Security Automation Simplified

oscalfoundation.org

Collaborative Maturation of OSCAL Models

A Team Effort

oscalfoundation.org

OSCAL FOUNDATION

- The OSCAL Foundation
- Standards Development – A Team Effort
- History of the Mapping Model
- What We've Accomplished
- Get Involved

Who am I?

Stephen Banghart

- OSCAL Foundation’s Technical Coordinator, leading the Foundation’s technical OSCAL development work.
- Member of the original team at NIST that created and developed OSCAL.
- Worked in Standards Developing Organizations (SDOs) around the world on technical and non-technical standards.
- Joined by the rest of the Foundation staff and our Foundation membership to work towards OSCAL’s continued success.

OSCAL Foundation

What is the OSCAL Foundation?

The OSCAL Foundation is a non-profit founded to centralize and coordinate the larger OSCAL community. The foundation helps facilitate the adoption, education, development, internationalization, and extension of OSCAL.

Our Mission

Adoption

Encouraging end users and vendors to implement and support OSCAL, including advocating for its use in regulatory use cases

Education

Providing educational materials, tutorials, examples, walkthroughs, and webinars to teach about the value of OSCAL and tips to get started implementing it

Development

The Foundation is leading efforts to continue developing and maturing the OSCAL models in partnership with NIST

Internationalization

Working towards broader international support of OSCAL, the Foundation engages with non-US organizations

Extension

The Foundation works with stakeholders to identify opportunities to extend the OSCAL models.

Standards - A Team Effort

- Standards development is, and always has been, a team effort.
- Technical standards like OSCAL only exist in the first place because we all want to interoperate with each other, after all.
- NIST has been leading open and community driven collaborative development of OSCAL for years, and OSCAL's success owes much to that approach.
- What does this process look like? How does it work and who does it involve? And most importantly, what if you wanted to get involved and help shape OSCAL?

Getting involved in any standards work, OSCAL included, is easier than you think!

A General Timeline

Use Case

- An OSCAL user has a use case that OSCAL does not support out of the box.

Implementation

- The user implements a custom solution to their problem.
- This may be an extension to the model or some new behavior.

Introduction

- The user introduces their use case and implementation to the community.

Collaborative Development

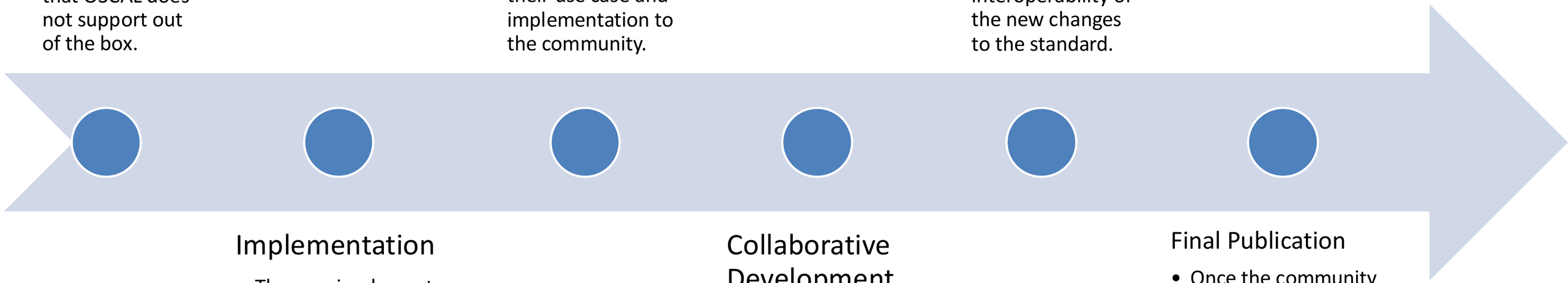
- If accepted, the community collaboratively works to integrate the use case into OSCAL, pulling from the existing implementation where possible.

Prototyping and Testing

- The community examines the functionality and interoperability of the new changes to the standard.

Final Publication

- Once the community reaches consensus, the changes are submitted to the maintainer (NIST) for approval.

