
AWS
re:Inforce
JULY 26 – 27, 2022 | BOSTON, MA

GRC304

Automating security and compliance with OSCAL

Dr. Michaela Iorga

OSCAL Strategic Outreach Director
National Institute of Standards and Technology

Matthew Donkin

Information Assurance Manager, U.S. Government Security & Compliance
AWS

Amber Pearson (she/her)

Head of U.S. Security Engagement, U.S. Government Security & Compliance
AWS

Open security controls assessment language (OSCAL)

Background

- From do-it-yourself IT systems to convenient cloud services (utility model)
- New trust model evolved
  - Security automation was key

Why are we all here today?

Information technology is complex
and calls for automation

Regulatory frameworks are burdensome
and need interop auto GRC tools

Paper-based A&A doesn't scale
and calls for auto updates

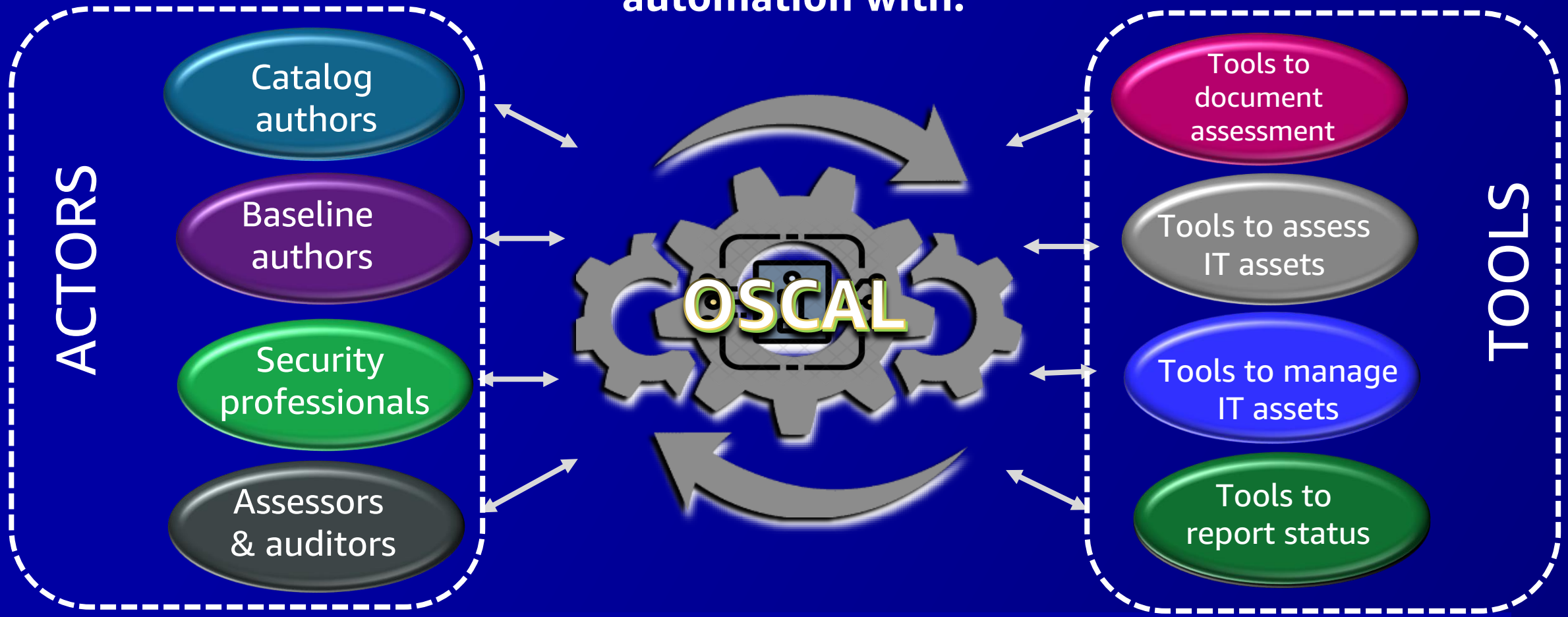
Security issues are everywhere
and call for auto updates

Risk management is hard
and experts need automation

DevOps and IaC are hard in multi-clouds
and call for interoperability and standardization

What was needed?

