud-service-model` property values:
>
> - `saas`
> - `paas`
> - `iaas`
> - `other`

Digital Identity Level (DIL) Determination

See Appendix E for appropriate OSCAL representation.

FIPS PUB 199 Level

See Appendix K for appropriate OSCAL representation.

Fully Operational as of

The fully operational date is represented in `system-characteristics`.

- A `system-characteristics` property (`prop`) entry must exist that includes:
  - A `name` set to `fully-operational-date`
  - A `ns` set to `http://fedramp.gov/ns/oscal`
  - A `value` set to the operational date.

Although the `value` field is a string, the date should be treated as an OSCAL date-time-with-timezone data type.

OSCAL Representation

```
system-security-plan:
  system-characteristics:
    props:
    - name: fully-operational-date
      ns: http://fedramp.gov/ns/oscal
      value: '2023-12-31T00:00:00Z'
```

Deployment Model

The Deployment Model is represented in `system-characteristics`.

- A `system-characteristics` property (`prop`) entry must exist that includes:
  - A `name` set to `deployment-model`
  - A `value` set to one of the allowed deployment model values below.
  - If the `value` is set to `other`, `remarks` is used to explain.
- Only one `cloud-deployment-model` property is permitted.

If the deployment model is `hybrid` or `other`, the remarks field is required. Otherwise, it is optional.

OSCAL Representation

```
system-security-plan:
  system-characteristics:
    props:
    - name: cloud-deployment-model
      value: hybrid-cloud
      remarks: Remarks are required if deployment model is "hybrid-cloud" or "other". Optional
otherwise.
```

> **FedRAMP Accepted Values** Valid `cloud-deployment-model` property values:
>
> - `public-cloud`
> - `private-cloud`

- `government-only-cloud`
- `hybrid-cloud`
- `other`

Although core OSCAL also allows `community-cloud`, FedRAMP authorizations do not include community clouds.

Authorization Path

This is an obsolete concept and does not need to be represented in OSCAL.

General System Description

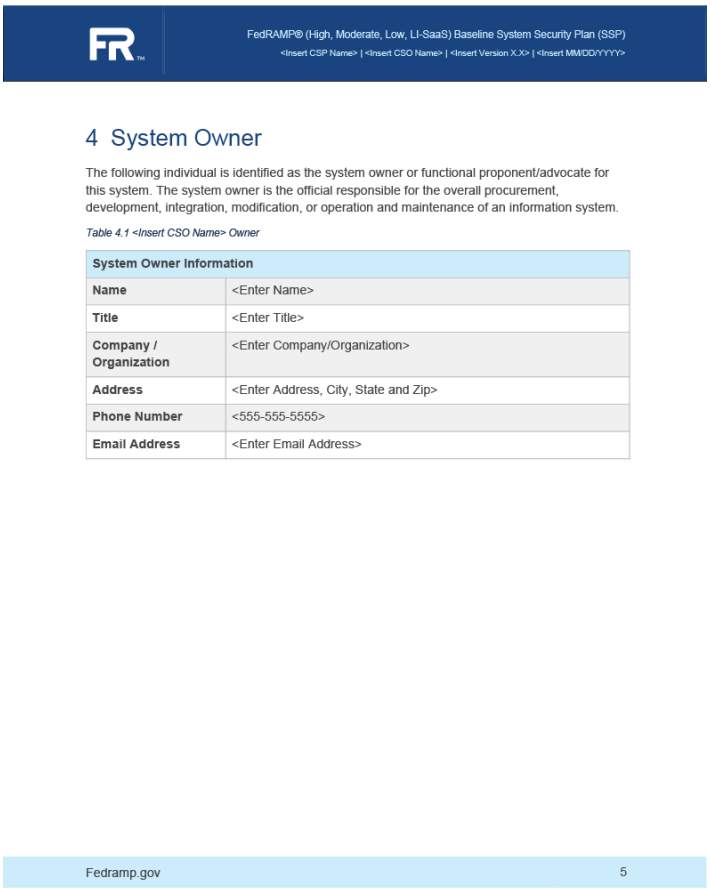
The General System Description is represented in `system-characteristics`.

- The `description` field contains the general system description.
- This is a markup-multiline field.

OSCAL Representation

```
system-security-plan:
  system-characteristics:
    description: '\[Insert CSO Name\] is delivered as \[a/an\] \[insert based on the Service
Model above\] offering using a multi-tenant \[insert based on the Deployment Model above\]
cloud computing environment. It is available to \[Insert scope of customers in accordance with
instructions above (for example, the public, federal, state, local, and tribal governments, as
well as research institutions, federal contractors, government contractors etc.)\].'
```

4. System Owner



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

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

4 System Owner

The following individual is identified as the system owner or functional proponent/advocate for this system. The system owner is the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Table 4.1 <Insert CSO Name> Owner

System Owner Information	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter Email Address>

