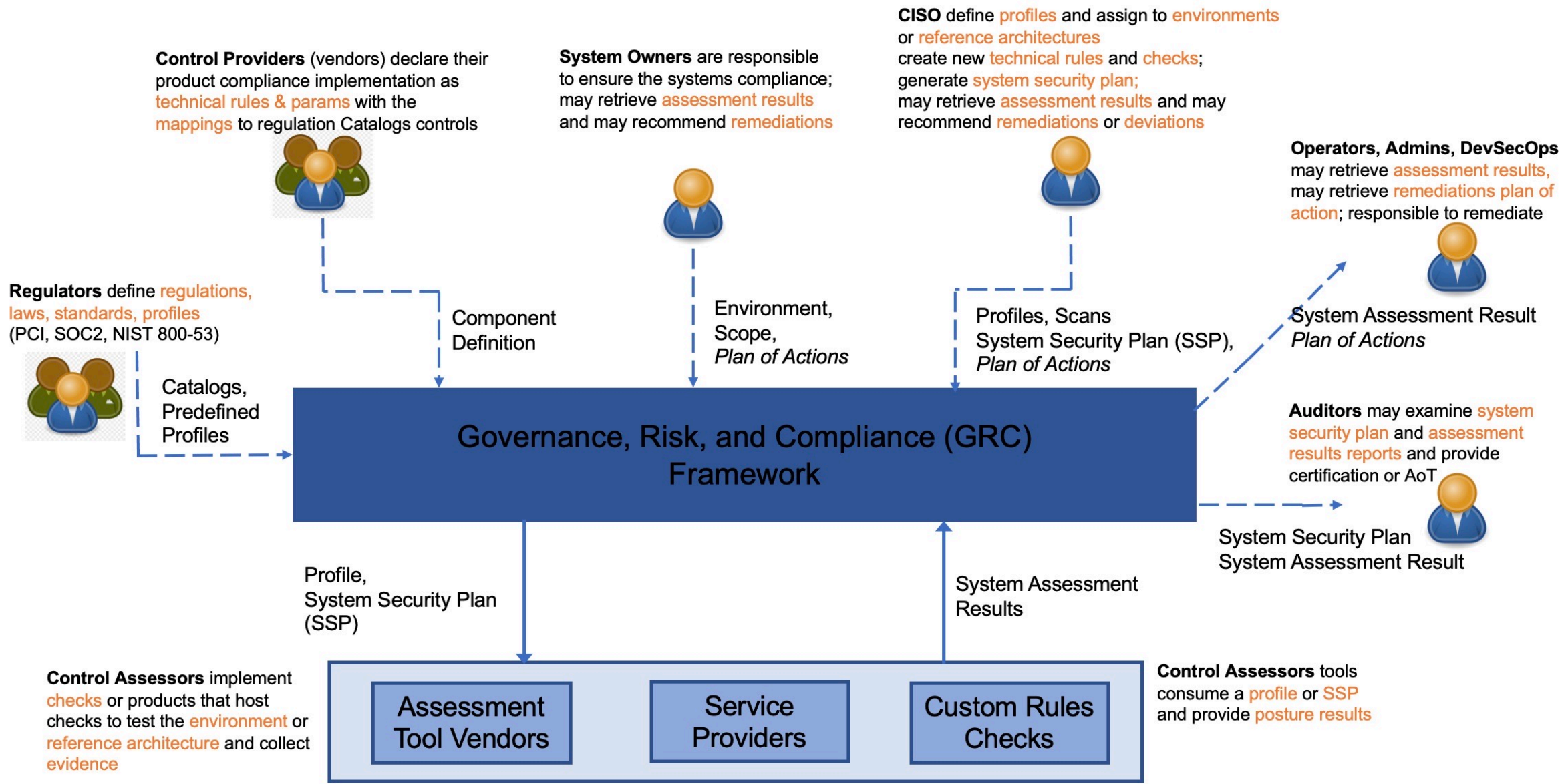


Trestle: Compliance-as-Code Orchestrator and Automation Workflows

Anca Sailer, Lou Degenaro, Vikas Agarwal
IBM Research

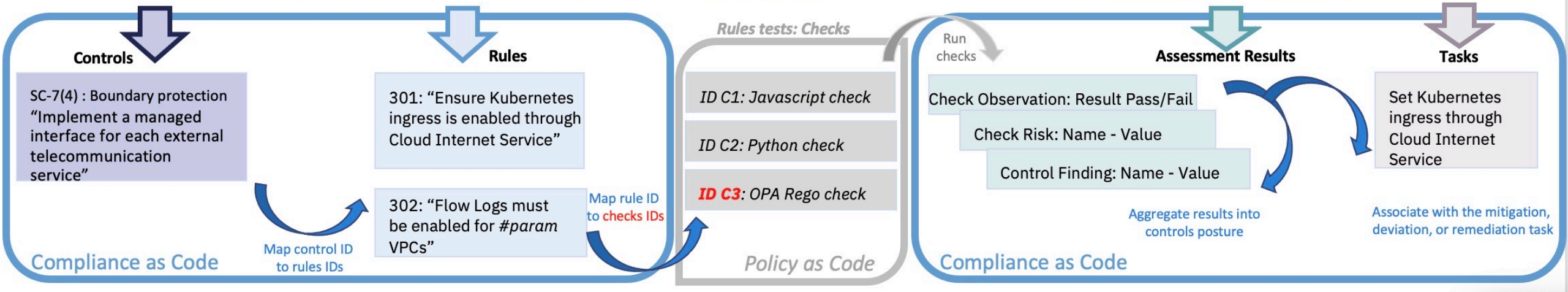
Who is Who in Compliance: Personas and Roles



