

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.

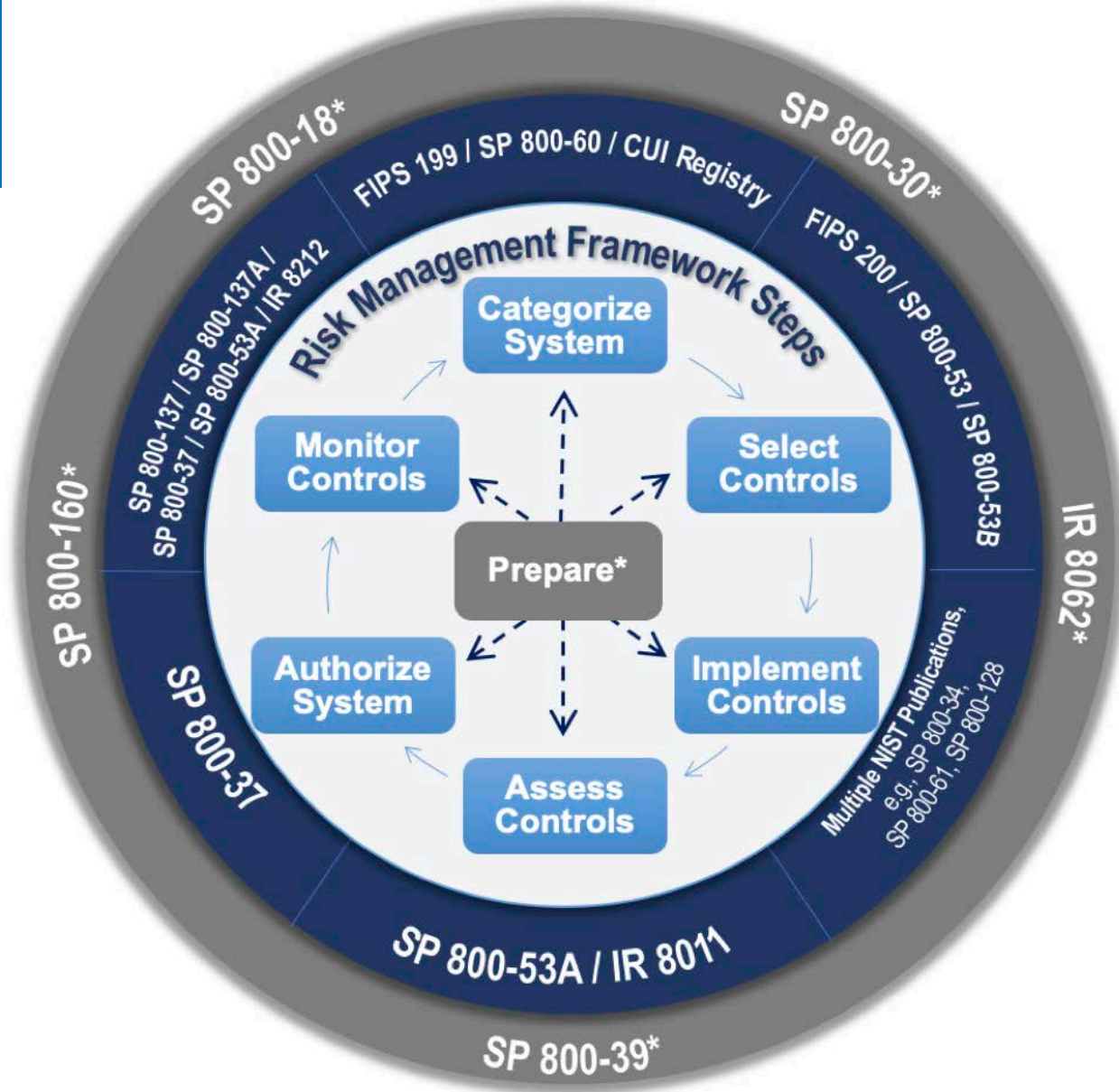


Illustration from NIST

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

DER-RM Prototype

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

The screenshot shows a web browser window displaying the NIST Publications search results for the keyword 'rmf'. The browser's address bar shows the URL: `nist.gov/publications/search?k=rmf&d%5Bmin%5D=&d%5Bmax%5D=&t=&a=&s=All&n=`. The page header includes the NIST logo, a search bar with the text 'Search NIST', and a 'Menu' button. The main content area is titled 'Publications' and features a search filter sidebar on the left. The sidebar contains a search box with 'rmf' entered, a 'Published date' filter with a 'From' input field, and an 'And' filter with a 'To' input field. Below the filters is an 'Advanced search' button with a plus sign. The main content area displays two search results. The first result is titled 'A Document-based View of the Risk Management Framework' by Joshua Lubell, dated August 3, 2020. The second result is titled 'The Next Generation Risk Management Framework (RMF 2.0): A Holistic Methodology to Manage Information Security, Privacy and Supply Chain Risk' by Victoria Y. Pillitteri, dated February 28, 2019.

nist.gov/publications/search?k=rmf&d%5Bmin%5D=&d%5Bmax%5D=&t=&a=&s=All&n=

CyberSecurity/oscal...

An official website of the United States government [Here's how you know](#)

