RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: GRC-F01

SECURITY AUTOMATION SIMPLIFIED VIA NIST OSCAL: WE’RE NOT IN KANSAS ANYMORE

David Waltermire

Security Automation Architect
National Institute of Standards and Technology (NIST)

Anil Karmel

Co-Founder and CEO
C2 Labs
@anilkarmel

Agenda

- We’re not in Kansas anymore
- NIST OSCAL: Technical Overview
- Where does the yellow brick road lead?
- Live Demo
- Why does this matter?
- Q&A

WE’RE NOT IN KANSAS ANYMORE

Why OSCAL?

Information Technology is complex

Security Vulnerabilities are everywhere

Regulatory Frameworks are burdensome

Risk Management is hard

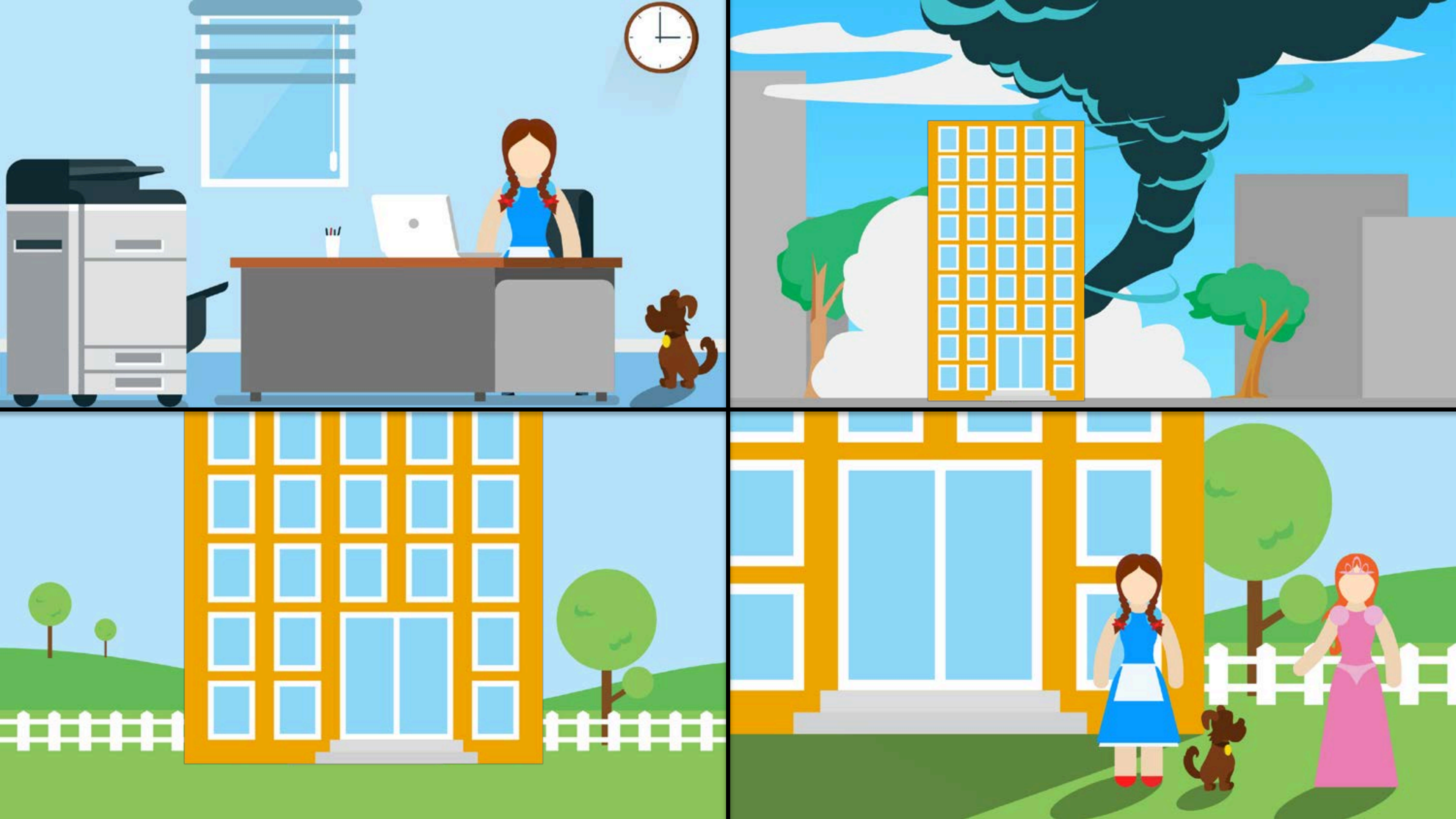
Documentation is out of date

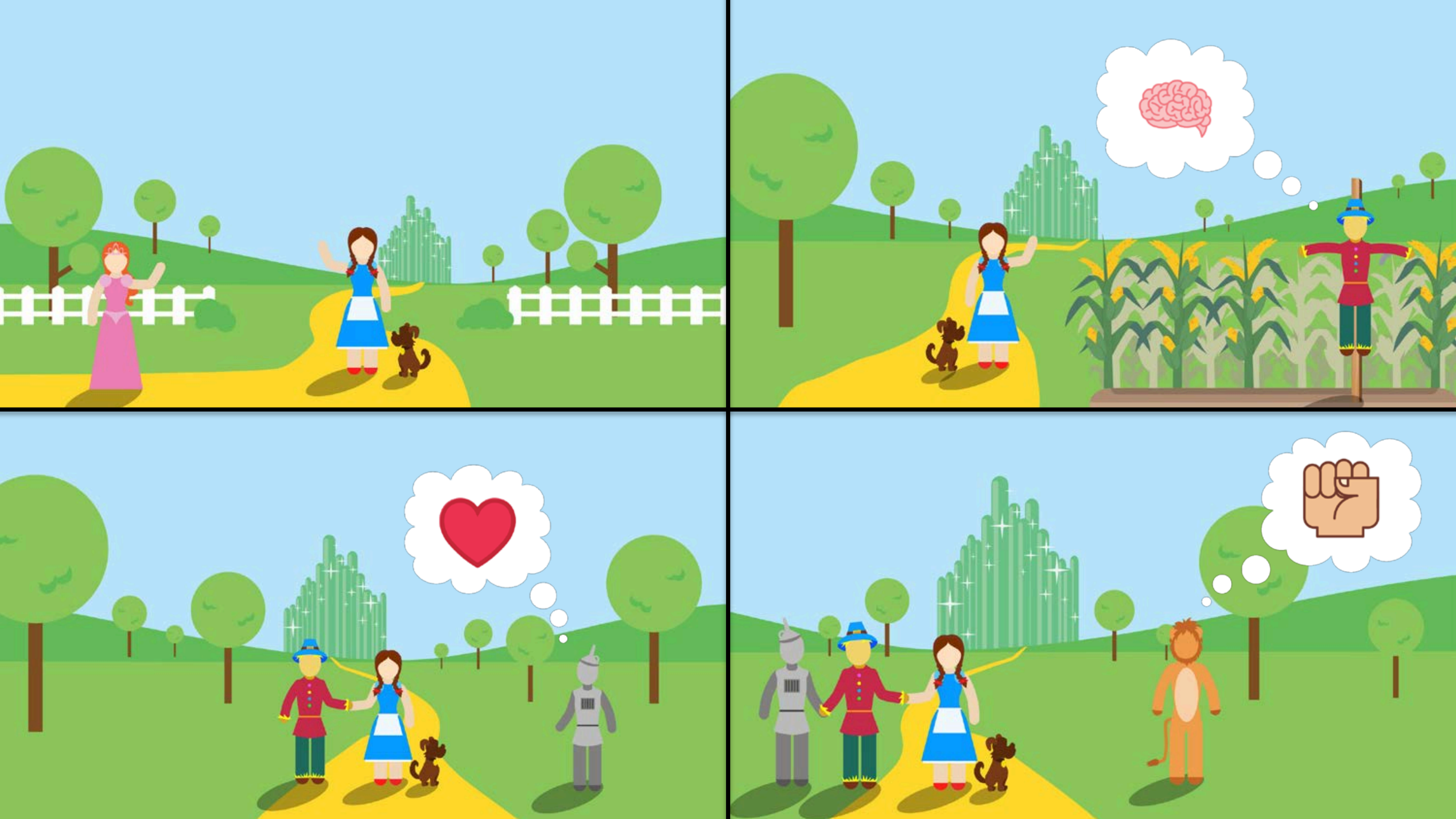
Major challenges in security controls assessment