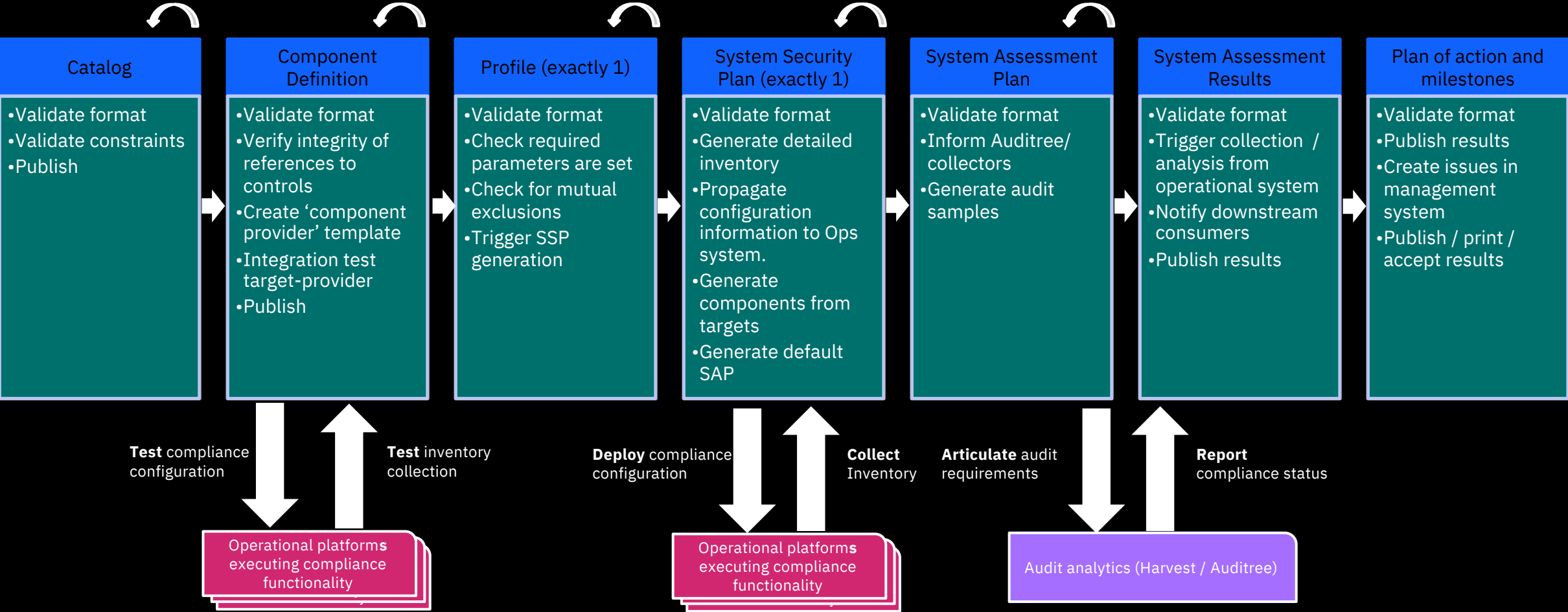
Persona's use of Compliance Artifacts

Compliance as Code vs. *Policy as Code*

Regulator	Compliance Officer/CISO	Control Provider / Vendor	System Owner & CISO	Auditor Intern / Extern	Assessor	System Owner & CISO
Catalog	Profile	Component Definition	SSP System Security Plan	SAP System Assessment Plan	SAR System Assessment Result	POAM Plan of Actions & Milestones
NIST-800-53 v4 PCI v4.0 FS Cloud v1	Profile Moderate {Subset of catalog controls} v1 FS Cloud DevTest v1	Component -> control- implementations -> implemented- requirements -> control -> props: - rule_id/version - check_id/version -> set-parameters	Profile controls Component -> control- implementations -> implemented- requirements -> control -> props: - rule_id/version - check_id/version	Scope, Profile Component -> control- implementations -> implemented- requirements. -> props: - rule_id/version - check_id/version	Scope, Profile, Results Observation, Risk -> props check_id/version - result -pass/fail/. risk_id - name – value finding - name – value	Scope, Profile, Results Observation, Risk -> mitigation -> remediation - tasks



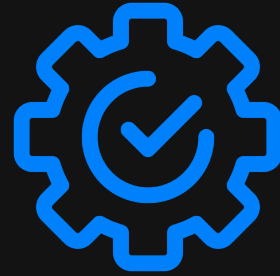
NIST's OSCAL language provides a standardized set of artifacts for compliance that can interoperate with operational systems.



DevSecOps provides a pattern for minimizing 'waterfall' roadblocks which can be leveraged for compliance.