NIST Search NIST Menu

Publications

Search

rmf

Search Title, Abstract, Conference, Citation, Keyword or Author

Published date

From

And

To

Advanced search +

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

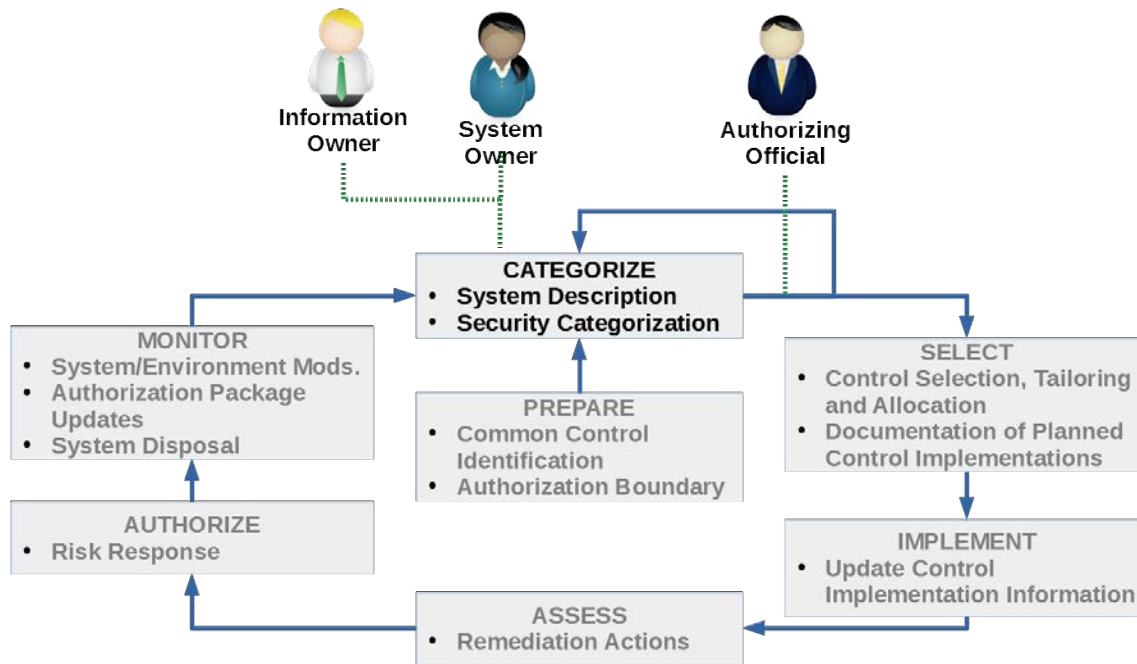
FEBRUARY 28, 2019

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

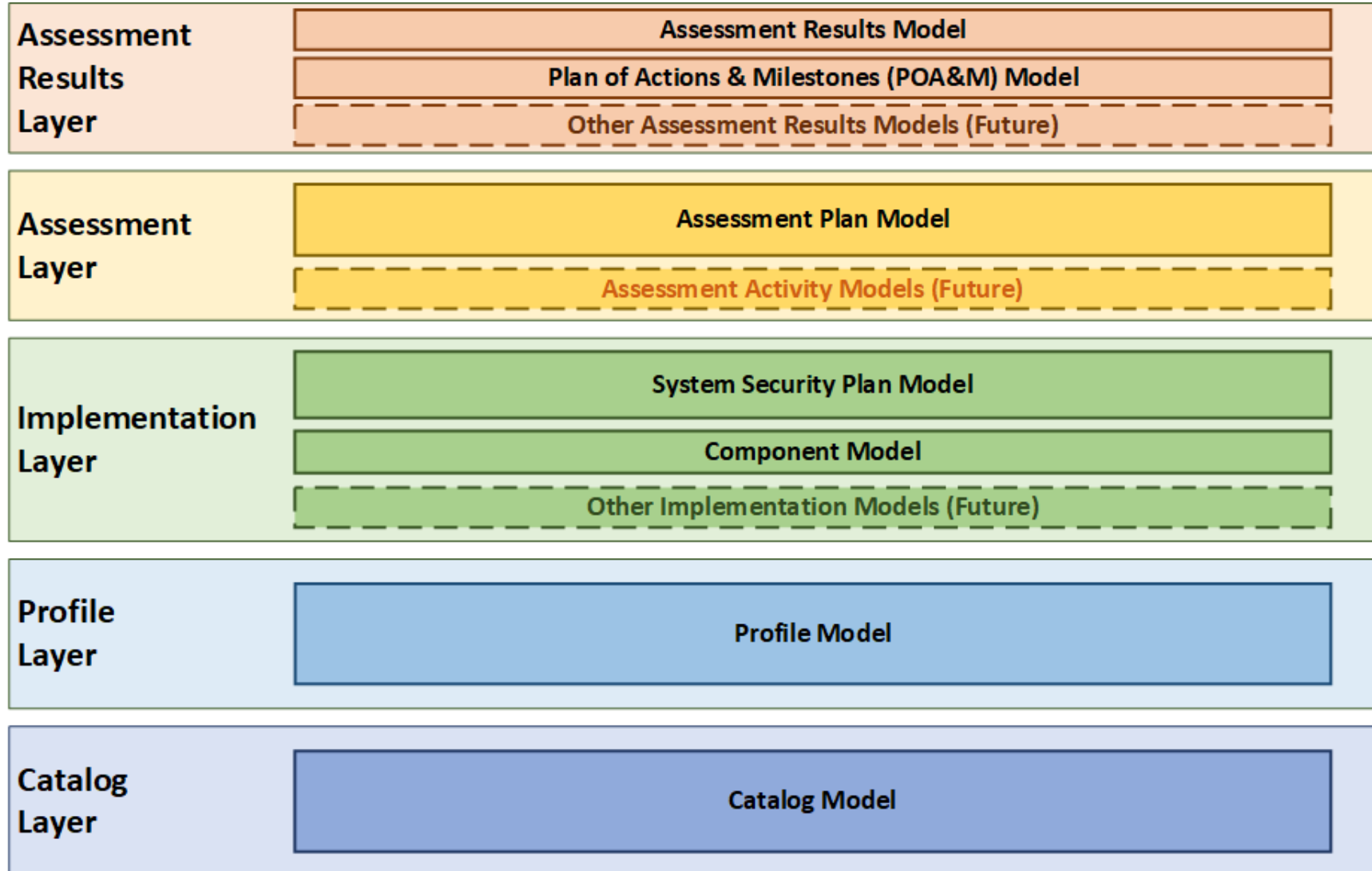
A document-based view of the RMF



system-security-plan	@id	example-ssp
>	metadata	
>	import-profile	
>	system-characteristics	> system-id
		system-name Enterprise Logging and Auditing System
		> description
		> annotation (2 rows)
		security-sensitivity-level moderate
		> system-information
		> security-impact-level
		> status
		> authorization-boundary
>	system-implementation	
>	control-implementation	

