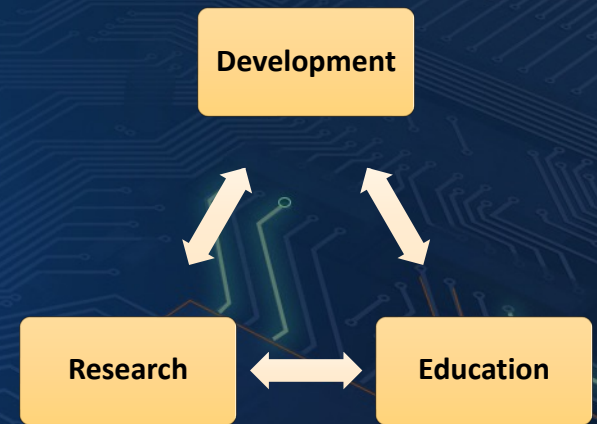


OSCAL DEFINE

Develop Enhancements, Future Implementations and New Education



NIST

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Information Technology Laboratory
Computer Security Division

What is this meeting about?

OSCAL DEFINE

Third Thursday of every month
11:00 AM ET

<https://pages.nist.gov/OSCAL/contribute/define-meeting/>

- Summarize current research efforts.
- Present findings from recent efforts.
- Gather feedback and input.

Discussion is vital.

Our goal is deeper understanding. Please help us to:

- ✓ **Ensure** that everyone feels welcome.
- ✓ **Encourage** sharing of individual perspectives and experiences.
- ✓ **Allow** everyone space to join in, as well as to finish speaking.
- ✓ **Ask** questions that expand ideas or uncover gaps.

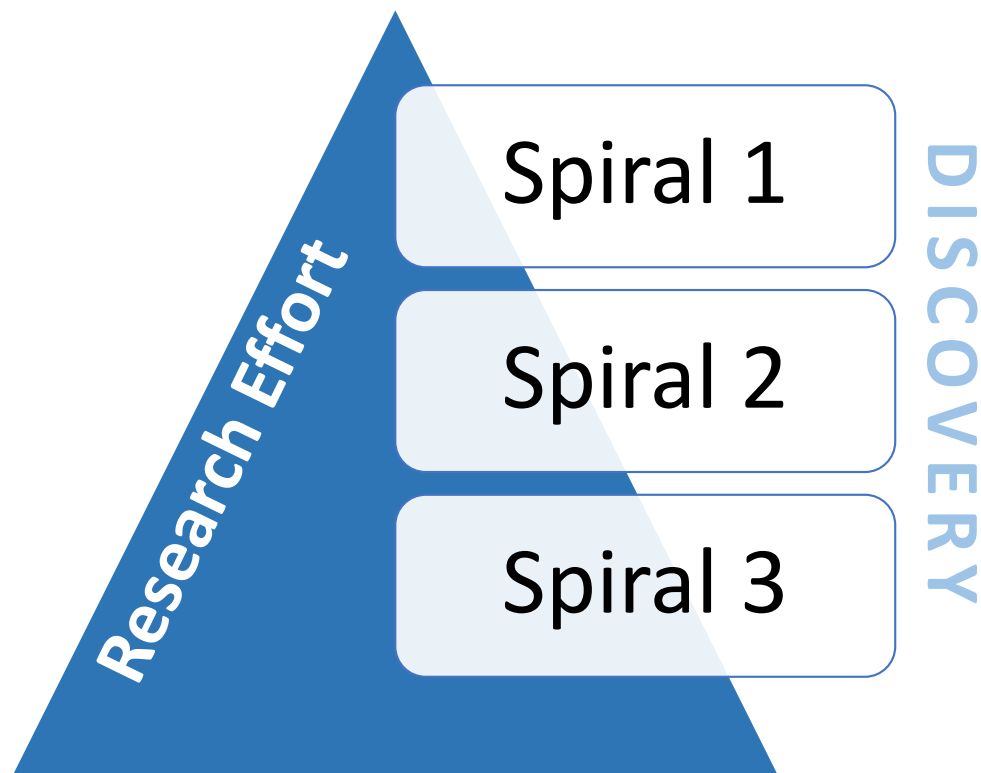
Research is essential.

Our goal is better decision-making. We are seeking:

- ✓ **Documentation** of concepts requiring thought and discovery.
- ✓ **Feedback** as a contribution to the best approach or alternatives.
- ✓ **Problem Statements** as catalysts for the future of OSCAL.
- ✓ **Time** to consider all input and to make informed decisions.

<https://github.com/usnistgov/OSCAL-DEFINE>

Research Efforts & Spirals

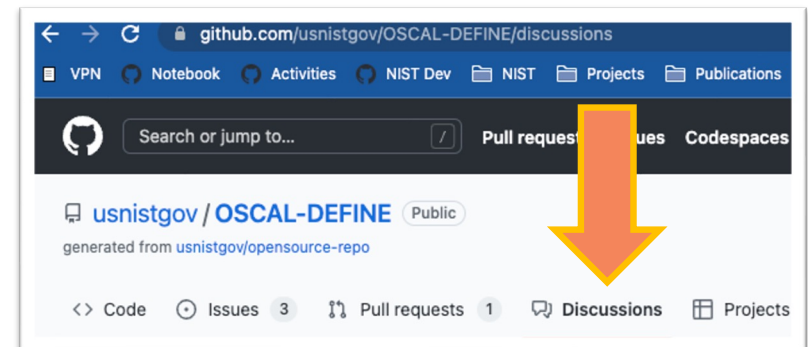


Knowledge and understanding is gained through each spiral.