A machine-readable cyber Esperanto that enables TOOLS, ACTORS, and ORGANIZATIONS to exchange information via automation with:

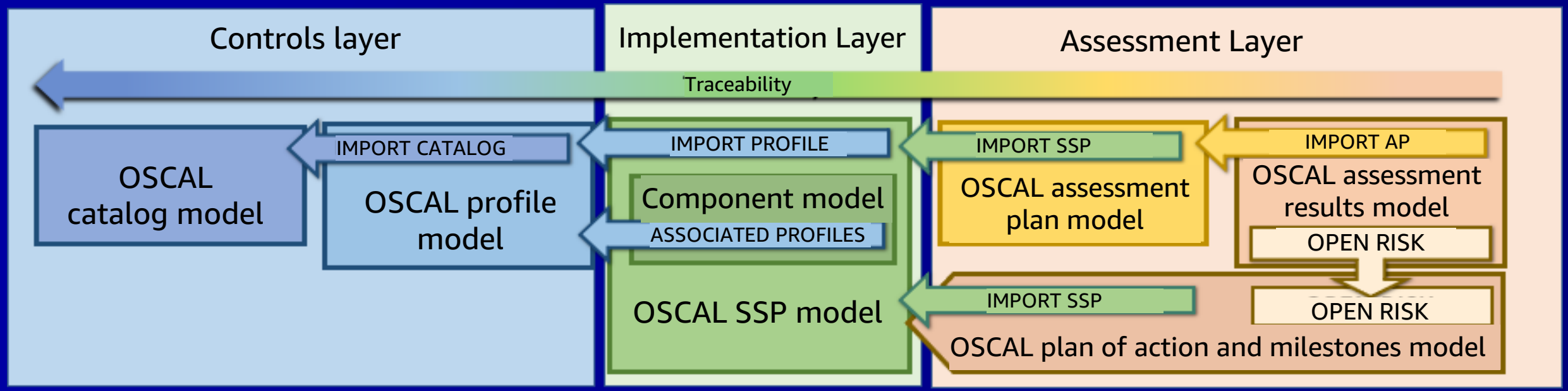


OSCAL sets the foundation for interoperable security automation

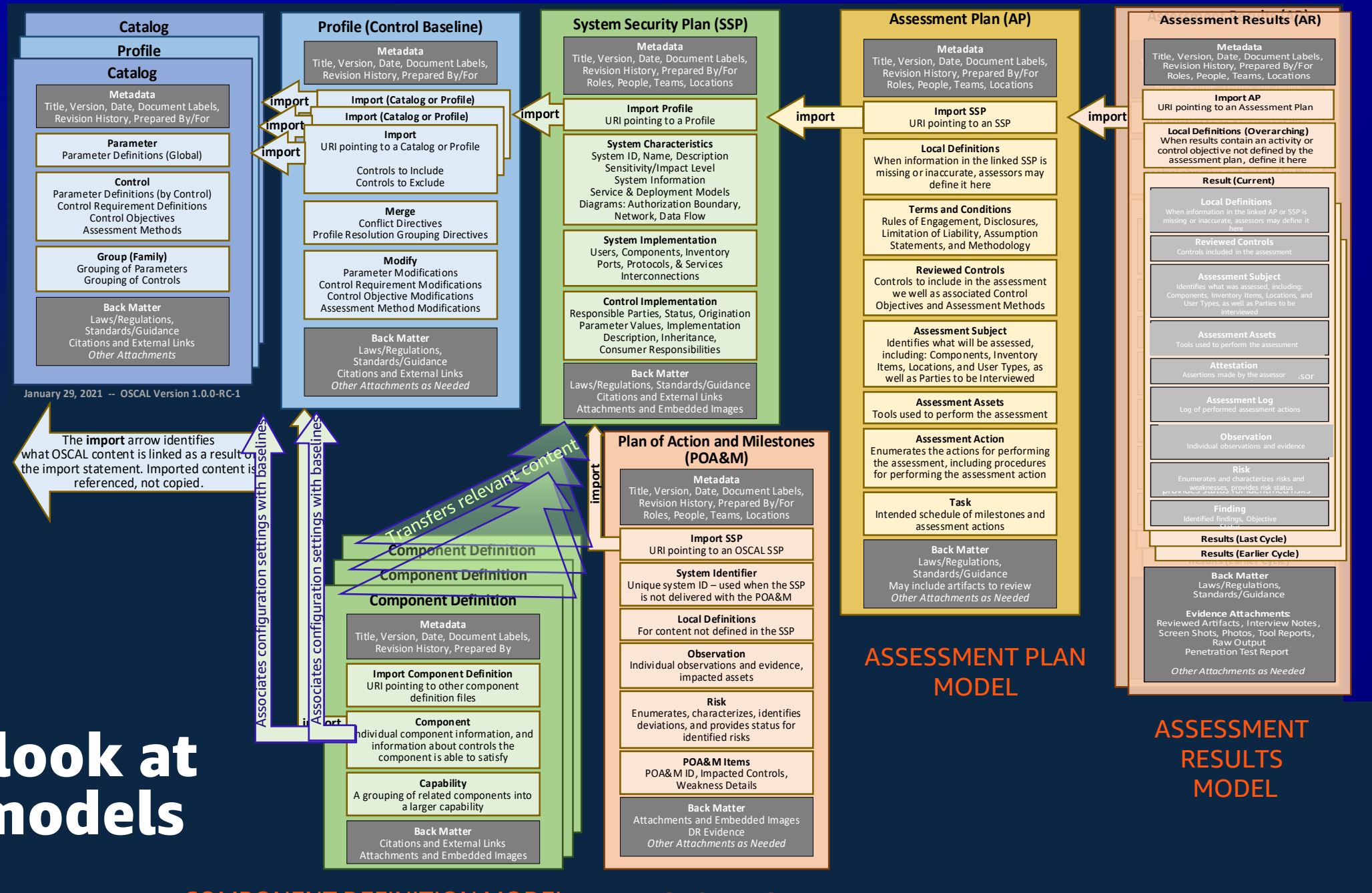
What is OSCAL?

