Automation for Distributed Energy Resources Risk Manager using OSCAL

Anuj Sanghvi
Cybersecurity Research Engineer
Paul Wand
Cybersecurity Visualization Engineer
The Distributed Energy Resources Risk Manager

• NREL extended the scope of the DERCF to include the NIST Risk Management Framework (RMF), addressing the challenges faced by federal energy managers when complying with the NIST RMF for DER systems.

• The NIST RMF is a cyclical process designed to incorporate principles of security and risk management into an organization’s system policies and procedures.

• As an additional tool, NREL’s **Distributed Energy Resources Risk Manager (DER-RM)** is independent of the DERCF’s existing self-assessment and allows users to focus on the RMF process.
DER-RM Goals

• **Navigate compliance**
  Manage cybersecurity risk with government requirements in an organized manner

• **Automate requirements**
  Adapt to specific organization needs and present the most aligned templates and recommendations

• **Provide knowledge**
  Apply NIST guidance and DER-RM specific approaches

• **User-friendly interaction**
  Calculate risk score and generate system-specific requirements through real-world examples

Streamline
Organize
Manage
Welcome to Professional DER Cyber Risk Management

The purpose of this application is help you gather the following documents via the RMF Procedure:

- RMF Steps
- Baseline Profile
- Security Plan
- Milestones
- Assessment Plan
Discovering OSCAL

NIST Authors in Bold

Displaying 1 - 8 of 8

A Document-based View of the Risk Management Framework
AUGUST 3, 2020
AUTHOR(S): JOSHUA LUBELL
Cybersecurity professionals know the Risk Management Framework as a rigorous yet flexible process for managing security risk. But the RMF lacks a document focus

The Next Generation Risk Management Framework (RMF 2.0): A Holistic Methodology to Manage Information Security, Privacy and Supply Chain Risk
FEBRUARY 28, 2019
AUTHOR(S): VICTORIA Y. PILLITTERI
This bulletin summarizes the information found in NIST SP 800-37, Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life
The Link Between OSCAL & RMF

A document-based view of the RMF

Illustration from NIST
# The Layers of OSCAL

<table>
<thead>
<tr>
<th>Layer</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment Results Layer</td>
<td>Assessment Results Model</td>
</tr>
<tr>
<td></td>
<td>Plan of Actions &amp; Milestones (POA&amp;M) Model</td>
</tr>
<tr>
<td></td>
<td>Other Assessment Results Models (Future)</td>
</tr>
<tr>
<td>Assessment Layer</td>
<td>Assessment Plan Model</td>
</tr>
<tr>
<td></td>
<td>Assessment Activity Models (Future)</td>
</tr>
<tr>
<td>Implementation Layer</td>
<td>System Security Plan Model</td>
</tr>
<tr>
<td></td>
<td>Component Model</td>
</tr>
<tr>
<td></td>
<td>Other Implementation Models (Future)</td>
</tr>
<tr>
<td>Profile Layer</td>
<td>Profile Model</td>
</tr>
<tr>
<td>Catalog Layer</td>
<td>Catalog Model</td>
</tr>
</tbody>
</table>

*Illustration from NIST*
The Extensible Nature of OSCAL

And why OSCAL is good for automation

Annotated Property

An attribute, characteristic, or quality of the containing object expressed as a namespace qualified name/value pair with optional explanatory remarks. The value of an annotated property is a simple scalar value.

```
   ▼ object {1}
        ▼ annotations [2]
               ▼ 0  {2}
                     name : deployment-model
                     value : private
               ▼ 1  {2}
                     name : service-models
                     value : iaas
```
The Extensible Nature of OSCAL