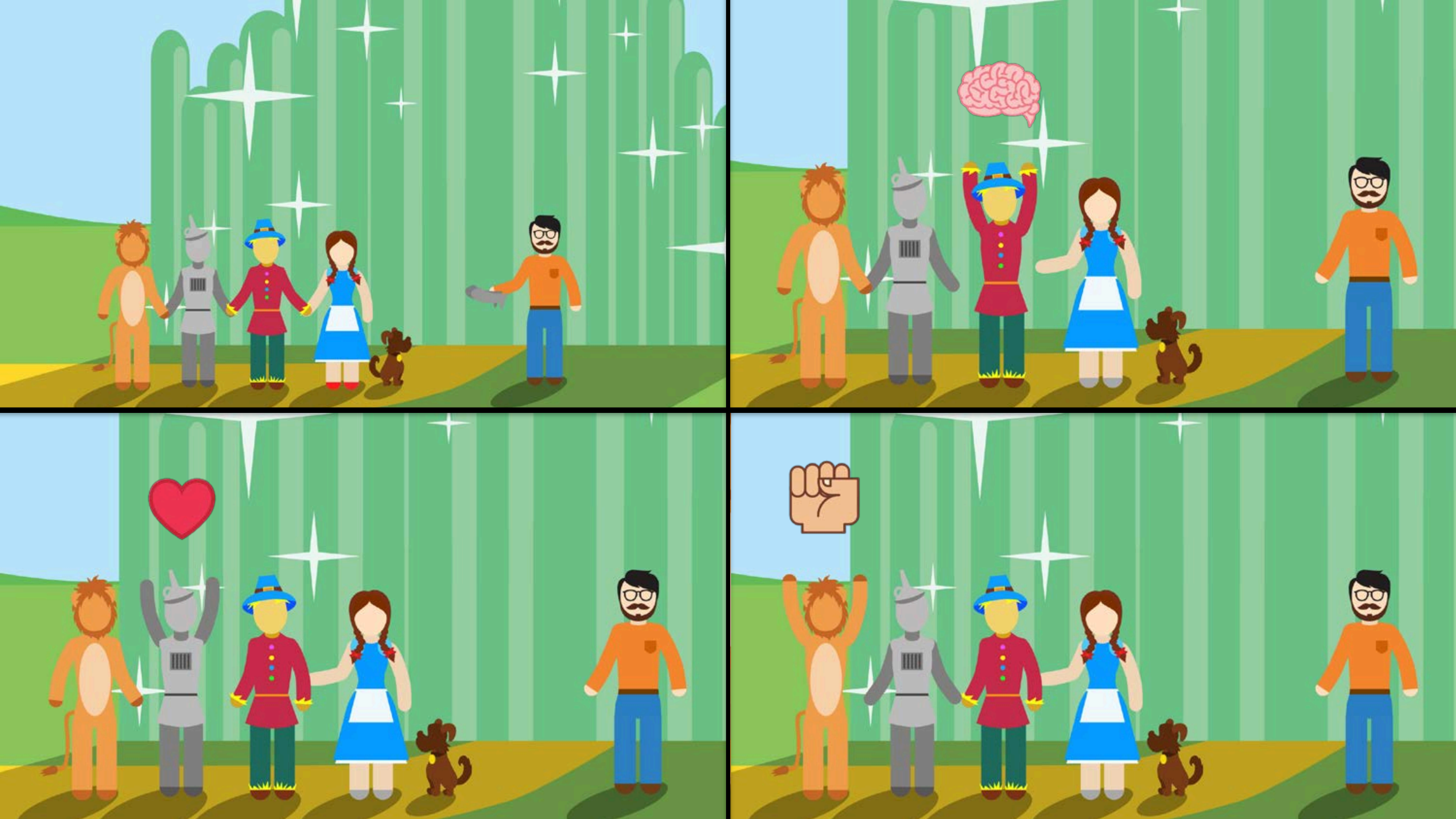
- Security controls and profiles are represented in proprietary ways
- Profile mappings to catalogs are often imprecise, not machine-readable
- Systems with many components require different profiles per component
- Multi-tenant and mixed ownership of components complicate assessment
- A single system may be subject to several regulatory frameworks
- Security control assessment is a complex, largely manual process

NIST OPEN SECURITY CONTROLS ASSESSMENT LANGUAGE (OSCAL)

Technical Overview







The End

What is OSCAL?

- New “Standard of Standards” normalizing how system security controls and corresponding assessment information are represented;

  Standardized: Provide security control, control implementation, and assessment information in an open, standardized way that can be used by both humans and machines

  Interoperable: Ensure OSCAL is well-defined so tools using OSCAL information are interoperable and use information consistently

  Easy to use: Promote developer adoption of OSCAL so tools are available for organizations to build, customize, and use OSCAL information

- Improve the efficiency, accuracy, and consistency of system security assessments.