Everything as code
providing cross team
visibility



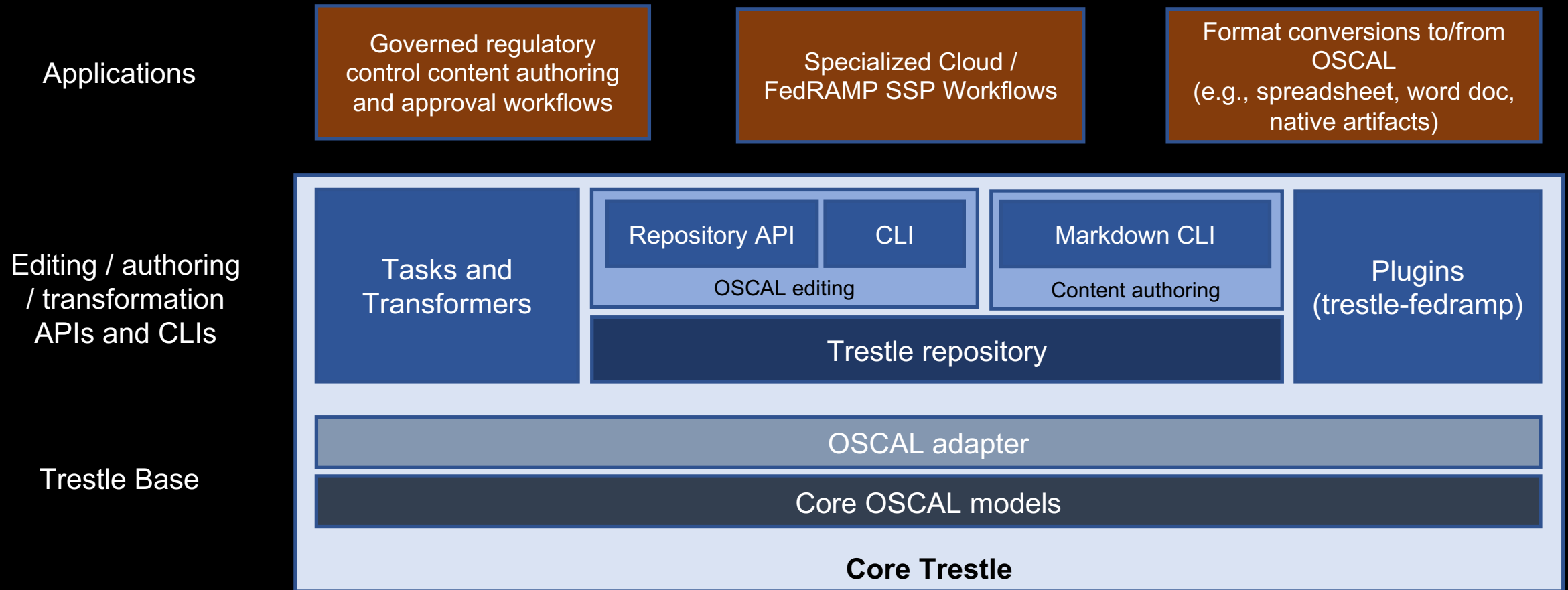
Automated testing &
verification



Systematic logging and
monitoring of systems

Trestle leverages this pattern for building compliance artifacts as code.

Conceptual Architecture



Trestle CLI

Requirement: As a new user to OSCAL the objects are extremely complex, I want tooling to help manage and create OSCAL files.

- Trestle provides functionality to manage large OSCAL files as fragments in a directory tree
- Utilities include generating object skeletons, import validation and release management on git based platforms
- Example below – use trestle to breakdown large OSCAL files to ease viewing / manipulation
