Adopting OSCAL for SSP Representation

SSP Adoption Strategies

The best way to adopt OSCAL for your system depends on your circumstances. The OSCAL Foundation defines two adoption strategies:

- **Retrofit Adoption Path**: Converting Legacy Documentation
- **Native Adoption Path**: Creating New Documentation

Retrofit Adoption Path

If you need to convert legacy documentation to OSCAL, follow the Retrofit Adoption Path.

Migrate existing content to OSCAL with the minimum necessary refactoring, and normalize content over time.

Native Adoption Path

If you are approaching OSCAL to intially create your system security plan and do not have legacy documentaiton to convert, follow the Native Adoption Path.

> The FedRAMP PMO prefers new systems follow the FedRAMP 20x Authorization Path. We will prioritize 20x representation in OSCAL based on demand from CSPs and Agency Authorizing Officials (AO).

Retrofit Adoption Path

If you need to convert legacy documentation to OSCAL, follow this path.

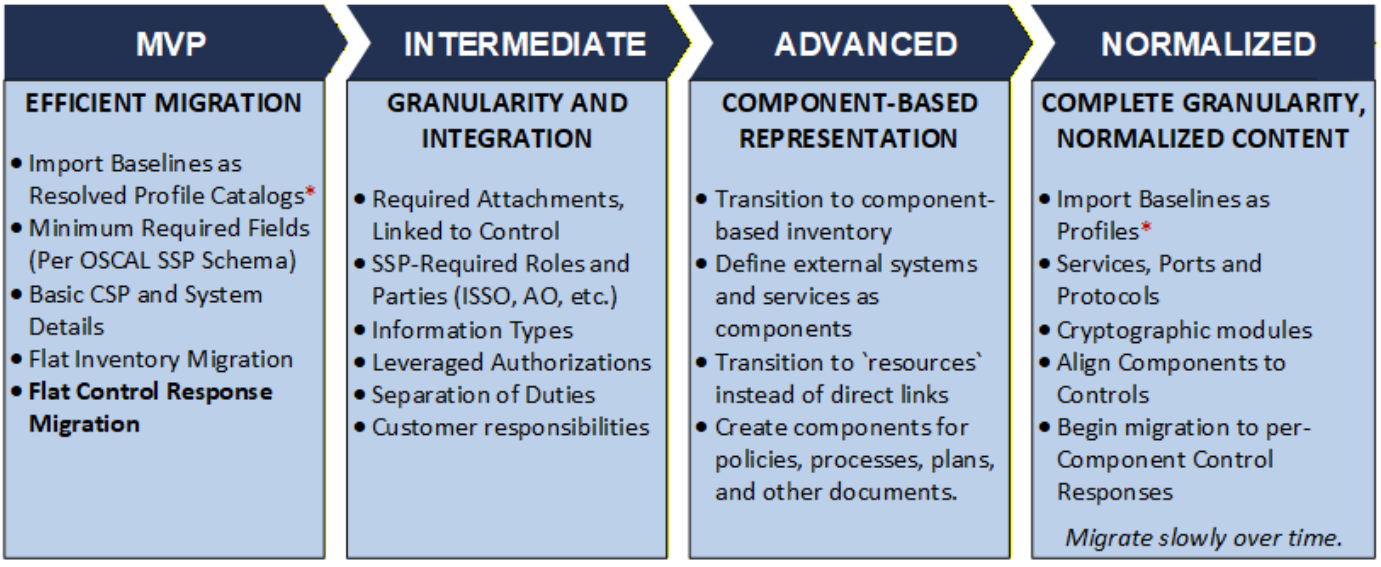
If you are approaching OSCAL to intially create your system security plan and do not have legacy documentation to convert, follow the Native Adoption Path.

Organizations with existing Word and Excel based authorization packages must first migrate their content to OSCAL with only the minimum necessary refactoring. The *Retrofit Adoption Path* starts with a minimum viable product (MVP) and evolves to more comprehensive use cases in phases.

This approach initially sacrifices data normalization in favor of a more rapid transition to OSCAL. It allows conversion of content as-is, then gradually eliminates redundancy and normalizes data in subsequent phases. This is possible because OSCAL is designed to meet you where you are, and it allows gradual progress toward its more normalized ideal representation.