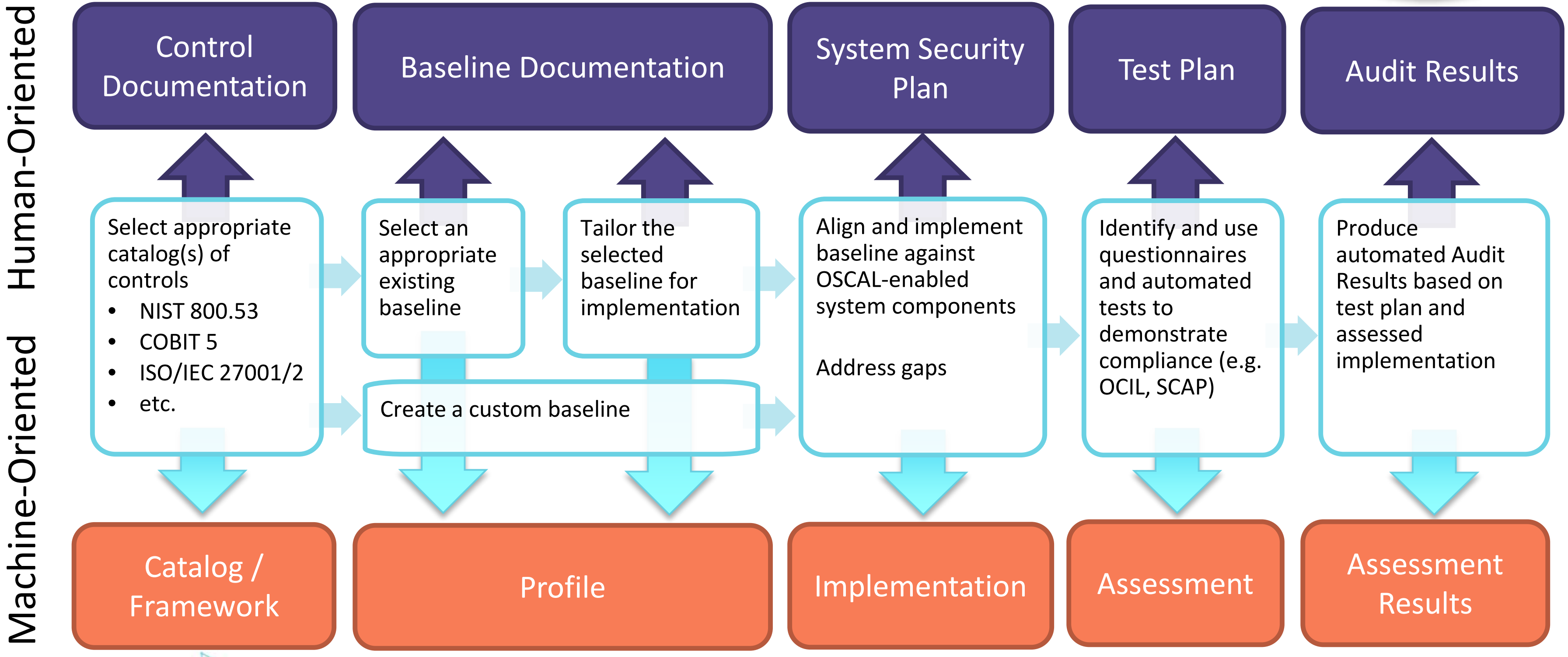
OSCAL goals

- Have OSCAL-enabled tools (existing and new) and OSCAL-formatted content widely available
- Have OSCAL use enable:
  - A large decrease in assessment-related labor
  - The ability to assess a system's security much more often, ideally continuously
  - The ability to assess a system's compliance with several sets of requirements simultaneously
  - The consistent performance of assessments, regardless of system type

A note about terminology

OSCAL Term	Meaning
Control	A safeguard or countermeasure designed to satisfy a set of defined security requirements. [based on NIST SP 800-53 definition]
Catalog	A set of security control definitions. Examples include the hundreds of controls in NIST SP 800-53, the 100+ controls in ISO 27002, and the practices in COBIT 5.
Profile	A set of security requirements; also called a baseline or overlay. Examples include the control baselines in NIST SP 800-53, the FedRAMP baselines, and the PCI DSS requirements.

OSCAL Workflow



Human-Oriented

Machine-Oriented

Control Documentation

Baseline Documentation

System Security Plan

Test Plan

Audit Results

Select appropriate catalog(s) of controls

- NIST 800.53
- COBIT 5
- ISO/IEC 27001/2
- etc.

Select an appropriate existing baseline

Tailor the selected baseline for implementation

Create a custom baseline

Align and implement baseline against OSCAL-enabled system components

Address gaps

Identify and use questionnaires and automated tests to demonstrate compliance (e.g. OCIL, SCAP)

Produce automated Audit Results based on test plan and assessed implementation

Catalog / Framework

Profile

Implementation

Assessment

Assessment Results

Phased Development of OSCAL

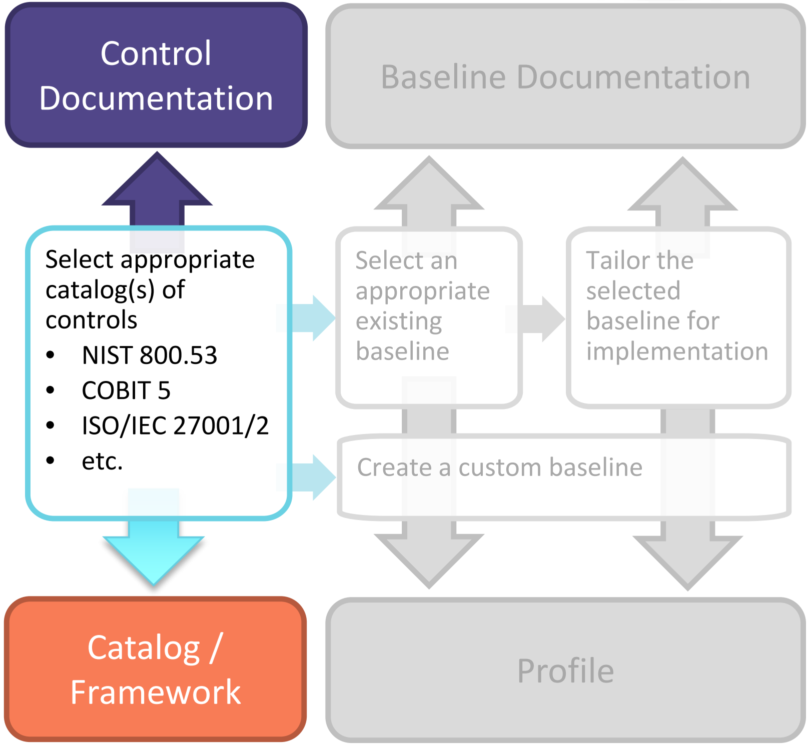
- OSCAL is being developed over a series of phases using an agile approach
  - Through a series of development sprints, provide increased value
  - Focus on the 80% of the solution we can implement in 20% of the time

Phase	Status	Description
0	Done	• Investigate existing control catalog approaches; • Develop prototype control catalog format
1	Done	• Stabilize catalog format • Develop prototype profile format
2	Near Done	• Stabilize profile format • Develop prototype implementation format • Open source GitHub project; promote community participation
3	Planned 2018	• Stabilize implementation format • Develop prototype framework, assessment, and assessment result formats
4	Planned early 2019	• Complete development of OSCAL 1.0

The OSCAL Catalog Model

Phases: 0 and 1 **Status:** Stable

- A normalized model for representing a control catalog
- Normalizes the representation of a control catalogs across multiple control catalog implementations
- Supports references to controls from other OSCAL models
- Developed to support SP 800-53, COBIT, ISO/IEC 27001, etc.
- Will support mapping to frameworks in Phase 3 (e.g., PCI DSS, NIST Cyber Security Framework, HIPAA)



Control Documentation

Baseline Documentation

Select appropriate catalog(s) of controls

- NIST 800.53
- COBIT 5
- ISO/IEC 27001/2
- etc.