OSCAL is the result of NIST and FedRAMP collaboration

- **OSCAL provides** a common/single machine-readable *language*, expressed in XML, JSON and YAML for:
  - Multiple compliance and risk management frameworks (e.g., SP 800-53, ISO/IEC 27001&2, COBIT 5)
  - Software and service providers to express implementation guidance against security controls (component definition)
  - Sharing how security controls are implemented (system security plans [SSPs])
  - Sharing security assessment plans (system assessment plans [SAPs])
  - Sharing security assessment results/reports (system assessment results [SARs])
- **OSCAL enables** automated traceability from selection of security controls through implementation and assessment



A closer look at OSCAL models



OSCAL v1 release

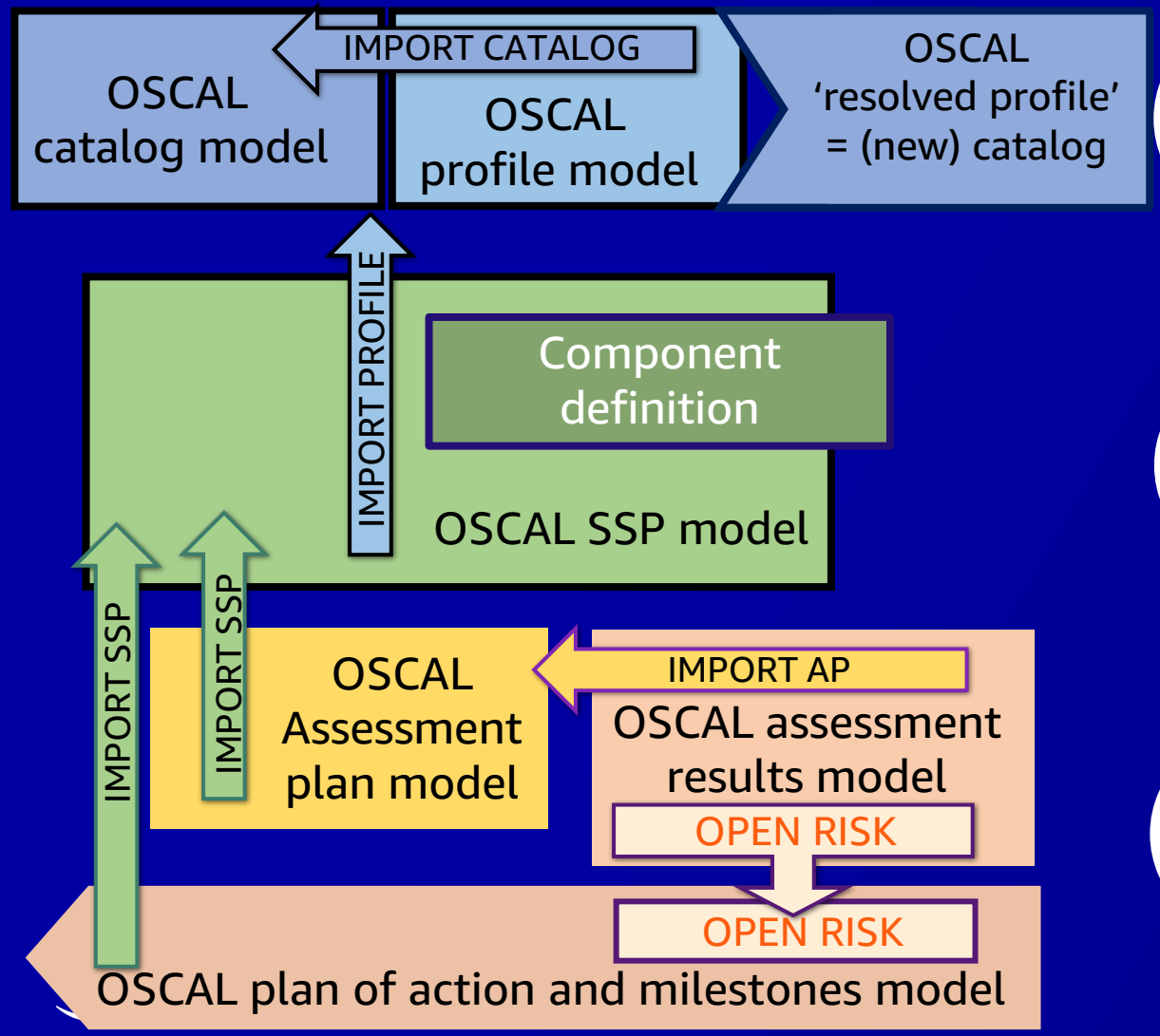
OSCAL 1.0.0 was released on June 7, 2021