And why OSCAL is good for automation

FedRAMP Specific Examples

<table>
<thead>
<tr>
<th>FedRAMP Information</th>
<th>Tag Value</th>
<th>Placement as designated by XPath Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Case Workbook Objective</td>
<td>assessment-objective</td>
<td>/*/modify/alter/add</td>
</tr>
<tr>
<td>Data Center</td>
<td>data-center</td>
<td>/*/metadata/location</td>
</tr>
<tr>
<td>Primary Data Center</td>
<td>primary-data-center</td>
<td>/*/metadata/location</td>
</tr>
<tr>
<td>Backup or Alternate Data Center(s)</td>
<td>alternate-data-center</td>
<td>/*/metadata/location</td>
</tr>
<tr>
<td>FIPS 140-2 Validated Component</td>
<td>fips-140-2-validated</td>
<td>/*/system-implementation/component</td>
</tr>
<tr>
<td>False Positive Details</td>
<td>false-positive</td>
<td>/*/results/finding/observation</td>
</tr>
<tr>
<td>Operational Requirement Details</td>
<td>operationally-required</td>
<td>/*/results/finding/observation</td>
</tr>
<tr>
<td>Risk Adjustment Details</td>
<td>risk-adjustment</td>
<td>/*/results/finding/observation</td>
</tr>
</tbody>
</table>

Custom NREL Baselines for DER

Assessment Results Layer
Control Catalog

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations

Control Group Families
- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization

Configuration Management
- Configuration Management Policy and Procedures
- Baseline Configuration
- Configuration Change Control
- Security Impact Analysis
- Access Restrictions for Change
- Configuration Settings
- Least Functionality
- Information System Component Inventory

Configuration Management Plan
- Software Usage Restrictions
- User-Installed Software

Baseline Configuration
- ADD TO BASELINE
- IMPLEMENT CONTROL

Statement
The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Guidance
This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

Objective
Determine if the organization:
OSCAL Input

Accepts forms for manual entry and a JSON endpoint for automation
OSCAL Input

Accepts forms for manual entry and a JSON endpoint for automation.
OSCAL Output

Exports PDF and OSCAL JSON

Source: https://pages.nist.gov/OSCAL/documentation/schema/
Automated Continuous Monitoring

Assessment results layer

### Interface RiskLogEntry

Identifies the result of an action and/or task that occurred as part of executing an assessment plan or an assessment event that occurred in producing the assessment results. Identifies the result of an action and/or task that occurred as part of executing an assessment plan or an assessment event that occurred in producing the assessment results.

#### Hierarchy
- RiskLogEntry

#### Index

##### Properties
- annotations
- description
- end
- links
- logged_by
- props
- related_responses
- remarks
- start
- status_change
- title
- uuid

### Assessment Results Model

- Plan of Actions & Milestones (POA&M) Model
- Other Assessment Results Models (Future)
Automated Continuous Monitoring

Assessment results layer

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RiskLogEntryUniversallyUniqueIdentifier</td>
<td><code>string</code>&lt;br&gt;Uniquely identifies an assessment event. This UUID may be referenced elsewhere in an OSCAL document when referring to this information. A UUID should be consistently used for this schedule across revisions of the document.</td>
</tr>
<tr>
<td>RiskResolutionDeadline</td>
<td><code>string</code>&lt;br&gt;The date/time by which the risk must be resolved.</td>
</tr>
<tr>
<td>RiskStatement</td>
<td><code>string</code>&lt;br&gt;An summary of impact for how the risk affects the system.</td>
</tr>
<tr>
<td>RiskStatus</td>
<td><code>string</code>&lt;br&gt;Describes the status of the associated risk.</td>
</tr>
</tbody>
</table>
Automating Risk Awareness

Combine automated security scanning with OSCAL to send notifications directly to the responsible parties for system components violating security controls.

“Your solar microgrid is vulnerable to a zero-day exploit! Please update.”
Connecting OSCAL to Network Monitoring Solution
Q&A

www.nrel.gov

Contact:
Tami Reynolds – Tami.Reynolds@nrel.gov
Anuj Sanghvi – Anuj.Sanghvi@nrel.gov
Paul Wand – Paul.Wand@nrel.gov