Select an appropriate existing baseline

Tailor the selected baseline for implementation

Create a custom baseline

Catalog / Framework

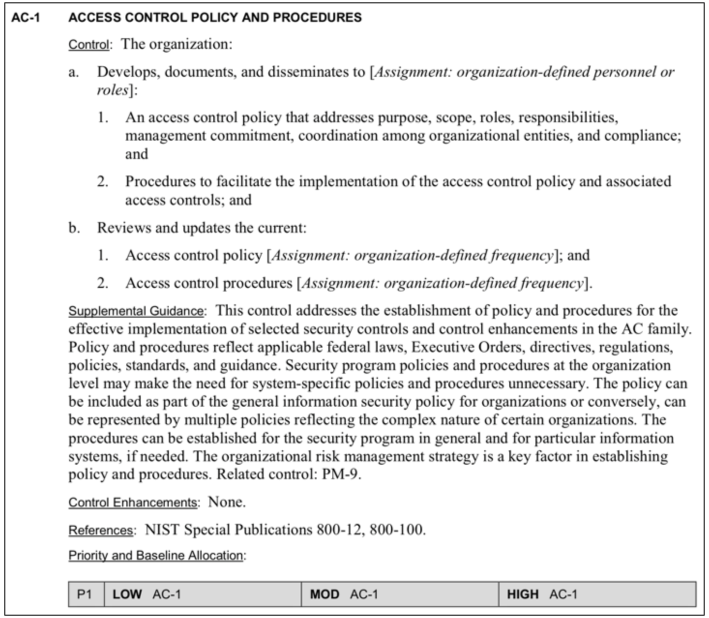
Profile

The OSCAL Catalog Format – Other Features

- A number of other features are also supported:
  - Inclusion of additional guidance text
  - References to related controls
  - Definition of control enhancements
  - Inclusion of assessment objectives and assessment methods (e.g., SP 800-53a)

OSCAL Catalog Example

Unstructured Prose



AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and

2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

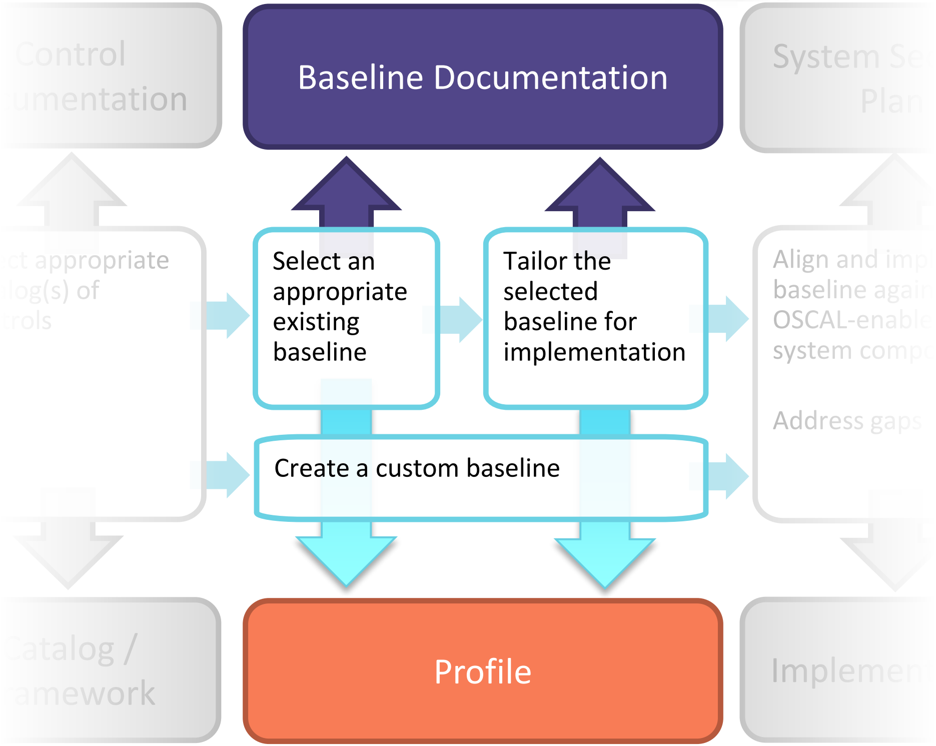
Structured OSCAL Catalog XML (partial)

```
<?xml version="1.0" encoding="UTF-8"?>
<catalog id="sp-800-53-rev4" xmlns="http://csrc.nist.gov/ns/oscal/1.0">
 <title>NIST SP800-53 Revision 4</title>
 <!-- snip -->
 <group class="family">
  <title>ACCESS CONTROL</title>
  <control class="SP800-53" id="ac.1">
   <title>ACCESS CONTROL POLICY AND PROCEDURES</title>
   <param id="ac-1_a">
    <desc>organization-defined personnel or roles</desc>
   </param>
   <!-- snip -->
   <prop class="name">AC-1</prop>
   <prop class="priority">P1</prop>
   <part class="statement">
    <p class="description">The organization:</p>
    <part class="item" id="smm_ac-1a.">
     <prop class="name">AC-1a.</prop>
     <p class="description">Develops, documents, and disseminates to <insert param-id="ac-1_a"/>:</p>
     <part class="item" id="sms_ac-1a.1.">
      <prop class="name">AC-1a.1.</prop>
      <p class="description">An access control policy that addresses purpose, scope, roles, responsibilities, management
commitment, coordination among organizational entities, and compliance; and</p>
     </part>
     <!-- snip -->
    </part>
    <!-- snip -->
   </part>
   <part class="guidance">
    <p>This control addresses the establishment of policy and procedures for the effective implementation of selected security
controls and control enhancements in the AC family. <!-- snip --> The organizational risk management strategy is a key factor in
establishing policy and procedures.</p>
    <link href="#pm.9"/>
   </part>
   <references>
    <ref>
     <citation href="http://csrc.nist.gov/publications/PubsSPs.html#800-12">NIST Special Publication 800-12</citation>
    </ref>
    <!-- snip -->
   </references>
  </control>
  <!-- snip -->
 </group>
</catalog>
```