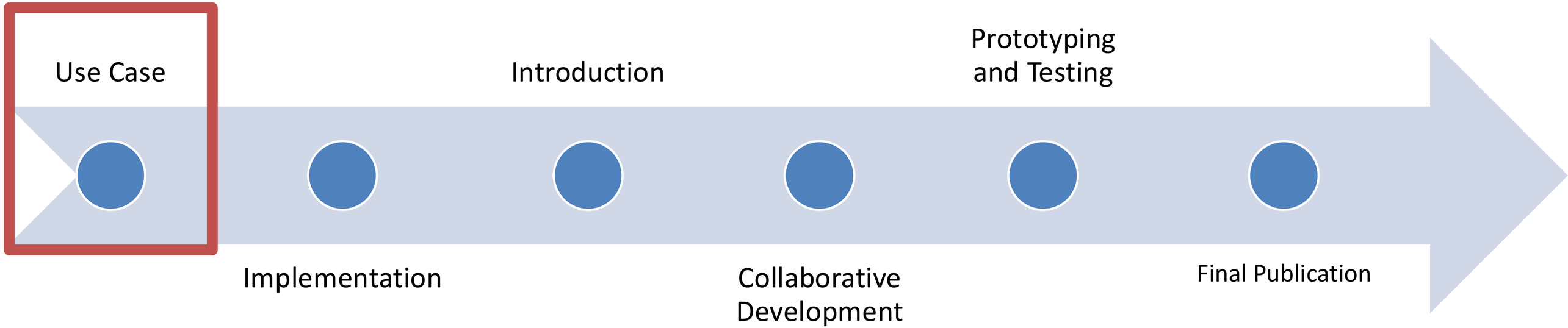


Standards - A Team Effort

- Sometimes use cases are introduced without an implementation. This is ok! Its still worth raising ideas, they will often resonate with others that have similar use cases.
  - An implementation *does* often make it easier/faster to iterate and develop once work is underway.

- Let’s jump to the topic of this presentation, the Mapping Model, and discuss how it fits into what we’ve discussed so far.

A Specific Timeline: The Mapping Model



Mapping Model: Use Case

- Creating a “mapping” or a “crosswalk” is a well-established activity wherever overlapping frameworks are relevant simultaneously.

- For example, an organization that is fully compliant with some NIST 800-53 baseline wants to know to what extent they are compliant with PCI DSS 4.0.
  - Or perhaps we want to understand how some framework “maps” or compares against some number of other frameworks.

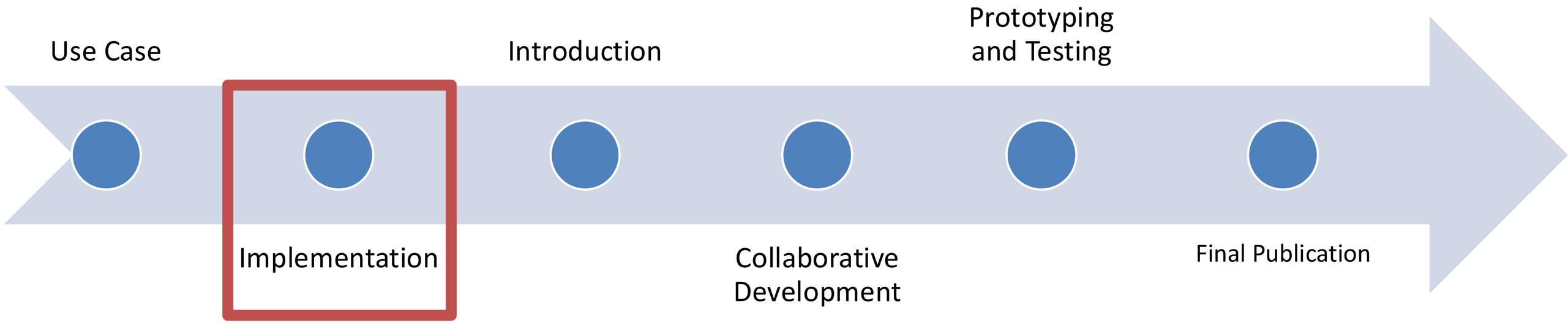
- If we could do that mapping in OSCAL – we could provide a machine-readable and actionable way of defining these mappings. All the work we’ve done setting up OSCAL for a specific framework could be applied to multiple.

- The OSCAL Compass team recognized this use case!

Mapping Model: Use Case

- OSCAL Mapping enables and enhances several new use cases:
  - Constructing a custom internal control framework to capture enterprise posture, then mapping that custom framework out to other requirements to demonstrate coverage.
  - Third-party analysts creating extensive and data rich stand alone mappings encoding the relationships between frameworks
  - Providing the connective tissue to automatically demonstrate the relationship between technical control implementations and some newly introduced controls or requirements.