https://github.com/usnistgov/OSCAL/releases/tag/v1.0.0

"…First official, major release of OSCAL provides a stable OSCAL 1.0.0 for wide-scale implementation …"

NIST, *GitHub*, *https://bit.ly/3J12F7z*

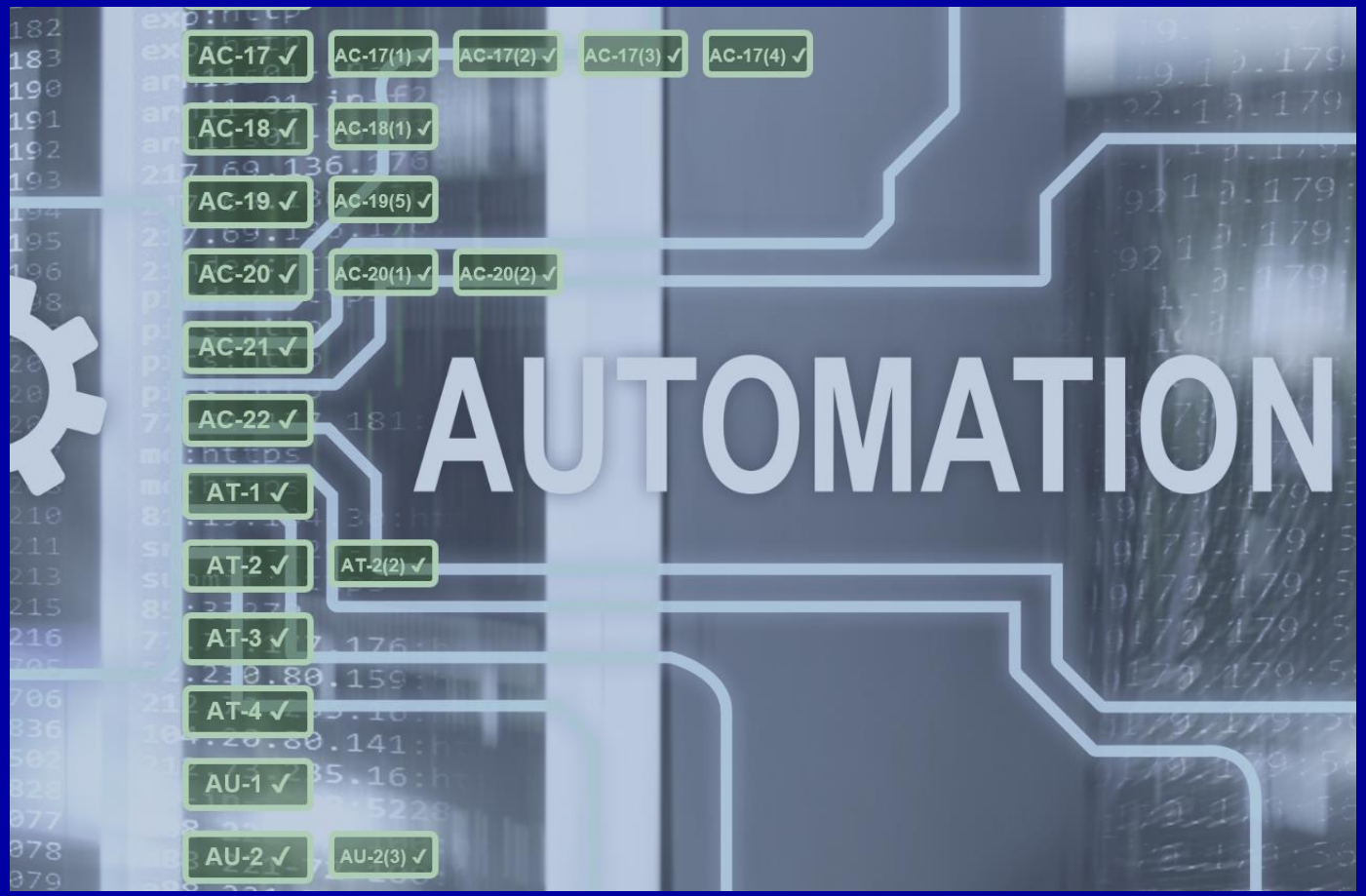
How is OSCAL different?