Illustration from NIST

The Layers of OSCAL



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

FedRAMP Information		All FedRAMP Compliance tags must use name='conformi ns='https://fedramp.gov/ns/oscal'
Data	Tag Value	Placement as designated by XPath Notation
Test Case Workbook Objective	assessment-objective	<code>/*/modify/alter/add</code>
Data Center	data-center	<code>/*/metadata/location</code>
Primary Data Center	primary-data-center	<code>/*/metadata/location</code>
Backup or Alternate Data Center(s)	alternate-data-center	<code>/*/metadata/location</code>
FIPS 140-2 Validated Component	fips-140-2-validated	<code>/*/system-implementation/component</code>
False Positive Details	false-positive	<code>/*/results/finding/observation</code>
Operational Requirement Details	operationally-required	<code>/*/results/finding/observation</code>
Risk Adjustment Details	risk-adjustment	<code>/*/results/finding/observation</code>

Source: https://github.com/GSA/fedramp-automation/blob/master/documents/FedRAMP_OSCAL_Registry.xlsx

Custom NREL Baselines for DER

Assessment Results Layer

The screenshot displays a web interface for selecting a baseline profile. The left sidebar is organized into sections: RMF (RMF Steps), SYSTEM (Baseline Profile, Security Plan, Milestones), DIRECTORY (Catalog), ASSESSMENT (Assessment Plan, Assessment Results), and HELP. The main content area is titled 'BASELINE PROFILE' and contains a definition of a baseline, followed by three selectable options:

- NIST Special Publication 800-53 Revision 5 HIGH IMPACT BASELINE**
Total Controls: 370
[SELECT](#)
- NIST Special Publication 800-53 Revision 5 MODERATE IMPACT BASELINE**
Total Controls: 287
[SELECT](#)
- NIST Special Publication 800-53 Revision 5 LOW IMPACT BASELINE**
Total Controls: 149
[SELECT](#)

Control Catalog

The screenshot displays a web application interface for a Control Catalog. At the top, there is a navigation bar with a hamburger menu, a home icon, the word "CATALOG", and a list icon. Below the navigation bar, the title "NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations" is shown, along with a small "i" icon on the right.

The interface is divided into three main sections:

- Control Group Families (Left Sidebar):** A vertical list of categories including Access Control, Awareness and Training, Audit and Accountability, Security Assessment and Authorization, Configuration Management (highlighted in green), Contingency Planning, Identification and Authentication, Incident Response, Maintenance, Media Protection, and Physical and Environmental Protection.
- Configuration Management (Main Content Area):** A list of specific controls under the "Configuration Management" heading. The controls listed are: Configuration Management Policy and Procedures, Baseline Configuration (highlighted in blue), Configuration Change Control, Security Impact Analysis, Access Restrictions for Change, Configuration Settings, Least Functionality, Information System Component Inventory, Configuration Management Plan, Software Usage Restrictions, and User-installed Software.
- Baseline Configuration (Detailed View):** A panel showing details for the "Baseline Configuration" control. It includes two buttons: "ADD TO BASELINE" and "IMPLEMENT CONTROL". Below the buttons, there are sections for "Statement" and "Guidance".
 - 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."

OSCAL Input

Accepts forms for manual entry and a JSON endpoint for automation



The screenshot shows the "PREPARE ORGANIZATION" application interface. The top navigation bar includes a home icon, the title "PREPARE ORGANIZATION", and a "ROLES" link. The left sidebar contains a menu with the following items: "Parties" (selected), "Roles", "Organization Strategy", "Baseline", "Common Controls", "Impact Level", and "Monitoring Strategy". The main content area displays the "Party (organization or person)" form. The form includes a description: "A responsible entity, either singular (an organization or person) or collective (multiple persons)". Under "Required Fields", the "Uuid" field is populated with the value "9832749528374952387459238475923847". The "Type" field is set to "Person". Under "Additional Fields", the "Party name" field is populated with "Test person".

OSCAL Input

Accepts forms for manual entry and a JSON endpoint for automation

The screenshot shows a web application interface for entering OSCAL system characteristics. The main heading is "SECURITY PLAN" with a document icon. Below it, the page title is "System Characteristics" with a back arrow. A description states: "Contains the characteristics of the system, such as its name, purpose, and security impact level." The form includes the following fields:

- System ids:** gov-id
- System-name:** Solar Microgrid
- Description:** A vast array of solar panels
- Security Sensitivity Level:** Moderate

At the bottom, there are four buttons for OSCAL components: SYSTEM-INFORMATION, SECURITY-IMPACT-LEVEL, STATUS, and AUTHORIZATION-BOUNDARY. A sidebar on the left contains a menu with items: METAD, IMPOR, SYSTE, SYSTE, CONTR, and BACK-I.

OSCAL Output

Exports PDF and OSCAL JSON

Enterprise Logging and Auditing System Security Plan v

System Characteristics
This is an example of a system that provides enterprise logging and log auditing capabilities.

Security Impact:

- availability-low
- integrity-moderate
- confidentiality-moderate

Logging Server operational

Provides a means for hosts to publish logged events to a central server.

Enterprise Logging, Monitoring, and Alerting Policy operational

Requires all components to send logs to the enterprise logging solution - Requires all components synchronize their time with the appropriate enterprise time service, and at what frequency. - Identifies the events that must be captured - Identifies who is responsible/accountable for performing these functions

System Integration Process operational

Ensures proper integration into the enterprise as new systems are brought into production.

Inventory Management Process operational

Source: <https://pages.nist.gov/OSCAL/documentation/schema/>

Automated Continuous Monitoring

Assessment results layer

Globals / RiskLogEntry /

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

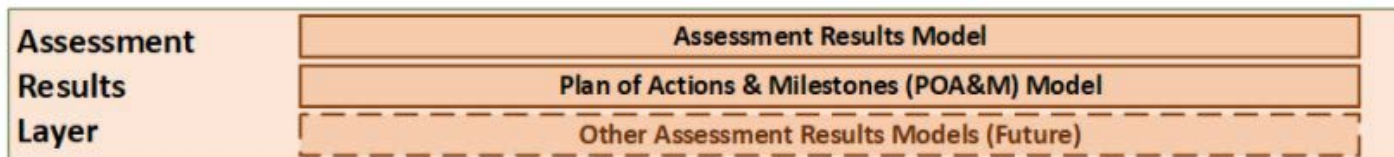
Properties

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

Globals

- 📦 RiskLogEntry
 - annotations
 - description
 - end
 - links
 - logged_by
 - props
 - related_responses
 - remarks
 - start
 - status_change
 - title
 - uuid

Properties



Automated Continuous Monitoring

Assessment results layer

RiskLogEntryUniversallyUniqueIdentifier

T RiskLogEntryUniversallyUniqueIdentifier: *string*

Defined in *src/poam/index.ts:214*

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.

RiskResolutionDeadline

T RiskResolutionDeadline: *string*

Defined in *src/poam/index.ts:188*

The date/time by which the risk must be resolved.

RiskStatement

T RiskStatement: *string*

Defined in *src/shared/IdentifiedRisk.ts:36*
Defined in *src/poam/index.ts:148*

An summary of impact for how the risk affects the system. An summary of impact for how the risk affects the system.

RiskStatus


T RiskStatus: *string*

Defined in *src/poam/index.ts:226*

Describes the status of the associated risk.

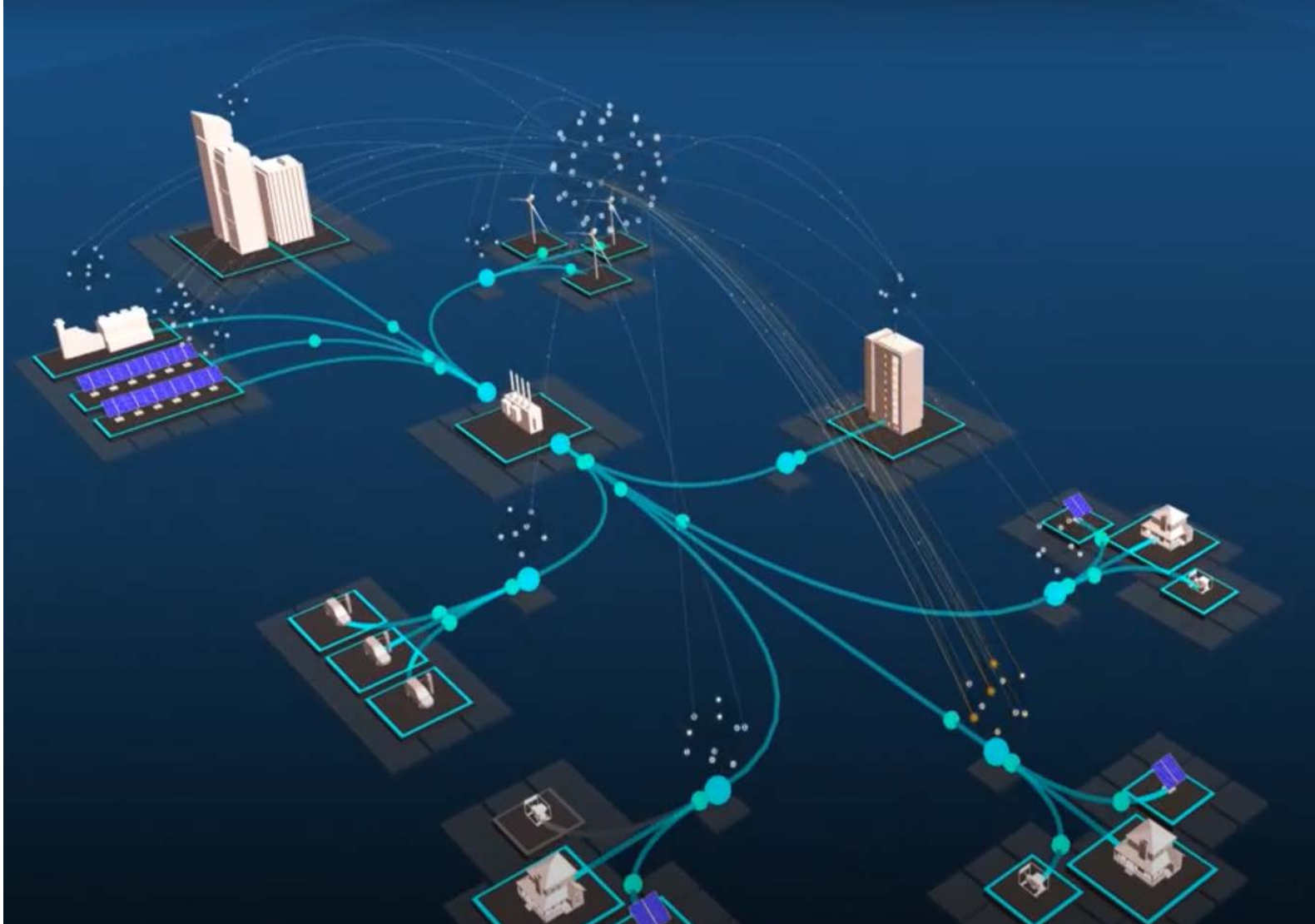
Automating Risk Awareness

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