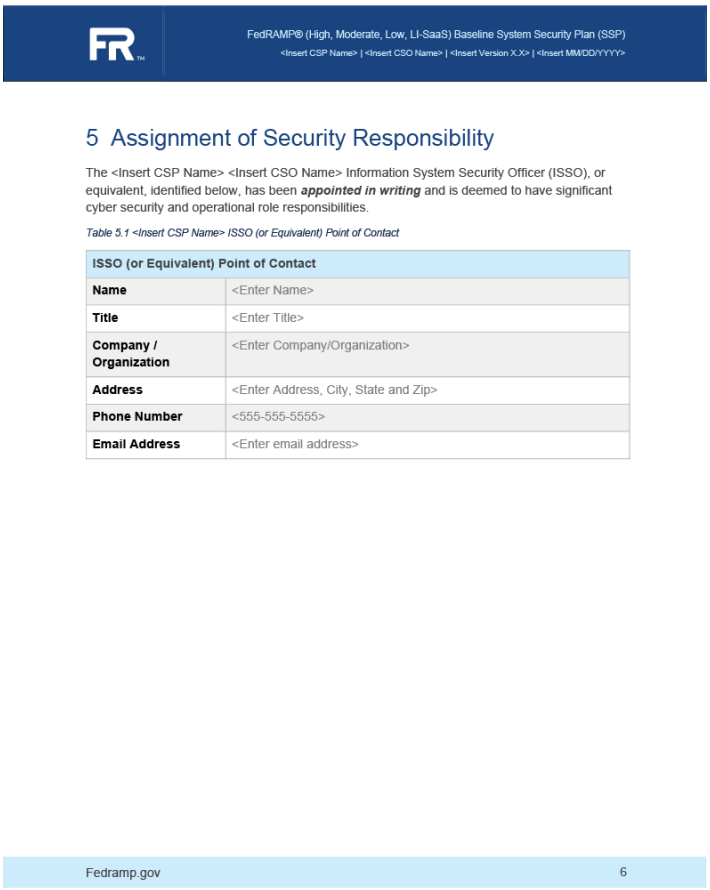
Fedramp.gov 5

System Owner follows the Roles pattern, using the `system-owner` role.

> **Defined Identifiers** Required Role ID:
>
> - `system-owner`

---

5. Assignment of Security Responsibility



FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP)
<Insert CSP Name> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>

5 Assignment of Security Responsibility

The <Insert CSP Name> <Insert CSO Name> Information System Security Officer (ISSO), or equivalent, identified below, has been ***appointed in writing*** and is deemed to have significant cyber security and operational role responsibilities.

Table 5.1 <Insert CSP Name> ISSO (or Equivalent) Point of Contact

ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Fedramp.gov 6

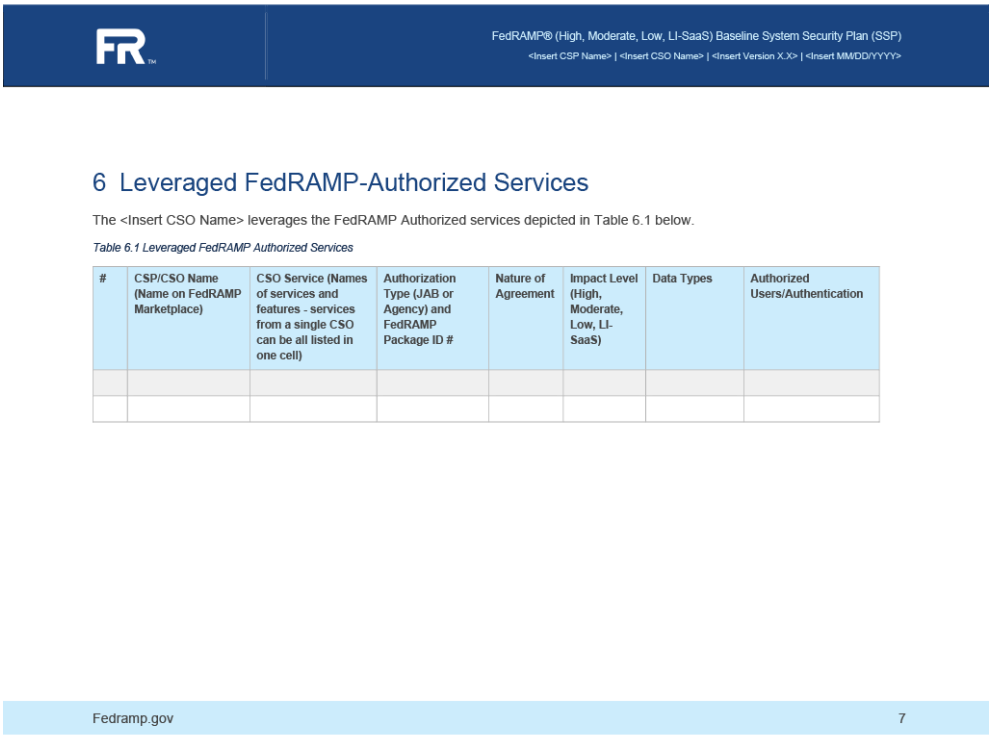
Information System Security Officer (ISSO) follows the Roles pattern, using the `information-system-security-officer` role.

> **Defined Identifiers** Required Role ID:
>
> - `information-system-security-officer`

---

6. Leveraged FedRAMP-Authorized Services

The leveraged FedRAMP-Authorized services table is used to list both underlying leveraged authorizations, such as a SaaS running on an IaaS, and use of external cloud services with FedRAMP authorizations, such as a FedRAMP-authorized third party identity management service.