- No information needs duplication
- Custom granularity (controls can be decomposed into statements)
- Unique identifiers for parameters and statements

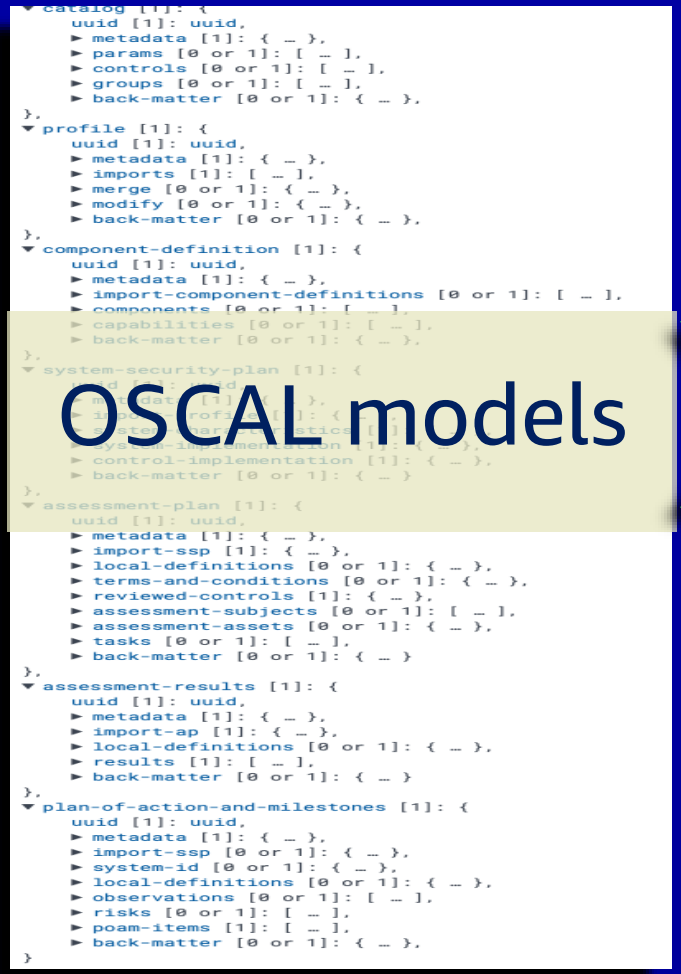
- Vendors can document their products
- Systems' security implementation can be decomposed

- Capture assessment plans and activities with custom cadence, and only for selected components
- POA&M conveys open risks aligned with the SSP capabilities and controls



What can you do with the OSCAL models?

OSCAL models > OSCAL content < OSCAL tools



OSCAL models

OSCAL content generation

Name	Provider/Developer	Description	Type
Compliance trestle	IBM	A python SDK and command line tool which manipulates OSCAL structures and supports transformation of data into OSCAL.	open source
OSCAL Java Library	NIST OSCAL Project	A Java-based programming API for reading and writing content conformant to the OSCAL XML, JSON, and YAML based models.	open source
OSCAL React Component Library	Easy Dynamics	A library of reusable React components and an example user interface application that provides a direct UI into OSCAL.	open source
OSCAL REST API	Easy Dynamics	An implementation of the OSCAL API that demonstrates how systems might manipulate catalogs, profiles, components, and SSPs.	open source
XSLT Tooling	NIST OSCAL Project	Extensible Stylesheet Language Transformations (XSLT), Cascading Style Sheets (CSS), and related utilities for authoring, converting, and publishing OSCAL content in various forms.	open source
XML Jelly Sandwich	Wendell Piez (NIST)	Interactive XSLT in the browser includes OSCAL demonstrations.	open source
Xacta 360		Xacta 360 is a cyber risk management and [illegible] platform [illegible] system security plans (SSPs) in OSCAL format. Future OSCAL capabilities [illegible] forthcoming as the [illegible]	[illegible] license
Atlasity: Continuous Compliance Automation	C2 Labs	Atlasity CE (release 2.0) runs in any environment and supports the development of OSCAL v1.0 content for Catalogs, Profiles, System Security Plans and Components. Additional detail can be found in this blog post: Atlasity Delivers Free Tools to Create OSCAL Content.	community edition

OSCAL editorial tools

OSCAL GRC tools

https://github.com/usnistgov/OSCAL

https://github.com/usnistgov/oscal-content

https://github.com/usnistgov/oscal-tools

OSCAL

https://nist.gov/oscal

NIST

OSCAL: the Open Security Controls Assessment Language

Get involved | Contact Us | Github

Learn More | Tutorials | Tools | Documentation | Downloads | Contribute | Contact Us

Providing control-related information in machine-readable formats.

NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSC
of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations
control baselines, system security plans, and assessment plans and results.

Open-source tools and libraries

https://pages.nist.gov/OSCAL/tools/#open-source-tools-and-libraries

	Provider/Developer	Description	Type
Compliance trestle	IBM	A python SDK and command line tool which manipulates OSCAL structures and supports transformation of data into OSCAL.	open source
OSCAL Java Library	NIST OSCAL Project	A Java-based programming API for reading and writing content conformant to the OSCAL XML, JSON, and YAML based models.	open source
OSCAL React Component Library	Easy Dynamics	A library of reusable React components and an example user interface application that provides a direct UI into OSCAL.	open source
OSCAL REST API	Easy Dynamics	An initial OpenAPI definition of an OSCAL REST API that describes how systems might manipulate catalogs, profiles, components, and SSPs.	open source
XSLT Tooling	NIST OSCAL Project	A variety of Extensible Stylesheet Language (XSL) Transformations (XSLT), Cascading Style Sheets (CSS), and related utilities for authoring, converting, and publishing OSCAL content in various forms.	open source
XML Jelly Sandwich	Wendell Piez (NIST)	Interactive XSLT in the browser includes OSCAL demonstrations.	open source
Xacta 360	Telos	Xacta 360 is a cyber risk management and compliance analytics platform that enables users to create and submit FedRAMP system security plans (SSPs) in OSCAL format. Future OSCAL capabilities are forthcoming as the standard evolves.	license
Atlasity: Continuous Compliance Automation	C2 Labs	Atlasity CE (release 2.0) runs in any environment and supports the development of OSCAL v1.0 content for Catalogs, Profiles, System Security Plans and Components. Additional detail can be found in this blog post: Atlasity Delivers Free Tools to Create OSCAL Content.	community edition
control_freak	Risk Redux	This tool seeks to provide folks with a searchable and easy-to-navigate reference for NIST SP 800-53 Revision 5. It is an open-source application from the Risk Redux project, built using parsed content directly from the OSCAL repositories.	open-source

How to contribute?

OSCAL is a community-driven effort.
Your participation directly impacts OSCAL's success!

Contact us at: oscal@nist.gov
Chat with us on Gitter:
https://gitter.im/usnistgov-OSCAL/Lobby

- ❑ Integrate support for OSCAL in your tools
- ❑ Implement OSCAL-based tools in your enterprise
- ❑ In GitHub

Contribute to the development of OSCAL:
htts://github.com/usnistgov/OSCAL

- ❑ Attend the biweekly community meetings hosted by NIST

https://pages.nist.gov/OSCAL/contribute/#community-meetings

A few OSCAL adopters

2021 presenters

- ❑ FedRAMP
- ❑ Noblis
- ❑ HHS CMS
- ❑ National Renewable Energy Lab
- ❑ GovReady
- ❑ C2 Labs
- ❑ cFocus Software
- ❑ Shujinko
- ❑ Robers Bosch (EU|Germany)
- ❑ Telos
- ❑ KPMG
- ❑ IBM Research

2022 new presenters

- ❑ AWS
- ❑ CSAM
- ❑ Easy Dymanics
- ❑ Volant Associates LLC
- ❑ Secureframe
- ❑ Red Hat
- ❑ Nirmata
- ❑ SunStone Secure

- ❑ US Air Force Platform One
- ❑ Booz Allen Hamilton
- ❑ eMASS
- ❑ Microsoft
- ❑ Coalfire
- ❑ Kratos
- ❑ Salesforce
- ❑ Oracle

Booz | Allen | Hamilton®

2021-2022 other adopters

AWS OSCAL implementation, successes and challenges

Documentation challenge

- **System security plan (SSP)**
  - 2 SSPs
  - 12 monthly updates
  - 1 annual assessment
  - GovCloud SSP is **735** pages
- **Customer responsibility matrix (CRM) and customer configuration guides (CCG)**
  - 24 monthly updates per year
  - **27,123** projected 2022 downloads
- **Total customer document downloads for 2021: 34,763**

OSCAL implementation

- **Xacta (Telos) governance, risk management and compliance (GRC) tool**
  - Provides **multiple classification** levels of OSCAL formatted authorization packages

- **OSCAL template**
  - FedRAMP GitHub:

OSCAL benefits to AWS customers

- **Current process**
  - Request access to digital rights management solution
  - Manually copy requisite security documentation into GRC
  - Manually update documentation on a monthly basis
  - Estimated **4,160** workforce hours per year to create and maintain ATO package
- **OSCAL simplification**
  - Request access to file repository
  - Download OSCAL format authorization package
  - Upload into OSCAL enabled GRC solution
  - Estimated **20-40** workforce hours per year to create and maintain ATO package
- **Streamline system authorization to operate (ATO) process**
  - Introduction of **machine-readable** representations of control catalogs, control baselines, system security plans, and assessment plans and results

OSCAL successes

- **AWS, in collaboration with Telos, was the first CSP to provide an OSCAL SSP to FedRAMP**
- **Able to provide feedback to industry partners to improve FedRAMP OSCAL template**
- **Partner with Accenture (3PAO) to provide a complete OSCAL authorization package by November 2022**
  - SAP
  - SAR

OSCAL authorization package timeline

- **System security plan (SSP)**
  - Status: **Complete**
- **Security assessment plan (SAP)**
  - Status: In progress
  - EDC: Q4 2022
- **Security assessment report (SAR)**
  - Status: In progress
  - ECD: Q4 2022
- **Plan of action and milestones (POA&M)**
  - Status: In progress
  - ECD: Q4 2022

OSCAL challenges

- **OSCAL SSP outputs verifying through NIST, but not on FedRAMP tools**
  - Different templates are causing issues with standardization

- **Erroneous information requirements that are not applicable to hyper-scaling CSPs**
  - How many users at any one time on the cloud
  - Role of each individual working within the environment

- **Aligning all information correctly from various documentation types**
  - SSPs are written differently and have appendices
  - Plans of action and milestones (POA&M) are written with various levels of information
  - Ensuring all pertinent data is in the correct layout for the OSCAL export

Automation of security authorization

Solutioning with customer obsession

AWS is working backwards from customers by addressing the problems of customers that have been federally regulated and by capturing the voices of customers.

These experiences and insights support AWS's customer obsession for solving customer friction points in the realm of security compliance, governance, and authorization.

Automating compliance solutions

Industry problem

- Constant technological innovation and protection requirements
- Evolving governance guidance that impacts the authorization process
- Determining exploitability and clarifying risk

Automation objective

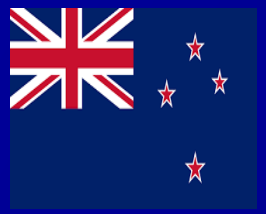
- Deliver compliance solutions that keep pace with the speed of business
- Streamline security documentation for shared responsibility, inheritance model and interconnections
- Standardize schema to encourage industry clarity and adoption

Driving automation forward

- **AWS actualizes conceptual models**
  - Invent and simplify within the security compliance industry
  - Convert authorization documents into machine readable artifacts
  - Develop APIs between GRC tools
- **Global adoption**
  - Expansion to other frameworks (ISO 27001/2, NIST 800-53 Rev5, COBIT 5)
  - Current global interests


