# FedRAMP Extensions and Allowed Values

NIST designed the core OSCAL syntax to model cybersecurity information that is common to most organization and compliance frameworks; however, NIST also recognized the need to provide flexibility or organizations with unique information needs.

*A summary of the FedRAMP extensions and allowed values appears in the FedRAMP OSCAL Registry.*

Instead of trying to provide a language that meets each organization's unique needs, NIST provided designed OSCAL with the ability to be extended.

As a result, FedRAMP-compliant OSCAL files are a combination of the core OSCAL syntax and extensions defined by FedRAMP. The [*Guide to OSCAL-Based FedRAMP Content*](https://github.com/GSA/fedramp-automation/raw/master/documents/Guide_to_OSCAL-based_FedRAMP_Content.pdf) describes the concepts behind FedRAMP extensions and allowed values. The extensions related to the System Security Plan (SSP) are cited in this document in context of their use.

*These concepts are described in the Guide to OSCAL-based FedRAMP Content.*

**FedRAMP extensions and allowed values are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.**

***Revised FedRAMP Registry Approach***

*The FedRAMP OSCAL Registry was originally provided as a spreadsheet. It now uses the draft OSCAL Extensions syntax and is offered in XML and JSON formats, with a human-readable HTML representation.*

* [*XML Version*](https://github.com/GSA/fedramp-automation/raw/master/dist/content/resources/xml/FedRAMP_extensions.xml)
* [*JSON Version*](https://github.com/GSA/fedramp-automation/raw/master/dist/content/json/FedRAMP_extensions.json)
* [*HTML Version*](https://github.com/GSA/fedramp-automation/raw/master/documents/FedRAMP_extensions.html)