For each row in Table 6.1 there must be:

- a `parties` entry
- a `leveraged-authorizations` entry
- a `components` entry

`parties` Entry

A `parties` entry to indicate the organizaiton that owns the leveraged system or external service

```
system-security-plan:
  metadata:
    parties:
    - uuid: 22222222-2222-4000-8000-004000000001
      type: organization
      name: Leveraged System Provider's Name
```

```
      short-name: LSPN
```

`leveraged-authorizations` Entry

The `leveraged-authorizations` entry must include:

- a `uuid`
- a `title` with the name of the system or service exactly as it appears in the FedRAMP Marketplace
- a `props` entry with:
  - `name` set to `package-id`
  - `ns` set to `http://fedramp.gov/ns/oscal`
  - `value` set to the package ID exactly as it appears in the FedRAMP Marketplace
- a `props` entry with:
  - `name` set to `security-sensitivity-level`
  - `ns` set to `http://fedramp.gov/ns/oscal`
  - `value` set to `fips-199-low`, `fips-199-modarete` or `fips-199-high` consistent with the FedRAMP Marketplace Information
- a `party-uuid` with the UUID of the `parties` entry above
- a `date-authorized` with the date listed in the FedRAMP Marketplace, expressed in OSCAL `date` format.

> **FedRAMP Extensions**
>
> FedRAMP Extensions are defined when there is no way to represent required information using core OSCAL. They are depicted as propterties (`props` entries) with a namespace (`ns`) value set to `http://fedramp.gov/ns/oscal`. Without the namespace, these properties may be ignored or flagged as invalid.

```
system-security-plan:
  system-implementation:
    leveraged-authorization:
    - uuid: 11111111-2222-4000-8000-019000000001
      title: CSO Name
      props:
      - name: package-id
        ns: http://fedramp.gov/ns/oscal
        value: F9999999999
      - name: security-sensitivity-level
        ns: http://fedramp.gov/ns/oscal
```

```
    value: fips-199-high
party-uuid: 22222222-2222-4000-8000-004000000001
date-authorized: '2015-01-01'
```

> **Allowed Values** The FedRAMP extension `security-sensitivity-level`:
>
> - `fips-199-high`
> - `fips-199-moderate`
> - `fips-199-low`

`components` Entry

The `components` entry must include:

- a `uuid`
- a `type` set to `system`
- a `title` set to the name of the leveraged system
- a `description` of the system. This is a core OSCAL requirement. FedRAMP has no specific requirement for the content of this field.
- a `props` entry with:
  - `name` set to `leveraged-authorization-uuid`
  - `value` set to the UUID of the `leveraged-authorization` entry above
- a `props` entry with:
  - `name` set to `nature-of-agreement`
  - `ns` set to `http://fedramp.gov/ns/oscal`
  - `value` set to `sla`, `contract` [needs more definition]
- a `props` entry with:
  - `name` set to `authentication-method`
  - `ns` set to `http://fedramp.gov/ns/oscal`
  - `value` set to the package ID exactly as it appears in the FedRAMP Marketplace
- One `props` entry for each "Data Type":
  - `name` set to `information-type`
  - `ns` set to `http://fedramp.gov/ns/oscal`
  - `value` set to the NIST SP 800-60 Volume 2 information ID
  - `class` set to `incoming` or `outgoing`
  - If the same information type is exchanged in both directions, there must be one `props` entry for incoming and a separate props entry for outgoing.
- The `status` assembly with the `state` field set to `operational`

    - For FedRAMP the value must always be operational; however, this is a required OSCAL field and cannot be omitted.
- One or more `responsible-roles` entries:
    - Identify the Provider (Required):
        - `role-id` set to `provider` (ensure `metadata` has a `roles` entry with `id` set to `provider`)
        - a `party-uuids` entry with the UUID of the `parties` entry defined above.
    - *Authorized Users*: One entry per authorized user type:
        - `role-id`
            - Use OSCAL-defined canonical values where appropriate.
            - If no canonoical value exists, create an appropriate value that conforms with the OSCAL `token` data type.
            - The value must also exist in the `metadata`/`roles` entries.

OSCAL Representation

```
system-security-plan:
  system-implementation:
    component:
    - uuid: 11111111-2222-4000-8000-009000100001
      type: system
      title: Leveraged Authorized System
      description: Briefly describe the leveraged system.

      props:
      - name: leveraged-authorization-uuid
        value: 11111111-2222-4000-8000-019000000001
      - name: nature-of-agreement
        ns: http://fedramp.gov/ns/oscal
        value: sla
      - name: authentication-method
        ns: http://fedramp.gov/ns/oscal
        value: 'yes'

      - name: information-type
        ns: http://fedramp.gov/ns/oscal
        value: C.3.5.1
        class: incoming
      - name: information-type
        ns: http://fedramp.gov/ns/oscal
        value: C.3.5.8
```

```
    class: outgoing

  status:
    state: operational

  responsible-roles:
  - role-id: provider
    party-uuids:
    - 11111111-2222-4000-8000-c0040000000a
  - role-id: asset-administrator
    party-uuids:
    - 11111111-2222-4000-8000-c0040000000a
```

FedRAMP Marketplace Information Matching

Information about *Leveraged FedRAMP Authorized Services* must match the content in the FedRAMP Marketplace. GSA updates a JSON file nightly that is used to render the FedRAMP Marketplace data.

