Compliance Testle

An Open-Source Opinionated Implementation of OSCAL

Anca Sailer, STSM  Hybrid Cloud Compliance, IBM Research

Chris Butler, STSM  Hybrid Cloud Compliance, IBM Research
NIST OSCAL and Our Collaborative Platform

Problem
- Difficult to streamline compliance automation and documentation without a common language among different compliance landscape components and a coordinated collaborative platform

- Teams often recreate documents for multiple stakeholders and regulatory regimes due to lack of consistent separation of responsible stakeholders' duties.

Research Solution https://ibm.github.io/compliance-trestle

- Trestle is an opinionated, open-source tool to allow coordinated collaborative editing and automation workflows of NIST OSCAL documents by managing compliance as code developed by Research.

- Trestle extends in collaboration with the open source compliance policy assessment tool Auditree:
  - Build automation on governed documentation artifacts to target multiple environments.
  - Allow teams to write once and re-use for many regulations and audits.
  - Construct and correctly validate FedRAMP SSPs using OSCAL – which is the strategic direction for the FedRAMP PMO office and for the general services administration.

Partners
Michaela Iorga
David Waltermire
What does OSCAL mean to us?
More than a comprehensive data model ... ... the glue to connect the complex workflows from regulation to control implementations to evidence to audit...

... to connect Compliance Officers to Engineers to Auditors
FROM OSCAL as formalized by NIST in collaboration with the FedRAMP team...

- Document the security control implementation in the SSP
- Perform gap analysis and update the SSP ensuring controls are addressed

- Establish assessment and audit plans based on system requirements
- Identify automated mechanisms to collect assessment and audit data
- Use automation to produce assessment and audit results based on implementation state
- Continuously monitor controls implementations

Select appropriate catalog(s) of controls:
- NIST 800 53
- COBIT 5
- ISO 27k
- ISM

Select a baseline or subset of security controls

Create a custom baseline

Establish assessment and audit plans based on system requirements

Identify automated mechanisms to collect assessment and audit data

Use automation to produce assessment and audit results based on implementation state

Continuously monitor controls implementations

https://pages.nist.gov/OSCAL/
Our OSCAL artifacts as pipelines of tasks behind which the automation runs
Compliance posture management solutions are not enough for compliance ... we need resolution

1. Define the system
2. Select security controls
3. Implement security controls
4. Assess security controls
5. Authorize the system
6. Monitor the system
**trestle:** Opinionated python toolchain for orchestrating multiple compliance tools.

- Python library / toolchain for interoperability with Auditree
- Automatically generated object model from OSCAL standard
- Support for OSCAL editing via ‘exploding’ OSCAL schema into
- Allowance for ‘distributed compliance’ where OSCAL objects can be inherited from various sources
- Designed to run as either:
  - CICD pipeline off of github (via travis / tekton)

[Diagram of Trestle toolchain]

https://ibm.github.io/compliance-trestle
trestle: Repository content & utilities
trestle: Repository structure to allow create, import, clone, add, remove, split, merge, validate, assemble
Collaboration with OSCAL Team

2020 *trestle* adaptations to OSCAL:

- Target Definition as template for the Component Definition
- Target Plan as template for the Assessment Plan
- Component Definition parametrization for products policy attributes

2021 *trestle* FedRAMP goals:

- *trestle* to validate FedRAMP SSP document compliance (1Q) in conjunction with the GSA team.
- *trestle* to generate boilerplate SSPs with default assumptions.
- *trestle* generate FedRAMP format SSP within a word document exploiting Red Hat open source efforts.

[https://github.com/GSA/fedramp-automation](https://github.com/GSA/fedramp-automation)