The OSCAL Profile Model

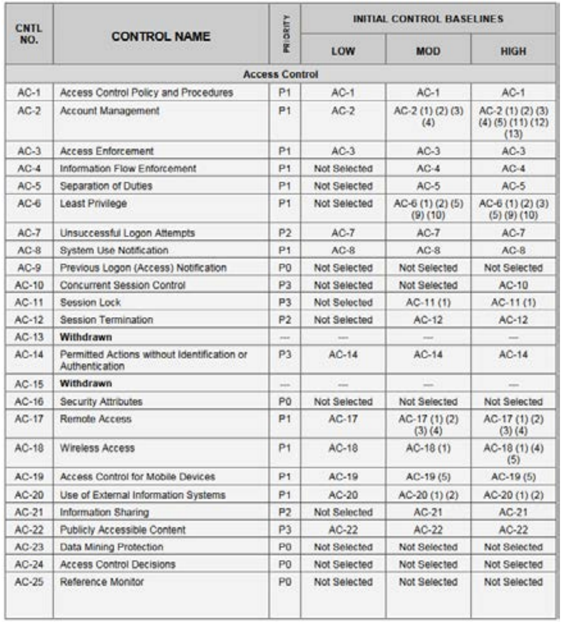
Phases: 1 and 2 **Status:** Near-Stable

- A normalized model for representing a profile
- A profile references underlying catalogs or other profiles
- Allows for the selection of a subset of controls and the further definition of parameters
- Developed to support SP 800-53 low/moderate/high, FedRAMP low/moderate/high, and customized baselines



OSCAL Profile Example

Semi-structured Prose



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

Structured OSCAL Profile XML (partial)

```xml
<?xml version="1.0" encoding="UTF-8"?>
<profile xmlns=http://csrc.nist.gov/ns/oscal/1.0
    id="uuid-051e9699-fc3e-4178-9c9c-5159f3e22dc1">
  <title>SP800-53 MODERATE BASELINE IMPACT</title>
  <import href="SP800-53-rev4-catalog.xml">
    <include>
      <call control-id="ac.1"/>
      <call control-id="ac.2"/>
      <call subcontrol-id="ac.2.1."/>
      <call subcontrol-id="ac.2.2."/>
      <call subcontrol-id="ac.2.3."/>
      <call subcontrol-id="ac.2.4."/>
      <call control-id="ac.3"/>
      <call control-id="ac.4"/>
      <call control-id="ac.5"/>
      <call control-id="ac.6"/>
      <!-- snip -->
    </include>
  </import>
</profile>
```

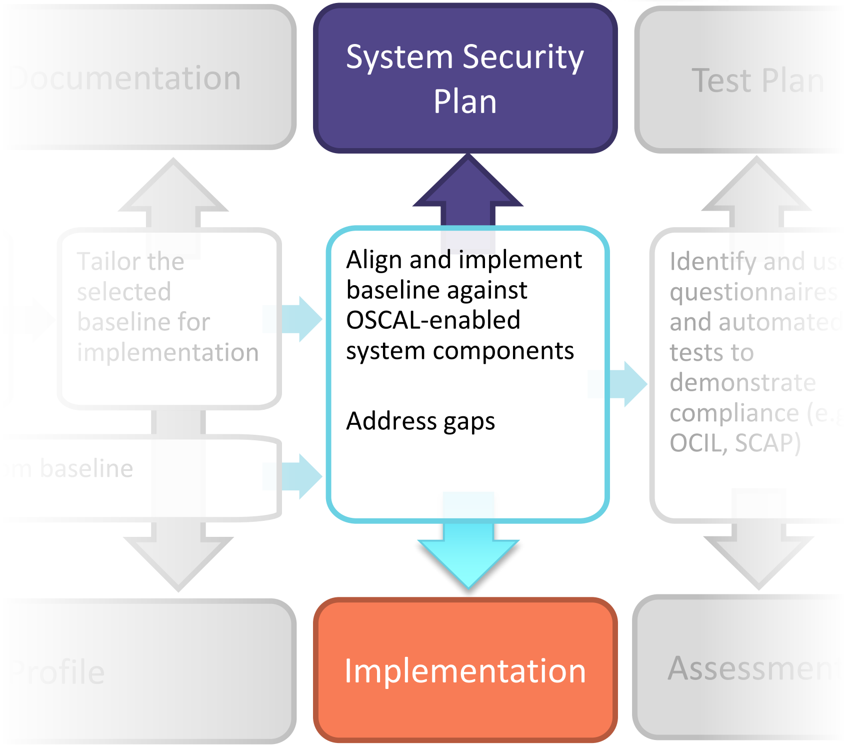
The OSCAL Profile Format – Other Features