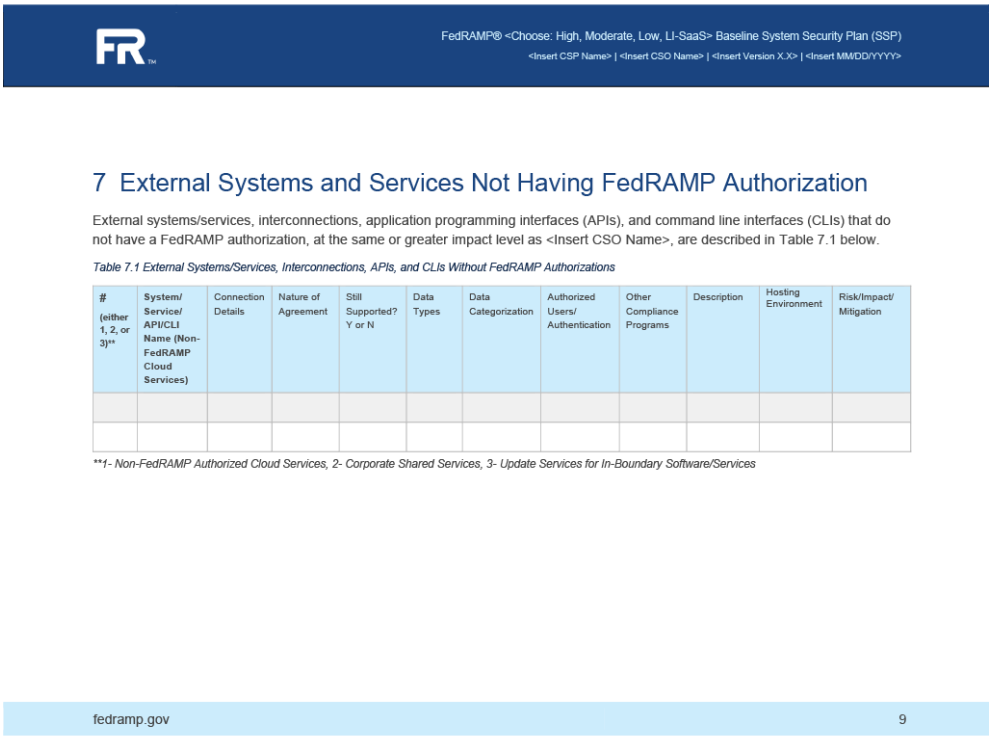
OSCAL Field	GSA Field
CSP Name	`/data/Providers/[#]/Cloud_Service_Provider_Name`
CSO Name	`/data/Providers/[#]/Cloud_Service_Provider_Package`
Package ID	`/data/Providers/[#]/Package_ID`
Authorization Date	`/data/Providers/[#]/Original_Authorization_Date`
Impact Level	`/data/Providers/[#]/Impact_Level`

IMPORTANT FOR LEVERAGED SYSTEMS:

While a leveraged system has no need to represent content here, its SSP SHOULD include special inheritance and responsibility information in the individual controls. See the *Response: Identifying Inheritable Controls and Customer Responsibilities* section for more information.

7. External Systems and Services Not Having FedRAMP Authorization

FedRAMP authorized services should be used, whenever possible, since their risk is defined. However, there are instances where CSOs have external systems or services that are not FedRAMP authorized. In OSCAL, these external systems and services must be identified using `component` assemblies with additional FedRAMP namespace and class properties as shown in the OSCAL representation below.



7 External Systems and Services Not Having FedRAMP Authorization

External systems/services, interconnections, application programming interfaces (APIs), and command line interfaces (CLIs) that do not have a FedRAMP authorization, at the same or greater impact level as <Insert CSO Name>, are described in Table 7.1 below.

Table 7.1 External Systems/Services, Interconnections, APIs, and CLIs Without FedRAMP Authorizations

# (either 1, 2, or 3)**	System/ Service/ API/CLI Name (Non-FedRAMP Cloud Services)	Connection Details	Nature of Agreement	Still Supported? Y or N	Data Types	Data Categorization	Authorized Users/ Authentication	Other Compliance Programs	Description	Hosting Environment	Risk/Impact/ Mitigation

***1- Non-FedRAMP Authorized Cloud Services, 2- Corporate Shared Services, 3- Update Services for In-Boundary Software/Services*