SSP Retrofit Adoption Overview

The OSCAL Foundation recommends the following addoption path for migrating legacy FedRAMP SSP content to OSCAL.



> To facilitate conversion of legacy Word content, OSCAL allows legacy control responses to be associated with the "this-system" component. CSPs can migrate slowly over time to the

> OSCAL's preferred per-component responses.

SSP Adoption Path

MINIMUM VIABLE PRODUCT (MVP)

- **Import Baselines as *Resolved Profile Catalogs***
  - Get started with Use pre-processed control baselines.
  - See Baselines for more information.
- **Minimum Required Fieldss and Basic CSP and System Details.**
  - `metadata` includes:
    - `title`, `published`, `last-modified`, `version`, `oscal-version`
    - `roles`: `cloud-service-provider`, `information-system-security-officer`, others as cited in controls.
      - See *Roles* for more information on roles.
    - `parties`: the CSP, the ISSO.
      - See *Parties and Locations* for more information on defining parties.
    - `responsible-parties`: exactly one, linking the CSP party to the CSP role
      - See *Roles* for more information on associating parties with roles.
  - `system-characteristics` includes:
    - `system-id`, `system-name`, `system-name-short`, `description`, *cloud-service-model* `prop` and *cloud-deployment-model* `prop`
      - See *3. System Information* for more information
    - `security-sensitivity-level` (`fips-199-high`, `fips-199-moderate`, `fips-199-low`)
    - `system-information`: exactly one entry with Appendix K pasted into the `description`
    - `status` set to `operational` (required OSCAL fields)
      - See *System Status* for more information.
    - `authorization-boundary`, `network-architecture` and `data-flow`: `description` and `links` entry identifying the external attachment.
      - See *8. Illustratred Architecture and Narratives* for more information.
  - `system-implementation` includes:
    - `components:
      - Exactly one, with `type` = `this-system` (Known as the "this-system" component, which represents the system as a whole.)
      - See *Components* for more information.
- **Flat Inventory Migration**
  - Convert directly from spreadsheet.

    - Non-normalized. No corrisponding components.
    - `system-implementation`:
        - `inventory-items`: All inventory converted from Excel spreadsheet
- **Migrate Control Response**
    - Minimum-necessary adjustments for OSCAL.
    - All response statements in the "this-system" component.
    - `control-implementation`
        - `implemented-requirement` (AC-1, AC-2, etc.)
            - `set-parameters`: set parameters as needed
            - `statement` (part a, part b, etc.
                - `by-component` ("this system")
                    - `description`: Content directly from legacy Word SSP (part a, part b, etc.)
                    - `implementation-status`
                    - `responsible-roles`: One entry per role. Use `role-id`. Must match `metadata/roles/id`.

> During transition, any portion of the Word SSP not yet converted to OSCAL should be attached to the OSCAL SSP content.

INTERMEDIATE

- **Required Attachments**
    - Add direct `links` from the appropriate controls to identify relevant attachments
- **Required SSP Roles**
    - `metadata/roles` The roles required by SSP (System owner, ISSO, AO, etc.)
    - `metada/parties`: the people, teams and organizations responsible for the above roles
    - `metadata/responsible-parties`: links the above `roles` and `parties`
- **Information Types**
    - `system-characteristics/system-information/information-types`
        - a single entry for each row in appendix K.
- **Leveraged Authorizations**
    - `system-implementation/leveraged-authorizations`:
        - one entry for leveraged authorization
        - corrisponding `metadata/parties` entry for each
        - corrisponding `system-implementation/components` for each.
- **Separation of Duties Matrix**
    - `system-implementation/users`
        - one entry per row in Table 11.1
        - `./authorized-privilege/functions-performed`: SSP Table 11.1 Duty Description (just one entry in the array)
        - `./authorized-privilege/title`: Required by OSCAL, not by FedRAMP. Recommend duplicating the `functions-performed` content.