- A number of other features are also supported:
  - Adding and removing control statements
  - Extending existing profiles
  - Merging duplicate controls

The OSCAL Implementation Model

Phases: 2 and 3 **Status:** Prototyping

- A normalized model for representing the implementation of controls for a system component
- An implementation references an underlying profile to provide the baseline
- Maps the selected baseline to the actual component implementation and provides definition of parameter values
- Supports the generation of a System Security Plan and supports analysis of control gaps in a system implementation


Documentation
System Security Plan
Test Plan
Tailor the selected baseline for implementation
Align and implement baseline against OSCAL-enabled system components
Address gaps
Identify and us questionnaires and automated tests to demonstrate compliance (e. OCIL, SCAP)
m baseline
rofile
Implementation
Assessmen

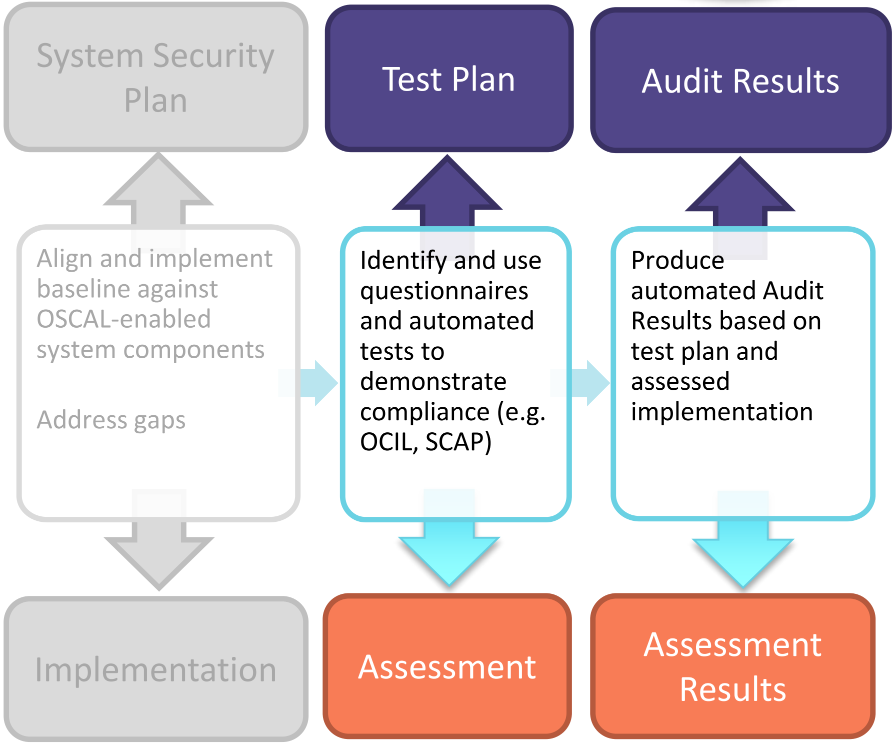
WHERE DOES THE YELLOW BRICK ROAD LEAD?

To the Emerald City...duh!

