FedRAMP

Dataset Origin & Versioning

Determining Catalog and Profile Origin

usnistgov/OSCAL#961

Alexander Stein

oscal@fedramp.gov

fedramp.gov

GSA

What Do We Have Now?

*As an OSCAL developer, I want to explicitly explain **what dataset** (NIST 800-53, ISO-27001 respectively) and **which version of that dataset** (respectively 4.0 and 5.1; ISO/IEC 27001:2013 and ISO/IEC 27001:2018) is the source of the catalog and resolved profile catalog without using human interpretation of semantic context, or externalized file and directory naming.*

- Metadata (Shared Header) Model
  - version
- Profile Model
  - import field with href attributes
- (Resolved Profile) Catalog Model
  - link field with rel “resolution-source”

Problem Statements

*As an OSCAL developer, I want to explicitly explain **what dataset** (NIST 800-53, ISO-27001 respectively) and **which version of that dataset** (respectively 4.0 and 5.1; ISO/IEC 27001:2013 and ISO/IEC 27001:2018) is the source of the catalog and resolved profile catalog without using human interpretation of semantic context, or externalized file and directory naming.*

1st Order Question

Within a given document, how do we determine the origin (provenance) and that origin's version when referenced in a particular document?

Problem Statements

*As an OSCAL developer, I want to explicitly explain what dataset (NIST 800-53, ISO-27001 respectively) and which version of that dataset (respectively 4.0 and 5.1; ISO/IEC 27001:2013 and ISO/IEC 27001:2018) is the **source of the catalog and resolved profile catalog** without using human interpretation of semantic context, or externalized file and directory naming.*

2nd Order Question

in a *resolved profile catalog*, how do I know the provenance of the catalog and profile that resolved it?

Possible Solutions

*As an OSCAL developer, I want to explicitly explain **what dataset** (NIST 800-53, ISO-27001 respectively) and **which version** of that dataset (respectively 4.0 and 5.1; ISO/IEC 27001:2013 and ISO/IEC 27001:2018) is the source of the catalog and resolved profile catalog without using human interpretation of semantic context, or externalized file and directory naming.*

1st Order Question

Within a given document, how do we determine the origin (provenance) and that origin's version when referenced in a particular document?

Add dataset assembly to the OSCAL metadata model to define this information.

Possible Solutions

*As an OSCAL developer, I want to explicitly explain what dataset (NIST 800-53, ISO-27001 respectively) and which version of that dataset (respectively 4.0 and 5.1; ISO/IEC 27001:2013 and ISO/IEC 27001:2018) is the **source of the catalog and resolved profile catalog** without using human interpretation of semantic context, or externalized file and directory naming.*

2nd Order Question

In a *resolved profile catalog*, how do I know the provenance of the profile the new profile is based off of?

Enhance the profile resolution spec to pass more context data into resolved profiles.

References

- Banghart, Stephen. OSCAL Document ID Linking and Referencing Model