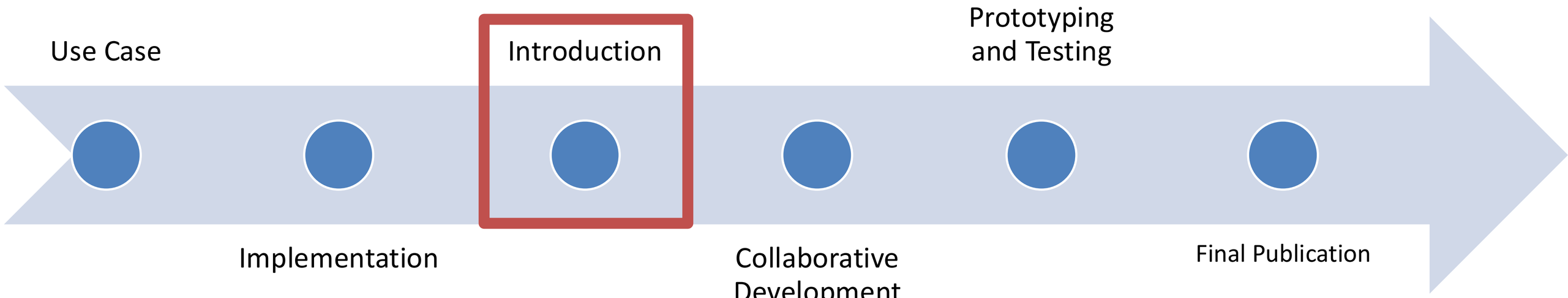
A Specific Timeline: The Mapping Model



Mapping Model: Implementation

- A way of doing this in OSCAL was developed in partnership with NIST as part of the oscal-compass open-source project.
- They developed this capability as an extension to OSCAL, a new type of document. This meant it didn’t break any existing OSCAL implementations.
- The prototype model was hosted by NIST to make it easier to share with other stakeholders.

A Specific Timeline: The Mapping Model



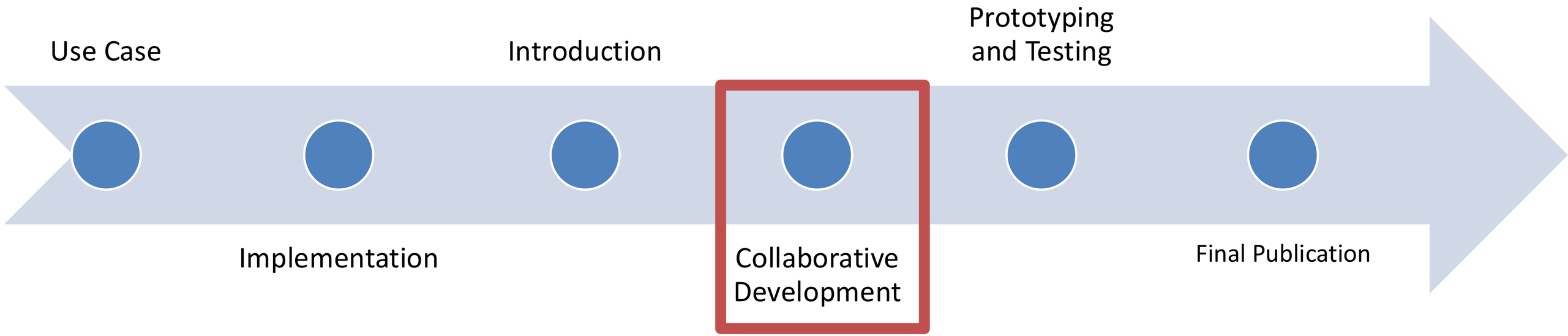
Mapping Model: Introduction

- The OSCAL Compass team socialized their work, both the extension to OSCAL and their implementation, through presentations and discussions at relevant forums.

- This use case resonated with the OSCAL Foundation Technical Working Group (TWG), and its value was clear, so we coordinated industry to provide more concentrated input/feedback on the model.

- We worked with NIST’s prototype model to mature and enhance it, and to build community consensus.

