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

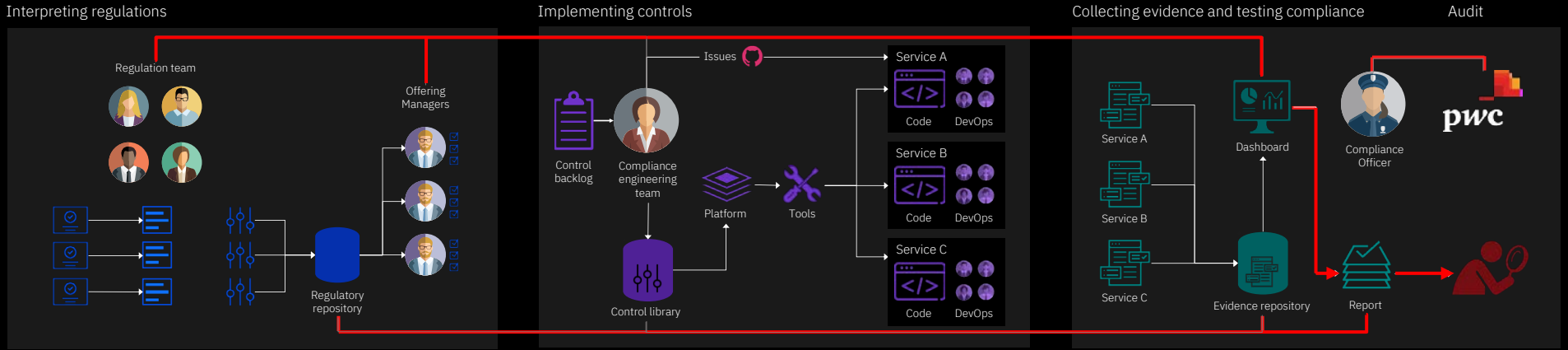
David Waltermire

What does OSCAL mean to us?

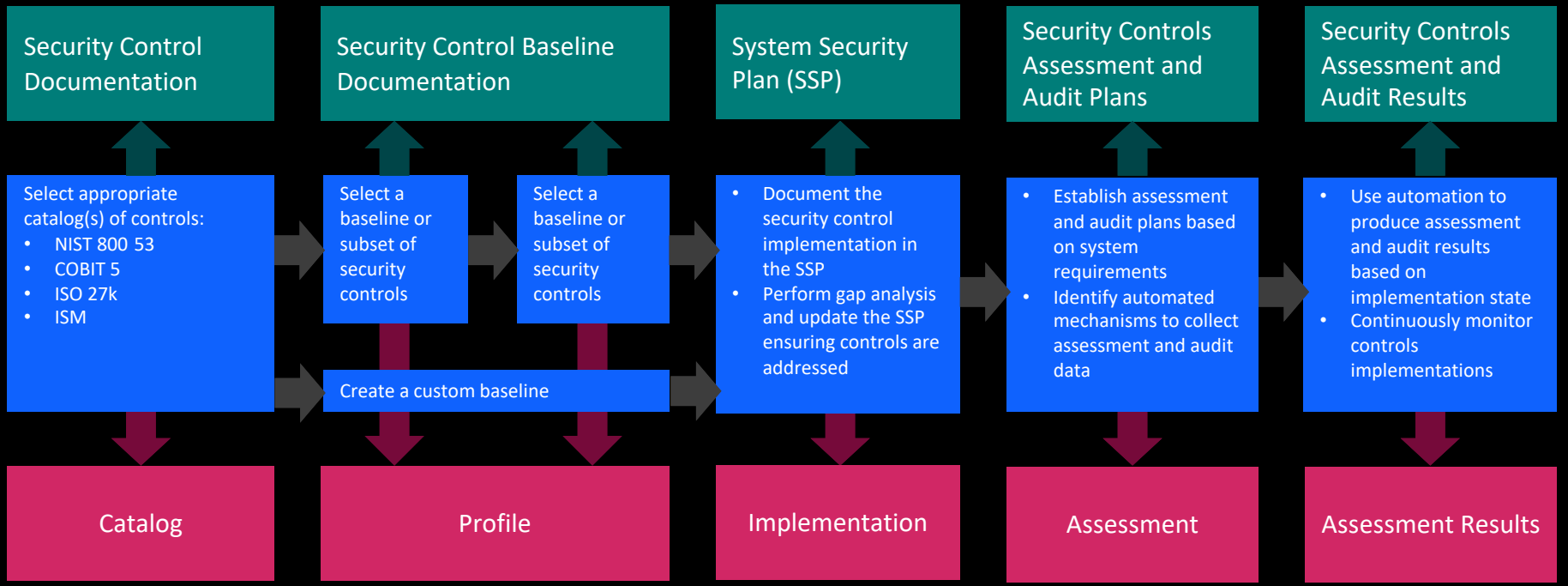
More than a comprehensive data model …

… the glue to connect the complex workflows from regulation to control implementations to evidence to audit…

… to connect Compliance Officers to Engineers to Auditors

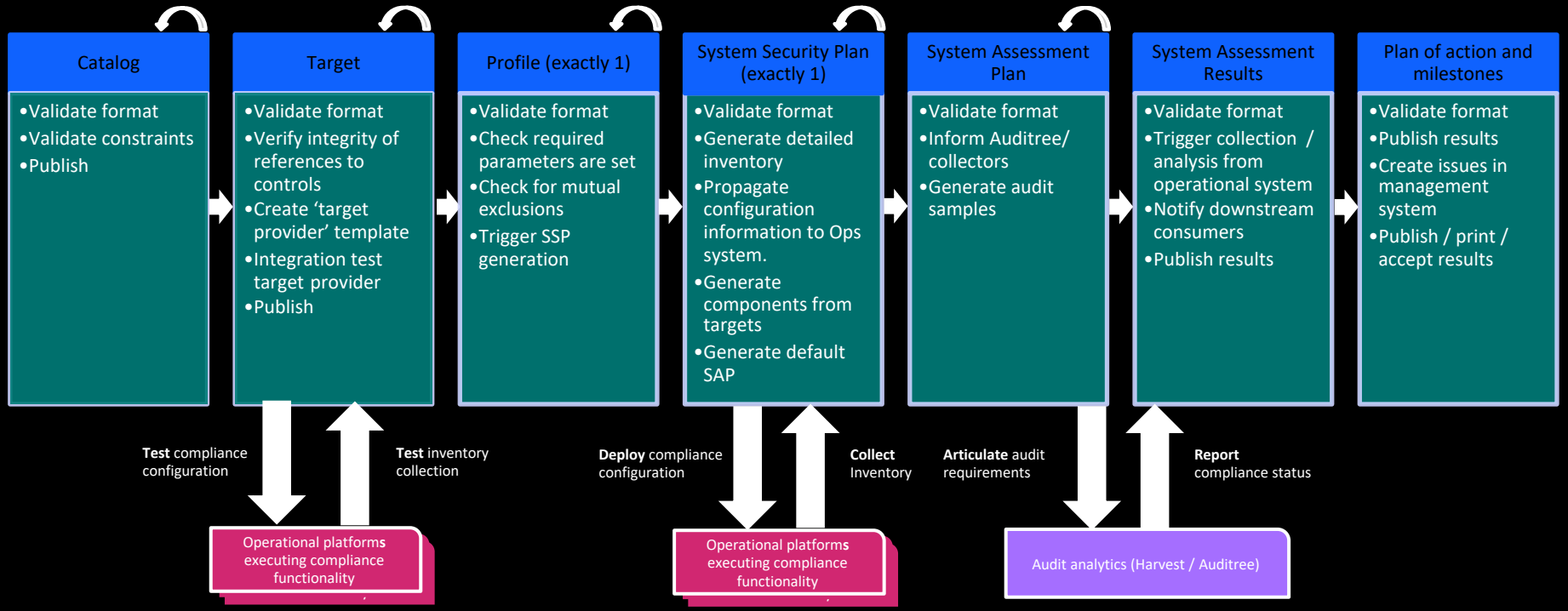


FROM OSCAL as formalized by NIST in collaboration with the FedRAMP team...

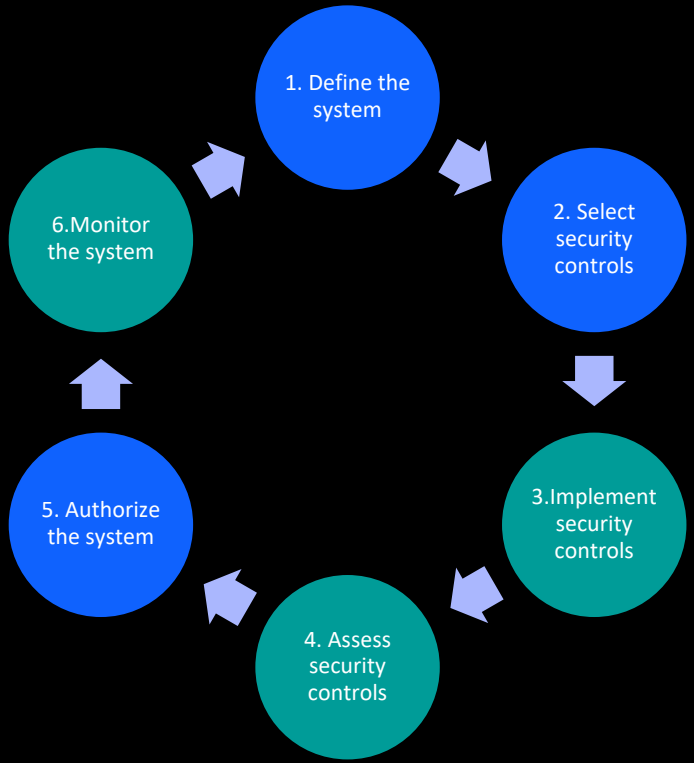


https://pages.nist.gov/OSCAL/

TO Our OSCAL artifacts as pipelines of tasks behind which the automation runs



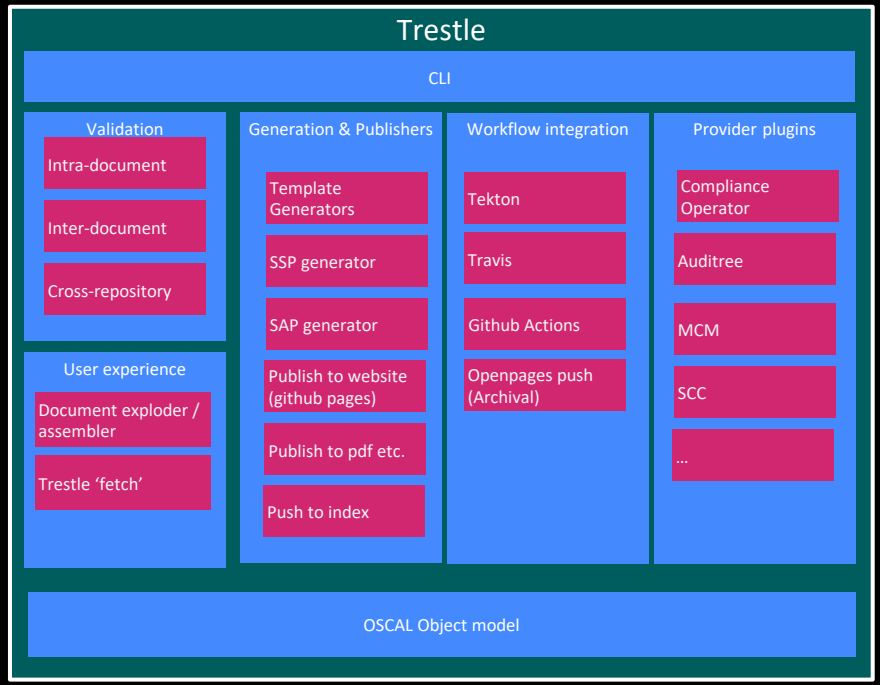
Compliance posture management solutions are not enough for compliance … we need resolution



https://www.cyber.gov.au/acsc/view all content/publications/anatomy cloud assessment and authorisation

`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)



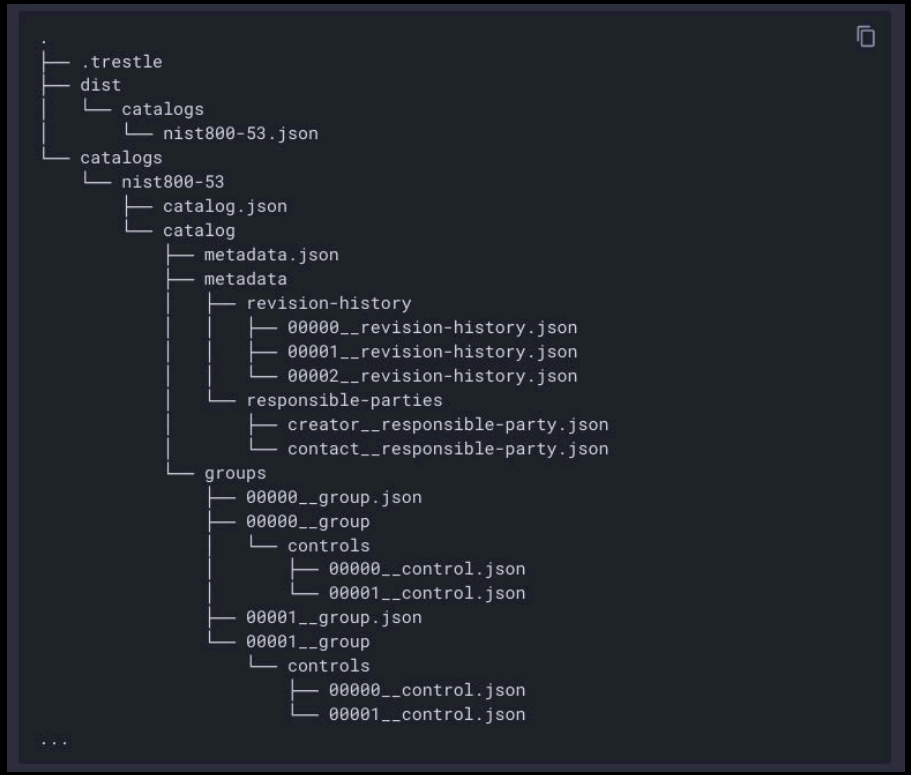
https://ibm.github.io/compliance-trestle

trestle: Repository content & utilities

```
(base) chris@jettopper Desktop % mkdir test_trestle
(base) chris@jettopper Desktop % cd ./test_trestle
(base) chris@jettopper test_trestle % trestle init
Initialized trestle project successfully in /Users/chris/Desktop/test_trestle
(base) chris@jettopper test_trestle % ls -alh
total 0
drwxr-xr-x  12 chris  staff   384B 14 Jan 22:14 .
drwx------@ 67 chris  staff   2.1K 14 Jan 22:14 ..
drwxr-xr-x   3 chris  staff    96B 14 Jan 22:14 .trestle
drwxr-xr-x   2 chris  staff    64B 14 Jan 22:14 assessment-plans
drwxr-xr-x   2 chris  staff    64B 14 Jan 22:14 assessment-results
drwxr-xr-x   2 chris  staff    64B 14 Jan 22:14 catalogs
drwxr-xr-x   2 chris  staff    64B 14 Jan 22:14 component-definitions
drwxr-xr-x  10 chris  staff   320B 14 Jan 22:14 dist
drwxr-xr-x   2 chris  staff    64B 14 Jan 22:14 plan-of-action-and-milestones
drwxr-xr-x   2 chris  staff    64B 14 Jan 22:14 profiles
drwxr-xr-x   2 chris  staff    64B 14 Jan 22:14 system-security-plans
drwxr-xr-x   2 chris  staff    64B 14 Jan 22:14 target-definitions
(base) chris@jettopper test_trestle % cd ./catalogs
(base) chris@jettopper nist-800-53 % ls
catalog.json
(base) chris@jettopper nist-800-53 % less catalog.json
(base) chris@jettopper nist-800-53 % wc -l catalog.json
   78598 catalog.json
(base) chris@jettopper nist-800-53 % trestle split -f catalog.json -e 'catalog.groups.*'
(base) chris@jettopper nist-800-53 % ls
catalog         catalog.json
(base) chris@jettopper nist-800-53 % cd ./catalog/groups
(base) chris@jettopper groups % ls
00000__group.json       00003__group.json       00006__group.json       00009__group.json
00001__group.json       00004__group.json       00007__group.json       00010__group.json
00002__group.json       00005__group.json       00008__group.json       00011__group.json
(base) chris@jettopper groups % less 00000__group.json
(base) chris@jettopper groups % cd ../
(base) chris@jettopper catalog % ls
groups
(base) chris@jettopper catalog % cd ../
(base) chris@jettopper nist-800-53 % trestle merge -e 'catalog'
```


```
{
    "group": {
        "id": "ac",
        "class": "family",
        "title": "Access Control",
        "controls": [
            {
                "id": "ac-1",
                "class": "SP800-53",
                "title": "Policy and Procedures",
                "params": [
                    {
                        "id": "ac-1_prm_1",
                        "label": "organization-defined personnel or roles"
                    },
                    {
                        "id": "ac-1_prm_2",
                        "select": {
                            "how-many": "one or more",
                            "choice": [
                                "organization-level",
                                "mission/business process-level",
                                "system-level"
                            ]
                        }
                    },
                    {
                        "id": "ac-1_prm_3",
                        "label": "organization-defined official"
                    },
                    {
                        "id": "ac-1_prm_4",
                        "label": "organization-defined frequency"
                    },
                    {
                        "id": "ac-1_prm_5",
                        "label": "organization-defined events"
                    },
                    {
                        "id": "ac-1_prm_6",
                        "label": "organization-defined frequency"
                    },
                    {
                        "id": "ac-1_prm_7",
                        "label": "organization-defined events"
                    }
                ],
                "props": [
                    {
                        "name": "label",
                        "value": "AC-1"
                    },
                    {
                        "name": "sort-id",
                        "value": "ac-01"
                    }
                ],
```

`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