    - `role-ids`: links `metadata/roles` to `functions-performed`
- **Customer Responsibility and Inheritance**:
    - Move customer responsibility statements to `//by-components/export/responsibilities`

ADAVANCED

- **Normalize Inventory**: Transition flat inventory to component-based inventory.
    - Use `components` to the greatest degree practical
    - `inventory-items` become implemented instances of components
- **External Systems and Services**
    - `system-implementation/components` entries for each
- **Transition to `resources`**
    - Where practical, use URI fragments in `links` to reference resources instead of direct links. See *[section citation and link]* for more information.
- **Components for Required Documents**
    - One for each required document (policies, procedures, plans, user guides, Rules of Behavior)
    - See *[Section citation and link]* for more information.

NORMALIZED

- **Import Baselines as Profiles**
    - Eliminate reliance on *resolved profile catalogs*
    - Ensure your tools have the ability to process profiles by this phase.
    - Ensure consumers of your SSP are able to process profiles.
- **Services, Ports and Protocols**
- **Migrate to component-based control responses**
    - Add `components` entries as needed to support normalized inventory
    - Add `by-components` entries to `implemented-requirements` for each relevant component
    - Add/move component-specific control responses to their associated `by-components` response.
    - Migrate slowly over time.
- **Cryptographic Modules (App Q table)**

> ### Profile Imports
>
> The decision to import a *profile* or *resolved profile catalog* is dependent on the profile processing capability of your tools and the tools of any receiving party.

> Pre-processed *resolved profile catalogs* are a simplified way to get started; however, OSCAL tools must ultimately process profiles. Processing OSCAL profiles is the only way tools can handle control overlays and multiple frameworks.
>
> If you elect to start with *resolved profile catalogs*, migrate to *profiles* as soon as yoru tools and your recipients tools can perform this processing.
>
> ### Easy Migration
>
> Within an OSCAL SSP, migration is performed simply by changing the `import-profile` statement to reference the appropriate *profile* instead of a *resolved profile catalog*.

Native Adoption Path

If you are approaching OSCAL to intially create your system security plan and do not have legacy documentation to convert, follow this path.

If you need to convert legacy documentation to OSCAL, follow the Retrofit Adoption Path.

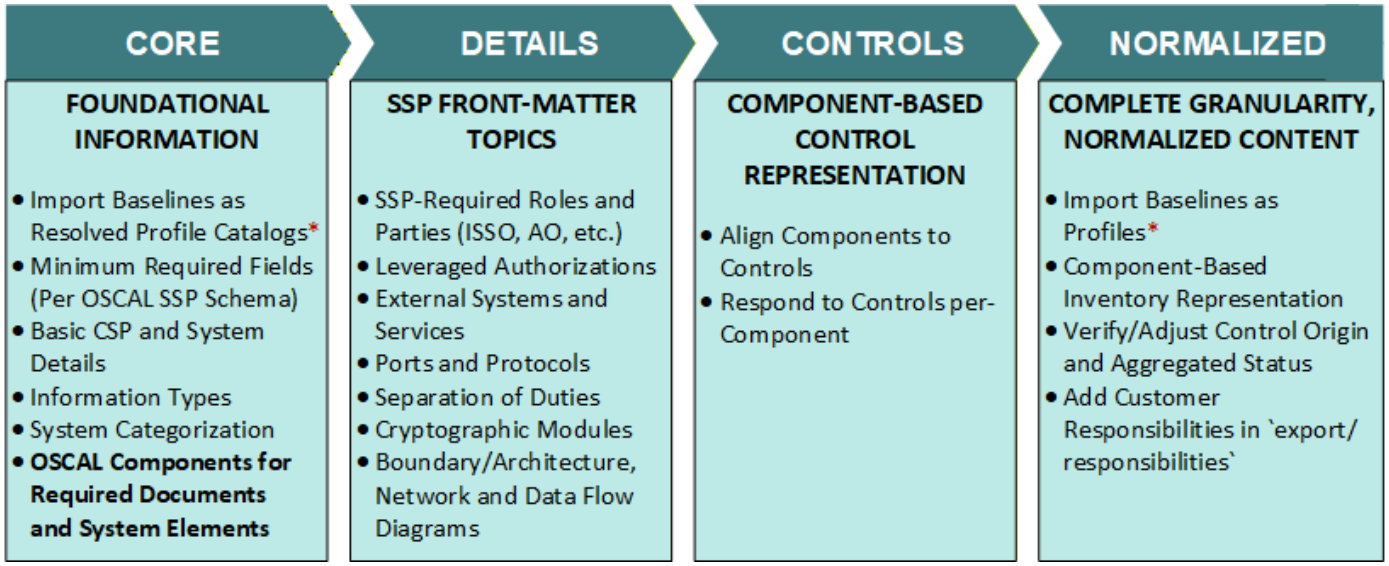
> The FedRAMP PMO prefers new systems follow the FedRAMP 20x Authorization Path. We will prioritize 20x representation in OSCAL based on demand from CSPs and Agency Authorizing Officials (AO).

Organizations adopting OSCAL for initial SSP creation must be mindful of OSCAL's relational dependencies to ensure efficient content population. The *Native Adoption Path* starts with `components` and other core system details, then builds on those components in later phases to achieve highly normalized and complete SSP content.

This approach prioritzes data normalization from the start. It establishes foundational data elements on which later phases build. This ensures logical sequencing of activties and efficient progression of SSP detail.

SSP Native Adoption Overview

The OSCAL Foundation recommends the following addoption path when creating an OSCAL-based FedRAMP SSP from scratch.



CORE

- **Import *Resolved Profile Catalogs***
  - Get started with Use pre-processed control baselines.
  - See Baselines for more information.
- **Minimum Required Fields and Basic CSP and System Details**
  - `metadata` includes:
    - `title`, `last-modified`, `version`, `oscal-version` (required OSCAL fields)
    - `roles`: `cloud-service-provider`
    - `parties`: the CSP
    - `responsible-parties`: exactly one, linking the CSP party to the CSP role.
  - `system-characteristics` includes:
    - `system-id`, `system-name`, `system-name-short`, `description` (required OSCAL fields)
    - *cloud-service-model* and *cloud-deployment-model* `props`
    - `status` set to `operational` (required OSCAL fields)
    - `authorization-boundary/description`: Only a brief description is required.
- **Information Types and System Categorization**
  - `system-characteristics` includes:
    - `system-information`
    - `security-sensitivity-level` (`fips-199-high`, `fips-199-moderate`, `fips-199-low`)
    - See Appendix K: FIPS-199 Worksheet for more information.
- **OSCAL Components for Required Documents and System Elements**
  - `system-implementation`
    - `components`:
      - Exactly one "this system" component (`type` = *`this-system`*) (Represents the system as a whole.)
      - One for each technical element (hardware, software, virtual appliance, service) used in the system
      - One for each required document (policies, procedures, plans, user guides, Rules of Behavior)
      - See *[Section citation and link]* for more information.

DETAIL

- **SSP-Required Roles and Parties**: See *[Seciton citation and link]*
- **Leveraged Authorizations**: See *[Seciton citation and link]*
- **External Systems and Services**: See *[Seciton citation and link]*
- **Ports and Protocols**: See *[Seciton citation and link]*
- **Separation of Duties**: See *[Seciton citation and link]*
- **Cryptographic Modules**: See *[Seciton citation and link]*
- **Diagrams**: See *[Seciton citation and link]* See *[Seciton citation and link]*
  - Boundary/Architecture Diagram and Narriative
  - Network Architecture Diagram and Narriative
  - Data Flow Diagram and Narriative

CONTROLS

- **Align Components to Controls**: See *[Seciton citation and link]*
- **Respond to Controls per-Component**: See *[Seciton citation and link]*

NORMALIZED

- **Import Baselines as Profiles**
  - Eliminate reliance on *resolved profile catalogs*
  - Ensure your tools have the ability to process profiles by this phase.
  - Ensure consumers of your SSP are able to process profiles.
- **Component-Based Inventory Representation**: See *[Seciton citation and link]*
- **Verify/Adjust Control Origin and Aggregated Status**: See *[Seciton citation and link]*
- **Add Customer Responsibilities**: See *[Seciton citation and link]*