A Specific Timeline: The Mapping Model



Mapping Model: Collaborative Development and Beyond

- The TWG has been hard at work as part of a collaborative process to mature this mapping model.
- This means lots of conversations, discussions, examples, and technical work.
- Requires a delicate balance: the goal is a result that meets the original use case while also supporting as many other closely related use cases as possible.
- I'll leave the details of this work to my colleagues!
- Next up, we focus on testing and examples to prove interoperability and applicability, then its off to (hopefully) our final step.

Mapping Model: The Work Continues

- But the work doesn’t stop at the end of our timeline!
- We can continue improving and iterating, and new use cases may show up that require adjustments.
- And of course, entirely new use cases and implementations start new projects entirely.

Get Involved!

- This example of the mapping model started because individuals saw a use case, thought about how OSCAL could be applied to, then started sharing that idea.

- It’s a relatively small place to start, but it can have a big impact.

- Get involved!
  - OSCAL Foundation
  - OSCAL Compass
  - NIST OSCAL Community

It's my pleasure to introduce two OSCAL Foundation members that have been instrumental to the Mapping Model work:

Anca Sailer, Distinguished Engineer, IBM Research

and

Vikas Agarwal, Senior Technical Staff Member, IBM Research - India

Anca and Vikas have pioneered the mapping model work and are responsible for much of the model as it exists today.

OSCAL Foundation

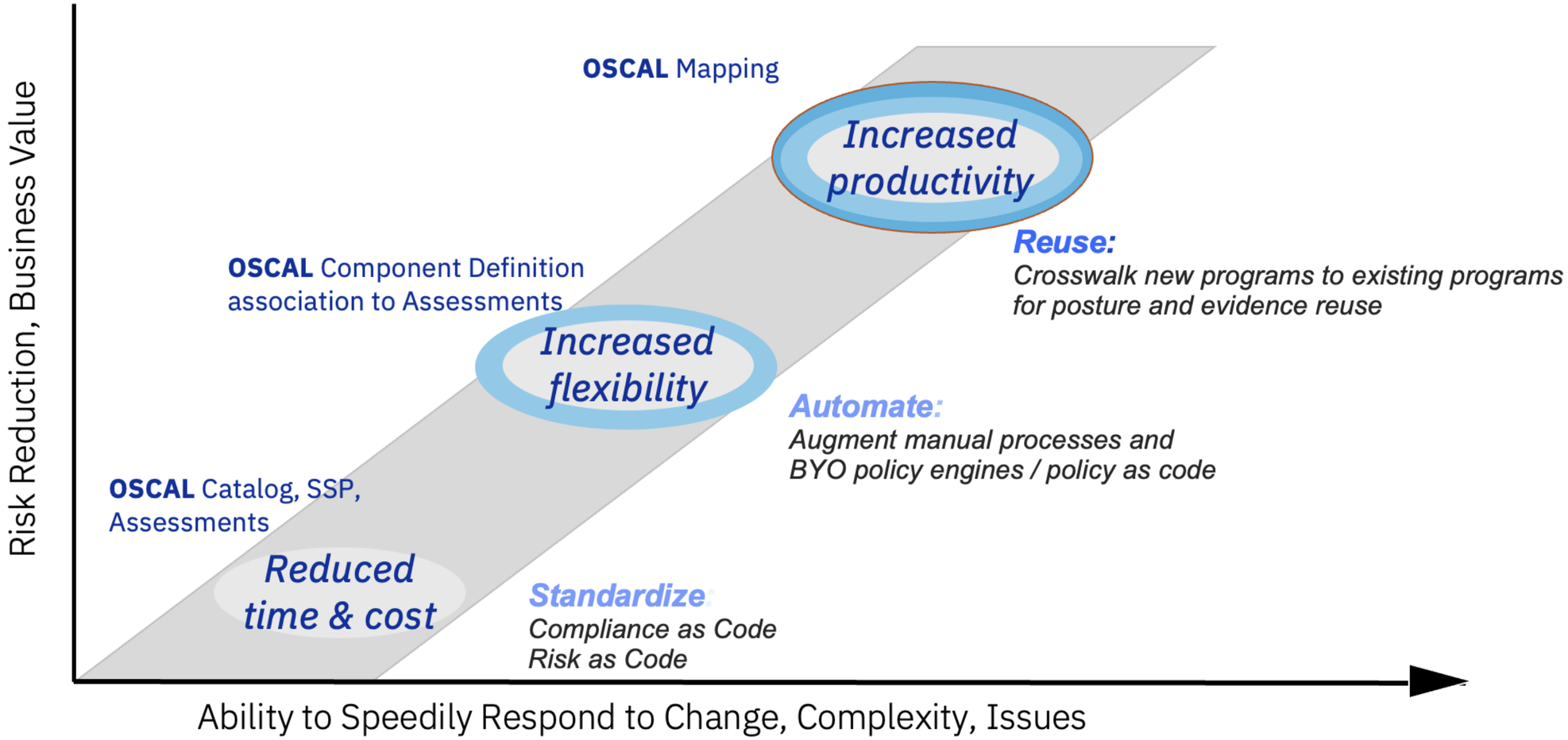
For more information, contact:

Stephen Banghart
sbanghart@oscalfoundation.org

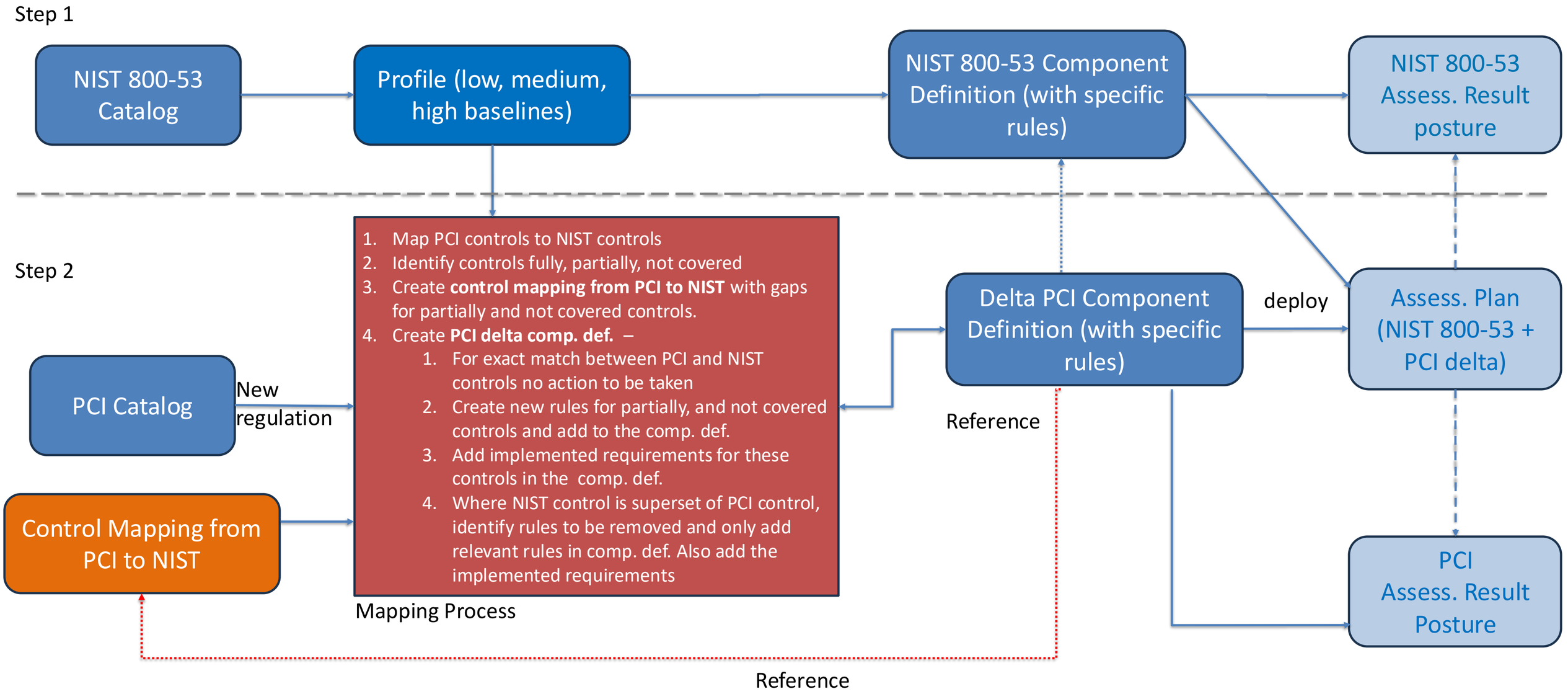
Collaboratively Maturing the OSCAL Control Mapping Model at the OSCAL Foundation