Australia


Israel

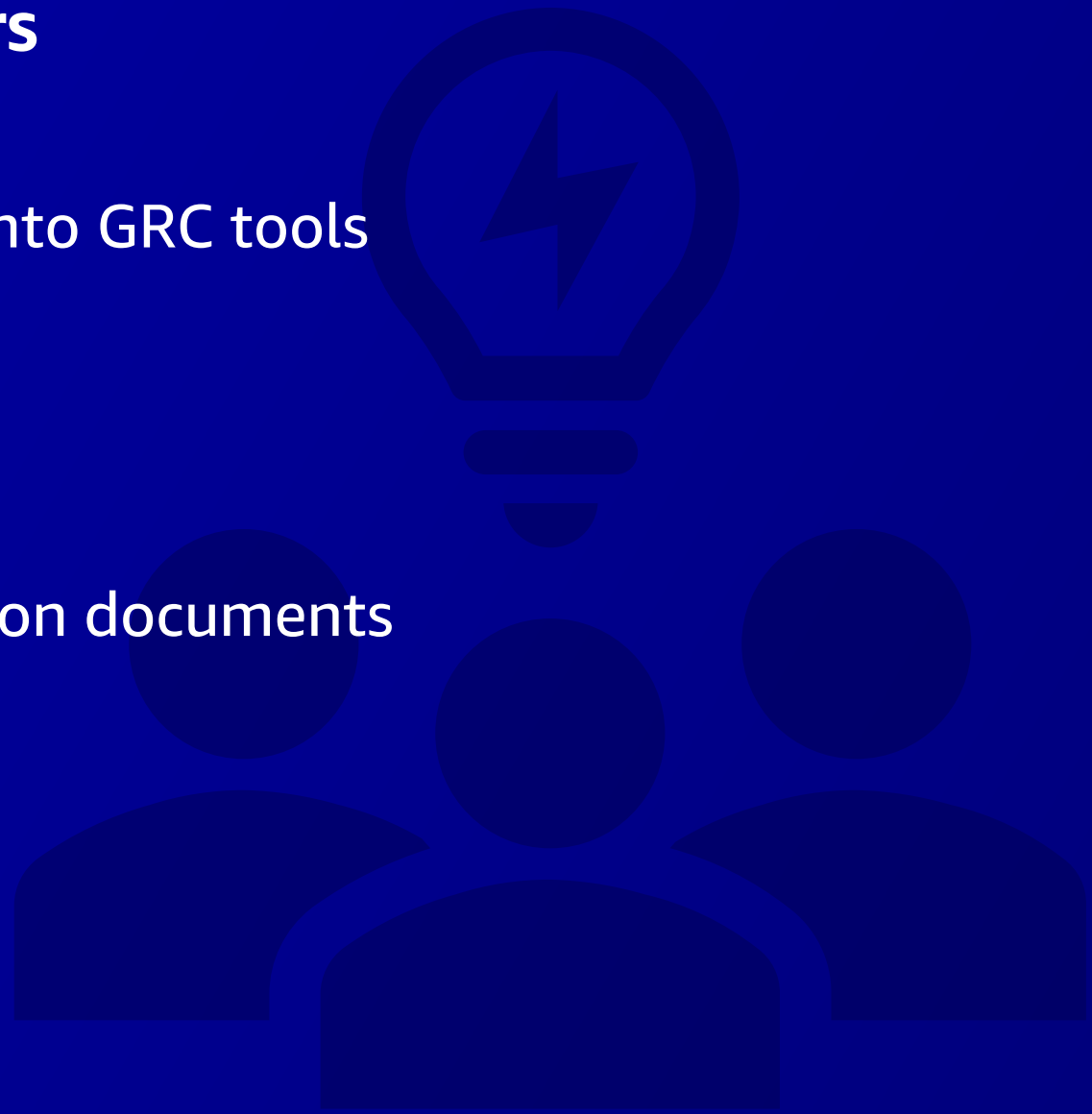

New Zealand


United Kingdom

Call to industry

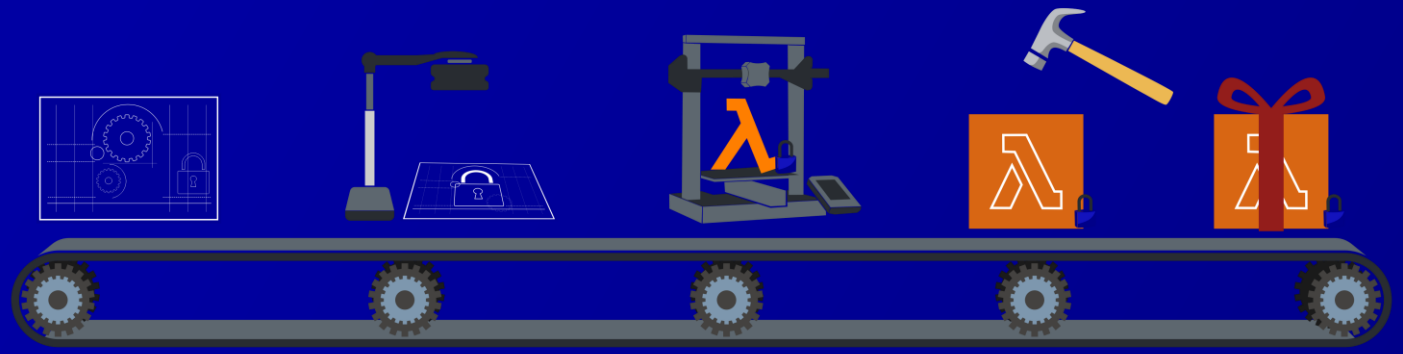
- **Collaboration with industry partners**
  - Automation progress and challenges
  - Ingestion of machine readable artifacts into GRC tools
  - Template granularity and consistency

- **AWS security automation summit**
  - Benefits of machine readable authorization documents
  - Increase adoption globally
  - Formalize templates



Transformation of security authorization

- Enhance customer authorization process through policy as code
- Drive towards zero-trust tailored controls rather than framework controls
- Provide prescriptive security controls that are automatically enforceable and measurable
- Deliver compliance automation to gain protection of cyberspace



“Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow.”

William Pollard

Physicist

Thank you!

Dr. Michaela Iorga

LinkedIn:

Matthew Donkin

LinkedIn:

Amber Pearson

LinkedIn: