

# Native Adoption Path

If you are approaching OSCAL to initially 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).

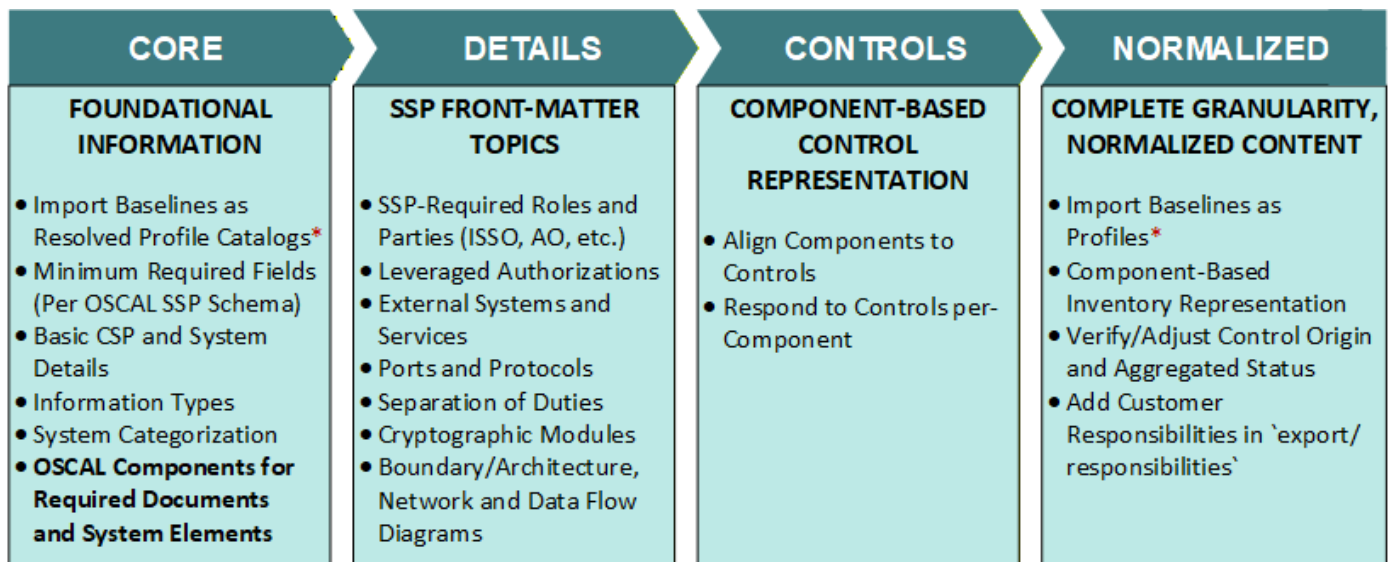
---

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

## SSP Native Adoption Overview

The OSCAL Foundation recommends the following adoption 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]*

---

Revision #19

Created 2026-03-26 18:02:39 UTC by Brian Ruf

Updated 2026-08-20 14:04:30 UTC by Brian Ruf