Anca Sailer, Distinguished Engineer, IBM Research
Stephen Banghart, Technical Coordinator, OSCAL Foundation
Vikas Agarwal, Senior Technical Staff Member, IBM Research - India

OSCAL Evolution & Phases of Adoption



Direct Mapping Process



NIST Prototype Mapping Model Schema

```
▼ mapping-collection [1]: {
      uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▼ provenance [1]: {
          method [1]: string,
          matching-rationale [1]: string,
          status [1]: string,
          confidence-score [1]: string,
          mapping-description [1]: markup-multiline,
        ▶ responsible-parties [0 or 1]: [ … ],
          remarks [0 or 1]: markup-multiline
      },
```

```
▼ mappings [1]: [
      Array members, or a singleton mapping object [1 to ∞] {
          uuid [1]: uuid,
        ▶ source-resource [1]: { … },
        ▶ target-resource [1]: { … },
        ▼ maps [1]: [
              An array of map objects [1 to ∞] {
                  uuid [1]: uuid,
                  ns [0 or 1]: uri,
                  matching-rationale [0 or 1]: string,
                  relationship [1]: token,
                ▶ sources [1]: [ … ],
                ▶ targets [1]: [ … ],
                ▶ qualifiers [0 or 1]: [ … ],
                ▶ props [0 or 1]: [ … ],
                ▶ links [0 or 1]: [ … ],
                  remarks [0 or 1]: markup-multiline
              }
          ]
      }
  ],
▶ source-gap-summary [0 or 1]: { … },
▶ target-gap-summary [0 or 1]: { … },
▶ back-matter [0 or 1]: { … },
}
```

https://pages.nist.gov/OSCAL-Reference/models/prototype-mapping-model/mapping/json-outline/

Example: PCI-DSS to NIST 800-53 (w/ existing posture)


```
mapping-collection:
  uuid:                  "0c914f7e-7302-4283-8071-d525bbbb8506"
  metadata:
    title:               "Mapping collection for PCI 4.0 to NIST 800-53 rev 5"
    last-modified:       "2025-07-11T19:35:38+00:00"
    version:             "V1.0"
    oscal-version:       "1.1.3"
  provenance:
    method:
      value:             "semi-automated"
      ns:                "https://oscal-compass.github.io/compliance-trestle/schemas/oscal/mapping"
    matching-rationale:  "semantic"
    status:              "draft"
    confidence-score:
      score:             "0.90"
      description:       "confident about this mapping"
    coverage:            "0.65"
    mapping-description: "This contains semantic mappings from PCI 4.0 to NIST 800-53 rev5"
```

Example: PCI-DSS to NIST 800-53 (w/ existing posture)


```
mappings:
  0:
    uuid:                 "f730ab92-5aec-4b0f-a671-ace32669d56d"
    source-resource:      { type: "catalog", href: "catalogs/PCI-4.0/catalog.json" }
    target-resource:      { type: "catalog", href: "catalogs/NIST_SP-800-53_rev5/catalog.json" }
    maps:
      0:
        uuid:             "16c3ce2c-8e99-4e4e-b3f3-11c6318c23a1"
        method:           { value: "semi-automated", ns: "https://oscal-compass.github.io/complian
        matching-rationale: "functional"
        confidence-score: { score: "0.95", description: "very confident about this mapping" }
        coverage:         "1.0"
        relationship:     "equivalent-to"
        sources:
          0:              { type: "control", "id-ref": "PCI-1.1.1" }
        targets:
          0:              { type: "control", "id-ref": "sc-1" }
      1:
        uuid:             "32f3615c-8d03-45c3-946e-f47c605b55f5"
        method:           { value: "semi-automated", ns: "https://oscal-compass.github.io/complian
        matching-rationale: "functional"
        confidence-score: { score: "0.95", description: "very confident about this mapping" }
        coverage:         "0.80"
        relationship:     "intersects-with"
        sources:
          0:              { type: "control", "id-ref": "PCI-1.1.2" }
        targets:
          0:              { type: "control", "id-ref": "ac-1" }
          1:              { type: "control", "id-ref": "sc-1" }
```

```
source-gap-summary:
  uuid:                   "32cd8b2a-1718-445f-97fa-3951d59eb60b"
  unmapped-controls:
    with-ids:
      0:                  "PCI-10.3.4"
      1:                  "PCI-10.4.1.1"
      2:                  "PCI-10.4.2.1"
      3:                  "PCI-11.5.2"
      4:                  "PCI-12.4.2.1"
      5:                  "PCI-12.6.3.2"
      6:                  "PCI-12.10.4.1"
```

OSCAL Foundation proposals

```
▼ mapping-collection [1]: {
      uuid [1]: uuid,
    ▶ metadata [1]: { … },
    ▼ provenance [1]: {
          method [1]: string,
          matching-rationale [1]: string,
          status [1]: string,
          confidence-score [1]: string,
          mapping-description [1]: markup-multiline,
        ▶ responsible-parties [0 or 1]: [ … ],
          remarks [0 or 1]: markup-multiline
      },
```

```
▼ mapping-collection:
    uuid:                "0c914f7e-7302-4283-8071-d525bbbb8506"
  ▼ metadata:
      title:             "Mapping collection for PCI 4.0 to NIST 800-53 rev 5"
      last-modified:     "2025-07-11T19:35:38+00:00"
      version:           "V1.0"
      oscal-version:     "1.1.3"
  ▼ provenance:
    ▼ method:
        value:           "semi-automated"
        ns:              "https://oscal-compass.github.io/compliance-trestle/schemas/oscal/mapping"
      matching-rationale: "semantic"
      status:            "draft"
    ▼ confidence-score:
        score:           "0.90"
        description:     "confident about this mapping"
      coverage:          "0.65"
      mapping-description: "This contains semantic mappings from PCI 4.0 to NIST 800-53 rev5"
```

User-defined methods with namespace

Numeric confidence score with description

Overall mapping coverage

OSCAL Foundation proposals (contd…)

Optional method
(overrides one in provenance)

```
▼ mappings [1]: [
    Array members, or a singleton mapping object [1 to ∞] {
      uuid [1]: uuid,
    ▶ source-resource [1]: { … },
    ▶ target-resource [1]: { … },
    ▼ maps [1]: [
        An array of map objects [1 to ∞] {
          uuid [1]: uuid,
          ns [0 or 1]: uri,
          matching-rationale [0 or 1]: string,
          relationship [1]: token,
        ▶ sources [1]: [ … ],
        ▶ targets [1]: [ … ],
        ▶ qualifiers [0 or 1]: [ … ],
        ▶ props [0 or 1]: [ … ],
        ▶ links [0 or 1]: [ … ],
          remarks [0 or 1]: markup-multiline
        }
      ]
    }
  ],
```

```
▼ mappings:
  ▼ 0:
      uuid:                "f730ab92-5aec-4b0f-a671-ace32669d56d"
    ▶ source-resource:     { type: "catalog", href: "catalogs/PCI-4.0/catalog.json" }
    ▶ target-resource:     { type: "catalog", href: "catalogs/NIST_SP-800-53_rev5/catalog.json" }
    ▼ maps:
      ▼ 0:
          uuid:            "16c3ce2c-8e99-4e4e-b3f3-11c6318c23a1"
        ▶ method:          { value: "semi-automated", ns: "https://oscal-compass.github.io/complian
          matching-rationale: "functional"
        ▶ confidence-score: { score: "0.95", description: "very confident about this mapping" }
          coverage:        "1.0"
          relationship:    "equivalent-to"
        ▼ sources:
          ▶ 0:             { type: "control", "id-ref": "PCI-1.1.1" }
        ▼ targets:
          ▶ 0:             { type: "control", "id-ref": "sc-1" }
```

Optional confidence score for each control mapping

Optional control coverage

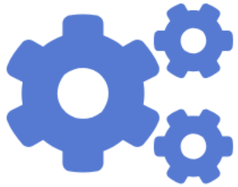
Next Steps

- Finalize the changes to the Mapping model
  - discussions in the OSCAL Foundation technical working group
- Create examples based on the proposed changes
- Update the OSCAL Metaschema
  - Create PR on NIST OSCAL github
- NIST to update the metaschema and create a new release of OSCAL models with Mapping model included

OSCAL Foundation

Where To Start

- Get involved
- Bring your use-cases and examples
- Share your needs
- Collectively mature the mapping model



Technical Working Group (TWG)

The TWG advances the core technical mission of the foundation to develop, improve, and extend the OSCAL standard and the OSCAL ecosystem. The group may work on the development of open source tools, submit collaborative code to NIST, and develop and register OSCAL extension modules and namespaces. Join the TWG here or send an email to technical-working-group+subscribe@oscalfoundationlists.org.