OSCAL Representation

```
system-security-plan:
  system-implementation:
    component:
      uuid: 11111111-2222-4000-8000-009000200001
      type: interconnection
      title: "[EXAMPLE]External System / Service Name"
      description: "Briefly describe the interconnection details."
      prop:
        - ns: "https://fedramp.gov/ns/oscal"
          name: service-processor
          value: "[SAMPLE] Telco Name"
```

```
    - ns: "https://fedramp.gov/ns/oscal"
      name: interconnection-type
      value: "1"
    - name: direction
      value: incoming
    - name: direction
      value: outgoing
    - ns: "https://fedramp.gov/ns/oscal"
      name: nature-of-agreement
      value: contract
    - ns: "https://fedramp.gov/ns/oscal"
      name: still-supported
      value: yes
    - ns: "https://fedramp.gov/ns/oscal"
      class: fedramp
      name: interconnection-data-type
      value: "C.3.5.1"
    - ns: "https://fedramp.gov/ns/oscal"
      class: fedramp
      name: interconnection-data-type
      value: "C.3.5.8"
    - ns: "https://fedramp.gov/ns/oscal"
      class: "C.3.5.1"
      name: interconnection-data-categorization
      value: low
    - ns: "https://fedramp.gov/ns/oscal"
      class: "C.3.5.8"
      name: interconnection-data-categorization
      value: moderate
    - ns: "https://fedramp.gov/ns/oscal"
      name: authorized-users
      value: "SecOps engineers"
    - ns: "https://fedramp.gov/ns/oscal"
      class: fedramp
      name: interconnection-compliance
      value: "PCI SOC 2"
    - ns: "https://fedramp.gov/ns/oscal"
      class: fedramp
      name: interconnection-compliance
      value: "ISO/IEC 27001"
```

```
      - ns: "https://fedramp.gov/ns/oscal"
        name: interconnection-hosting-environment
        value: PaaS
      - ns: "https://fedramp.gov/ns/oscal"
        name: interconnection-risk
        value: None
      - name: isa-title
        value: "system interconnection agreement"
      - name: isa-date
        value: "2023-01-01T00:00:00Z"
      - name: ipv4-address
        class: local
        value: "10.1.1.1"
      - name: ipv4-address
        class: remote
        value: "10.2.2.2"
      - name: ipv6-address
        value: "::ffff:10.2.2.2"
      - ns: "https://fedramp.gov/ns/oscal"
        name: information
        value: "Describe the information being transmitted."
      - ns: "https://fedramp.gov/ns/oscal"
        name: port
        class: remote
        value: "80"
      - ns: "https://fedramp.gov/ns/oscal"
        name: interconnection-security
        value: ipsec
        link:
          - href: "#uuid-of-ICA-resource-in-back-matter"
            rel: isa-agreement
back-matter:
  resource:
    uuid: "11111111-2222-4000-8000-001000000050"
    title: "[SAMPLE]Interconnection Security Agreement Title"
    props:
    - name: published
      value: '2023-01-01T00:00:00Z'
    - name: version
      value: Document Version
```

```
    - name: type
      value: agreement
      class: interconnection-security-agreement
    rlinks:
    - href: ./attachments/ISAs/ISA-1.docx
```

External System and Services

To map the legacy FedRAMP SSP table for **External Systems and Services** into a machine-readable OSCAL format, the data is primarily stored within the `system-implementation` section, specifically under `component` definitions where the `type` is set to `interconnection`.

The following data points are captured using various OSCAL fields and FedRAMP-specific properties (`prop`):

- **Identity & Nature:** The system, service, or API name is defined by the component `title`, while the specific `interconnection-type` (e.g., dedicated line, VPN) and the `nature-of-agreement` (e.g., MOU, ISA) are captured as properties.
- **Operational Details:** Connection characteristics are recorded via properties for `direction` (inbound/outbound), whether the service is `still-supported` (Y/N), and a general `description` of the interface.
- **Data Characteristics:** The `data-type` and its associated `data-categorization` (Security Impact Level) are explicitly defined to track what information is leaving or entering the boundary.
- **User Access:** Information regarding `authorized-users` and their specific `privilege-level` is linked back to the `user` definitions within the system implementation.
- **Compliance & Risk:** Any `other-compliance-programs` (like SOC2 or ISO), the specific `hosting-environment`, and a summary of the `risk-impact-mitigation` strategies are all stored as specific metadata properties attached to the interconnection component.

When documenting multiple external services, each service is treated as a separate instance of an interconnection component within the OSCAL file.

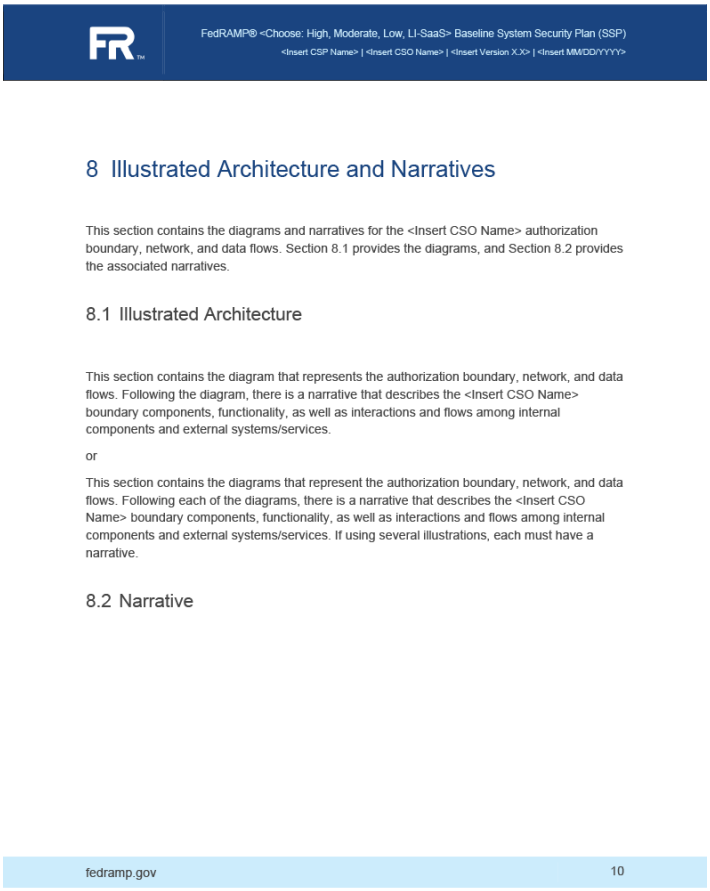
---

8. Illustratred Architecture and Narratives

The Architecture, Network and Data Flow Diagramss are each represented using the same OSCAL patterns, with only the top level assemby name changing.

Authorization Boundary

The OSCAL approach to this type of diagram is to treat the image data as either a linked or base64-encoded `resource` in the `back-matter` section of the OSCAL file, then reference the diagram using the `link` field. The narrative describing the system architecture must be provided in the `description` field of the `authorization-boundary` assembly.



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>

8 Illustrated Architecture and Narratives

This section contains the diagrams and narratives for the <Insert CSO Name> authorization boundary, network, and data flows. Section 8.1 provides the diagrams, and Section 8.2 provides the associated narratives.

8.1 Illustrated Architecture

This section contains the diagram that represents the authorization boundary, network, and data flows. Following the diagram, there is a narrative that describes the <Insert CSO Name> boundary components, functionality, as well as interactions and flows among internal components and external systems/services.

or

This section contains the diagrams that represent the authorization boundary, network, and data flows. Following each of the diagrams, there is a narrative that describes the <Insert CSO Name> boundary components, functionality, as well as interactions and flows among internal components and external systems/services. If using several illustrations, each must have a narrative.

8.2 Narrative

fedramp.gov 10

OSCAL Representation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000
  system-characteristics:
    authorization-boundary:
      description: A holistic, top-level explanation of the FedRAMP authorization boundary.
```

```
      diagrams:
      - uuid: 11111111-2222-4000-8000-007000000001
        description: A diagram-specific explanation.
        links:
        - href: '#11111111-2222-4000-8000-001000000054'
          rel: diagram
        caption: Authorization Boundary Diagram


  back-matter:
    resources:
    - uuid: 11111111-2222-4000-8000-001000000054
      title: Boundary Diagram
      description: The primary authorization boundary diagram.
      props:
      - name: type
        value: image
        class: authorization-boundary
      rlinks:
      - href: ./attachments/diagrams/boundary.png
```

To represent the **Authorization Boundary** from the legacy SSP in an OSCAL-based System Security Plan, the data is centered within the `system-characteristics` section under the `authorization-boundary` element.

The following elements and structures are used to capture the boundary definition:

- **Boundary Narrative:** An `overall-description` is used to provide a high-level technical and functional summary of the system's limits.
- **Visual Documentation:** The model tracks the total number of boundary diagrams present to ensure compliance with the minimum requirement of at least one visual representation.
- **Diagram Linking:** Each diagram is referenced via a `link` containing a unique identifier or path. This link either points to an external URI or a local reference within the OSCAL document.
- **Resource Storage:** The actual image data or file location for a diagram is stored in the `back-matter` section. This is handled as a `resource` which can either contain the raw `base64` encoded image data or a remote link (`rlink`) to the hosted file.
- **Contextual Details:** Individual diagrams can also include their own specific `description` to clarify the components, data flows, or sub-networks depicted in that particular view.

When multiple diagrams are required to show different perspectives of the boundary, each is listed as a sequential entry within the authorization boundary array.

Network Architecture

The network architecture diagram follows the same patter as the *Authorization Boundary* diagram, except the content is placed under `network-architecture` instead of `authorization-boundary`.

OSCAL Representation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000
  system-characteristics:
    network-architecture:
      description: A holistic, top-level explanation of the network architecture.
      diagrams:
      - uuid: 11111111-2222-4000-8000-007000000002
        description: A diagram-specific explanation.
        links:
        - href: '#11111111-2222-4000-8000-001000000055'
          rel: diagram
        caption: Network Diagram

  back-matter:
    resources:
    - uuid: 11111111-2222-4000-8000-001000000055
      title: Network Diagram
      description: The primary network diagram.
      props:
      - name: type
        value: image
        class: network-architecture
      rlinks:
      - href: ./attachments/diagrams/network.png
```

Data Flow

The data flow diagram follows the same pattern as the *Authorization Boundary* diagram, except the content is placed under `data-flow` instead of `authorization-boundary`.