What is today's agenda?

- Summary of OSCAL Issues for Research
- Review of Efforts
 - Control Mapping
(OSCAL-DEFINE/discussions/14)
 - Responsibility Modeling
(OSCAL-DEFINE/discussions/13)
- Questions and Open Discussion
- Upcoming Meetings

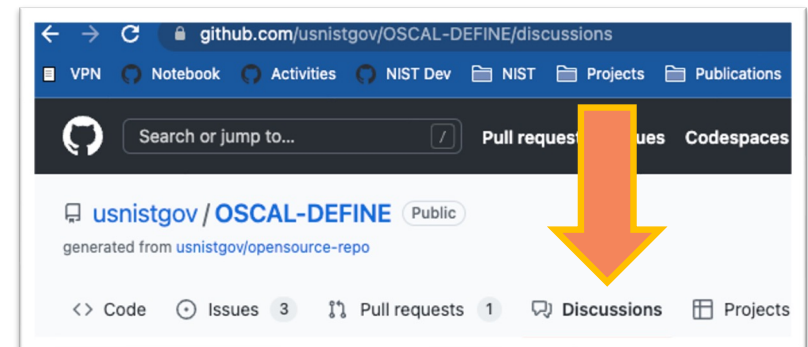
Your feedback and input is encouraged!



A few notes.

- Recording for Research Participation and Collaboration
- Where we are:
 - Session 1: Intro to DEFINE
 - Session 2: Responsibility Modeling
 - **Session 3: Today**
- **Remember Discussions!**
 - Subscribe where interested.
 - Feedback when possible.

Your feedback and input is encouraged!



OSCAL DEFINE



Research Backlog

NIST

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Information Technology Laboratory
Computer Security Division

Research Backlog

Category	General Characterization	Count
 Responsibility and Mapping Models	Current research focus.	4
 Component Definition	Emerging as a focus due to a number of questions and perceptions around its use.	4
New or Modified Models	Issues focused on new or modified models. Includes metrics/rules work.	7
Approaches and Tools	Implementation specific and similar issues. May still desire modifications to model assemblies.	11
Rendering and Interaction	Issues focused on rendering OSCAL content or products.	5
Fragmented or Partial Content	Issues focused on use of fragments of OSCAL content.	4
Example and Learning	Issues that are most relative to demonstration of concepts using OSCAL.	5

OSCAL DEFINE

Spiral 1: Coming Soon

Control Mapping Effort (Soon)

Control Mapping Effort

Notes:

-

- ❖ **Open the Effort, Initiation and Discovery**
- ❖ **Spiral 1: Summary of input and findings (May)**
- ❖ **Spiral 2: Draft of updates to model (June)**

Control Mapping Effort

Notes:

-

- ✓ **Discussion is open. Comments welcome.**
- ✓ **Discussion panel at OSCAL Conference in May.**

OSCAL DEFINE

Spiral 3: Export Examples

Responsibility Modeling Effort

Responsibility Modeling Effort

Notes:

-

- ❖ **Spiral 3: Closing this week with addition**
- ❖ **Synthetic control response content (May)**
- ❖ **Spiral 4: Draft model (June)**

Spiral 3: Export Examples

```
control-implementation:
  implemented-requirements:
    - uuid: NISTDEMO-IR01-0000-0000-000000000000
      control-id: pe-11
      by-components:
        - component-uuid: NISTDEMO-BC01-0000-0000-000000000000
          uuid: NISTDEMO-CD01-0000-0000-000000000000
          description: >-
            The infrastructure is supported by multiple uninterruptible power supplies, and a redundant
            backup generator system capable of continuous operation for an extended period of time.
          # Implementation Status Assembly
          implementation-status:
            - state: implemented
              remark: "Optional communication of intent"
          # Export Assembly
          export:
            description: Infrastructure as a Service - This is actually the redacted content to share for the control.
          responsibilities:
            - uuid: NISTDEMO-RES1-0000-0000-000000000000
              provided-uuid: NISTDEMO-PRO1-0000-0000-000000000000
              description: >-
                Customer fully inherits this control from the Cloud Service Provider (CSP).
          provided:
            - uuid: NISTDEMO-PRO1-0000-0000-000000000000
              description: >-
                Customers do not have physical access to any system resources in Provider datacenters.
```

OSCAL DEFINE

Spiral 4: Model Draft

Responsibility Modeling Effort

Spiral 4: Model Draft

Notes:

- ❖ **We are ready to start a draft. (Spiral 4)**
- ❖ What do we need?
- ❖ What do we wish it could do?
- ❖ How should it look?

Interested/Input: chris.compton@nist.gov

Questions?

NIST | NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Information Technology Laboratory
Computer Security Division



NIST

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

May 23-24, 2023: 4th OSCAL Conference

Save the Dates

AUTOMATION

Herbert C. Hoover Federal Building
1401 Constitution Avenue, NW, Washington

May 24-25, 2023: 4th Multi-cloud Conference

Zero Trust and High Assurance for
Cloud-Native Applications





Open Security Controls Assessment Language (OSCAL)

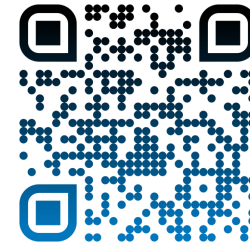


OSCAL DEFINE:

May 18, 2023 @ 11:00 AM EDT

OSCAL Model Engineering:

May 4, 2023 @ 10:00 AM EDT



oscal@nist.gov