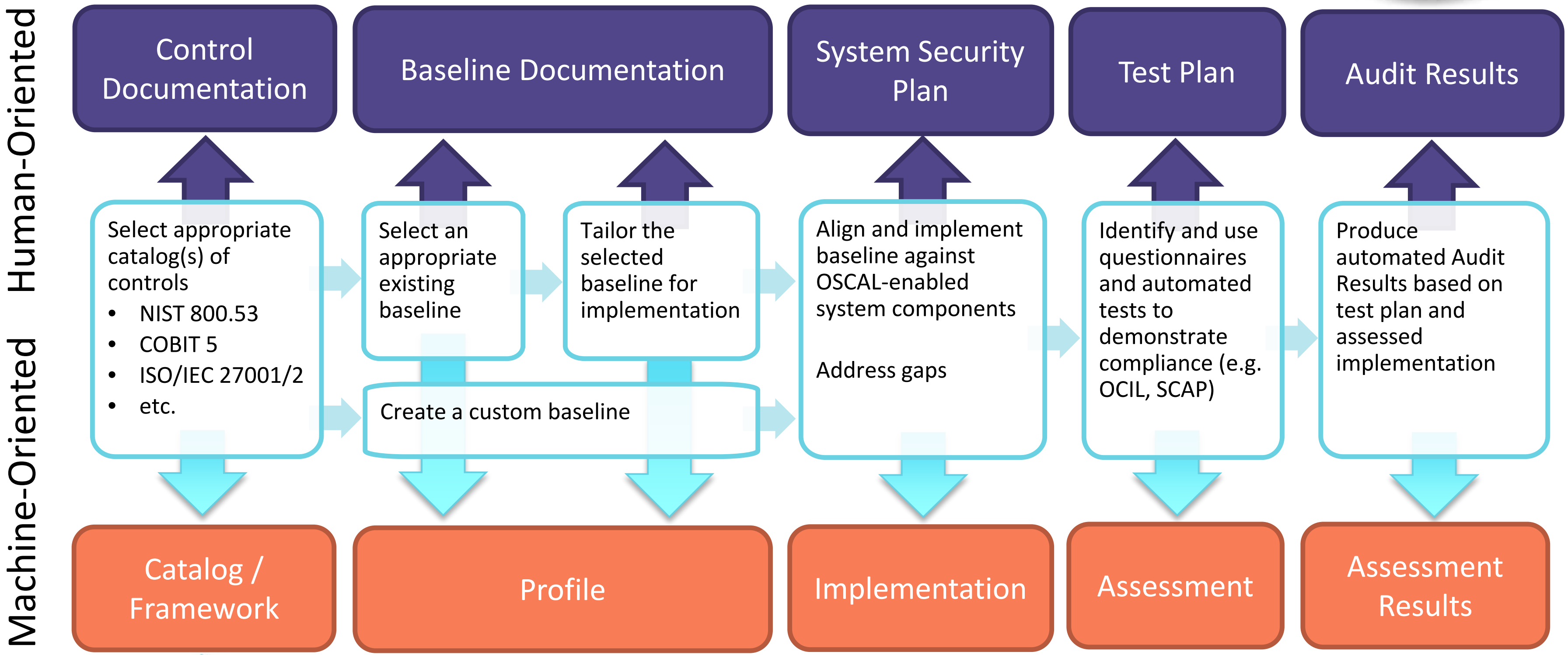
Remaining Work

Phases: 3 thru 5 **Status:** Planned

- Provide models that support automated assessment of control implementations, and associated assessment results
- Tie-in use of standardized questionnaires and evaluation of device state using the Security Content Automation Protocol (SCAP)


System Security Plan
Align and implement baseline against OSCAL-enabled system components
Address gaps
Implementation
Test Plan
Identify and use questionnaires and automated tests to demonstrate compliance (e.g. OCIL, SCAP)
Assessment
Audit Results
Produce automated Audit Results based on test plan and assessed implementation
Assessment Results

OSCAL Workflow



Human-Oriented

Machine-Oriented

Control Documentation

Baseline Documentation

System Security Plan

Test Plan

Audit Results

Select appropriate catalog(s) of controls

- NIST 800.53
- COBIT 5
- ISO/IEC 27001/2
- etc.

Select an appropriate existing baseline

Tailor the selected baseline for implementation

Create a custom baseline

Align and implement baseline against OSCAL-enabled system components

Address gaps

Identify and use questionnaires and automated tests to demonstrate compliance (e.g. OCIL, SCAP)

Produce automated Audit Results based on test plan and assessed implementation

Catalog / Framework

Profile

Implementation

Assessment

Assessment Results

LIVE DEMO

Enough talking, time to prove it...

WHY DOES THIS ALL MATTER?

C’mon, I love Word docs and Excel spreadsheets!

Live Poll

- Do you have compliance programs that operate off of Word documents and Excel spreadsheets?
  - Yes
  - No
  - Wait...I LOVE Excel spreadsheets!   #ExcelNinja
- Would you like to see more automation in your compliance program?
  - Yes
  - No
  - Automation, what’s that?

Why Does this All Matter?

- Information Technology and IoT are becoming increasingly complex
  - Hybrid Cloud deployments are on the rise
  - IoT is becoming increasingly commoditized, resulting in an inverse intersection of price vs. security vulnerabilities
  - Regulatory requirements are challenging
  - Manual security and compliance processes are not scalable

Summary

- OSCAL serves as the standard of standards to level the playing field
  - Standardized representation of control catalogs and profiles makes it easier to understand and map complex security requirements to information systems
  - Application of profiles to implementation ensures continuous compliance against your security requirements
  - System Security Plans (SSPs), Test Plans, Plan of Action Memos (POAMs) and Audit Findings can now be generated on demand
- OSCAL-enabled tools
  - Standardized formats allow automation across integrated tools
  - Chains of new or existing OSCAL-enabled tools will drive innovation

Team

Project co-leaders:

Michaela Iorga
NIST

David Waltermire
NIST

Email the OSCAL team at oscal@nist.gov

Team

Team members:

Anil Karmel
C2 Labs

Wendell Piez
C2 Labs

Karen Scarfone
C2 Labs

Andrew Weiss
Docker

Email the OSCAL team at oscal@nist.gov

Apply What You Have Learned Today

- Next week you should:
  - Familiarize yourself with the resources available on the OSCAL website
  - Understand where manual processes within your security and compliance program can be automated using OSCAL and OSCAL-based tools
- In the first three months following this presentation you should:
  - Talk to GRC tool vendors as to how they can leverage OSCAL to automate your security and compliance requirements
- Within six months you should:
  - Begin an automated compliance pilot with an OSCAL-based tool vendor

Questions and Answers

Q&A

Don’t be a cowardly lion. Ask your questions now!

OSCAL Resources

✉ oscal@nist.gov

pages.nist.gov/OSCAL

github.com/usnistgov/OSCAL

Anil Karmel
Co-Founder and CEO
C2 Labs, Inc.
akarmel@c2labs.com
@anilkarmel

David Waltermire
Security Automation Architect
NIST
David.Waltermire@nist.gov