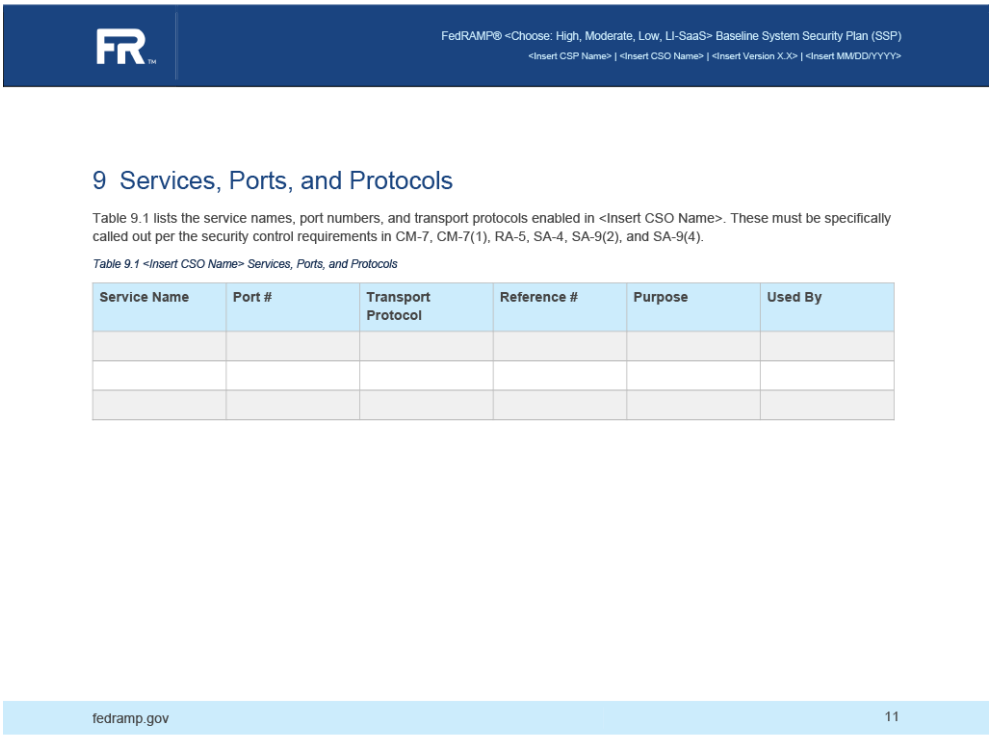
OSCAL Representation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000
  system-characteristics:
    data-flow:
      description: A holistic, top-level explanation of the system's data flows.
      diagrams:
      - uuid: 11111111-2222-4000-8000-007000000003
        description: A diagram-specific explanation.
        links:
        - href: '#11111111-2222-4000-8000-001000000056'
          rel: diagram
        caption: Data Flow Diagram

  back-matter:
    resources:
    - uuid: 11111111-2222-4000-8000-001000000056
      title: Data Flow Diagram
      description: The primary data flow diagram.
      props:
      - name: type
        value: image
        class: data-flow
      rlinks:
      - href: ./attachments/diagrams/dataflow.png
```

9. Services, Ports and Protocols

Entries in the services, ports, and protocols table are represented as component assemblies, with the component-type flag set to "service". Use a protocol assembly for each protocol associated with the service. For a single port, set the port-range start flag and end flag to the same value.



OSCAL Representation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000
  system-implementation:
    components:
    - uuid: 11111111-2222-4000-8000-009000500004
      type: service
      title: API Service
      description: 'A service offered by this system to external systems, such as
        an API. As a result, communication crosses the boundary.



        Describe the service and what it is used for.'
      props:
      - name: implementation-point
```

```
    value: internal
  - name: public
    value: 'yes'
  - name: information-type
    ns: http://fedramp.gov/ns/oscal
    value: C.3.5.1
    class: incoming
  - name: information-type
    ns: http://fedramp.gov/ns/oscal
    value: C.3.5.8
    class: outgoing
  - name: connection-security
    ns: http://fedramp.gov/ns/oscal
    value: tls-1.3
  - name: authentication-method
    ns: http://fedramp.gov/ns/oscal
    value: 'yes'
  - name: nature-of-agreement
    ns: http://fedramp.gov/ns/oscal
    value: other
  - name: allows-authenticated-scan
    value: 'no'
  - name: scan-type
    ns: http://fedramp.gov/ns/oscal
    value: infrastructure
links:
- href: '#11111111-2222-4000-8000-009000100003'
  rel: used-by
- href: '#11111111-2222-4000-8000-009000100004'
  rel: used-by
- href: '#11111111-2222-4000-8000-001000000048'
  rel: poam-item
  resource-fragment: 11111111-3333-4000-8000-000000000004
- href: https://api.example.com/v1
  rel: api
status:
  state: operational
responsible-roles:
- role-id: administrator
  props:
```

```
      - name: privilege-uuid
        ns: http://fedramp.gov/ns/oscal
        value: 11111111-2222-4000-8000-008000000004
      party-uuids:
      - 11111111-2222-4000-8000-004000000010
      - 11111111-2222-4000-8000-004000000011
      - 11111111-2222-4000-8000-004000000012
    - role-id: provider
      party-uuids:
      - 11111111-2222-4000-8000-004000000001
  protocols:
  - uuid: 11111111-2222-4000-8000-010000000002
    name: tls
    title: API Service
    port-ranges:
    - start: '443'
      end: '443'
      transport: TCP
```

To represent **Network Services and Ports** within an OSCAL System Security Plan, the data is organized under the `system-implementation` section, specifically categorized by components where the `type` is defined as `service`, `hardware` or `software`.

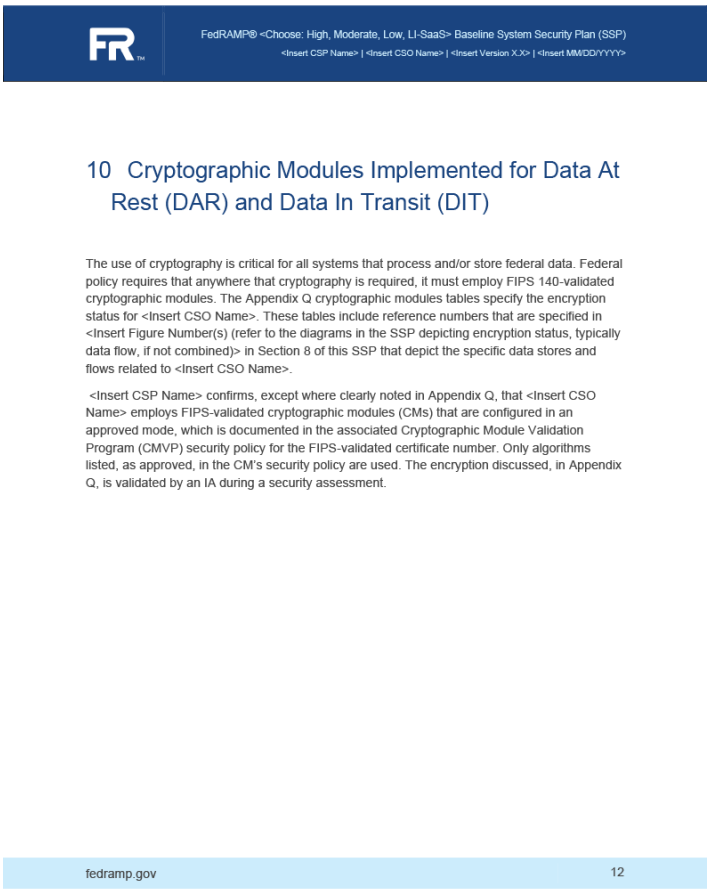
The mapping for each service entry includes the following technical details:

- **Service Identity:** Each entry starts with a `title` that identifies the specific service or application name (e.g., "HTTPS" or "SSH").
- **Protocol Configuration:** The specific network `protocol` name (such as TCP or UDP) is identified to define how the service communicates.
- **Port Management:** Detailed port information is captured within a `port-range`, specifying the exact `start` and `end` values. This also includes the `transport` layer designation to ensure the specific communication path is fully defined.
- **Functional Justification:** A dedicated `purpose` field provides the business or technical rationale for why the service is required within the system boundary.
- **Component Relationships:** The model tracks which internal system elements are utilizing the service by linking to the `title` of other defined components via their unique identifiers (UUIDs).

For systems with multiple services, each is documented as an individual service component, with the ability to define multiple protocols and port ranges within each entry to maintain a complete and granular inventory.

---

10. Cryptographic Modules Implemented for DAR and DIT



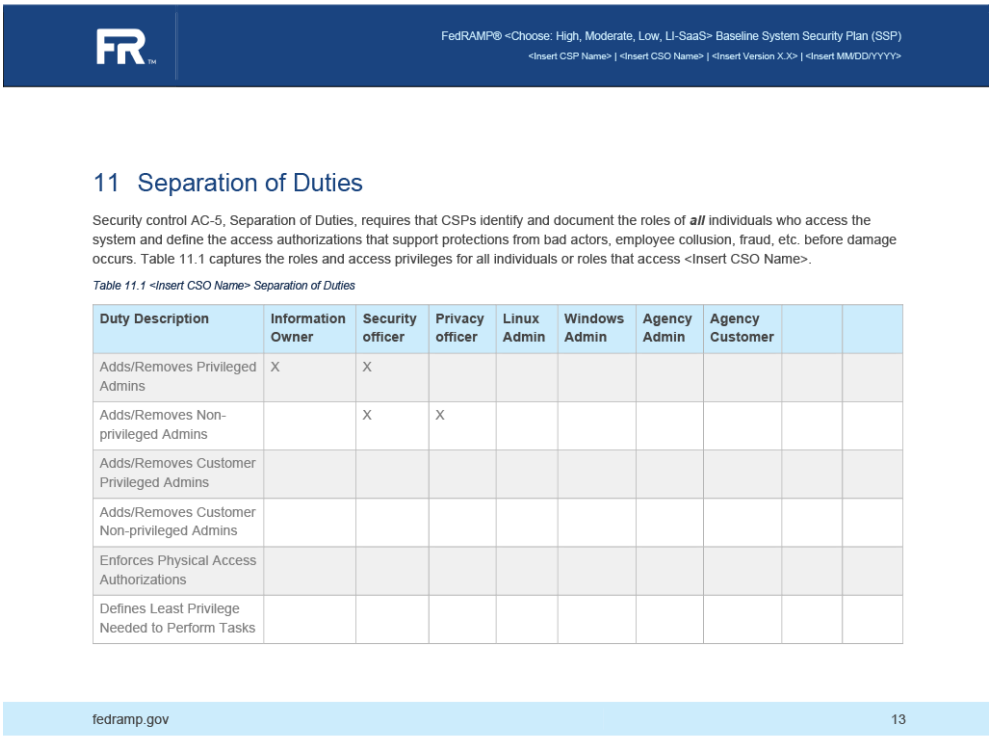
10 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT)

The use of cryptography is critical for all systems that process and/or store federal data. Federal policy requires that anywhere that cryptography is required, it must employ FIPS 140-validated cryptographic modules. The Appendix Q cryptographic modules tables specify the encryption status for <Insert CSO Name>. These tables include reference numbers that are specified in <Insert Figure Number(s) (refer to the diagrams in the SSP depicting encryption status, typically data flow, if not combined)> in Section 8 of this SSP that depict the specific data stores and flows related to <Insert CSO Name>.

<Insert CSP Name> confirms, except where clearly noted in Appendix Q, that <Insert CSO Name> employs FIPS-validated cryptographic modules (CMs) that are configured in an approved mode, which is documented in the associated Cryptographic Module Validation Program (CMVP) security policy for the FIPS-validated certificate number. Only algorithms listed, as approved, in the CM's security policy are used. The encryption discussed, in Appendix Q, is validated by an IA during a security assessment.

This is address in Appendix Q: Cryptographic Modules.

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.