- (https://ibm.github.io/compliance-trestle/tutorials/trestle_sample_workflow)

```
(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
(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    00012__gro
00001__group.json    00004__group.json    00007__group.json    00010__group.json    00013__grc
00002__group.json    00005__group.json    00008__group.json    00011__group.json    00014__grc
(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'
```

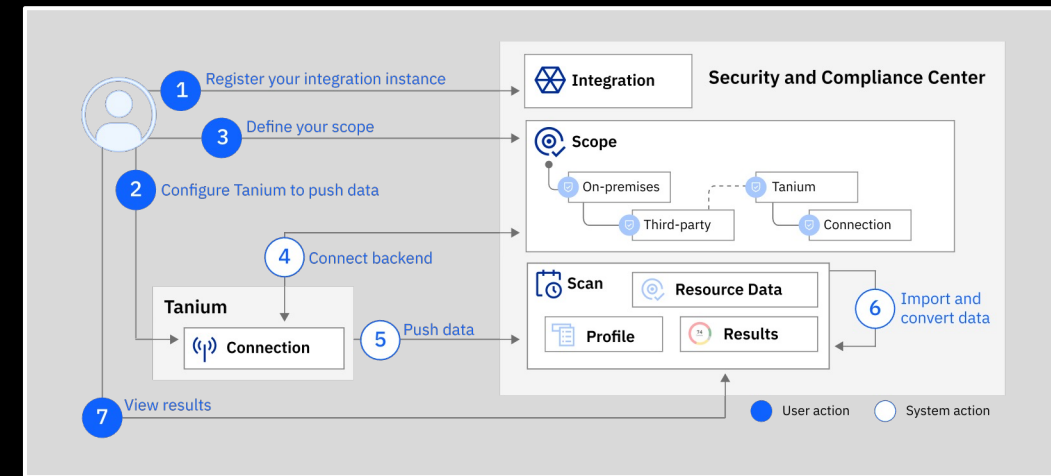
Trestle used to break down an OSCAL catalog

Trestle merging and validating content meets schema / extended requirements

Trestle SDK: Tasks and Transformers

Requirement: Using trestle as an SDK to safely and automatically create OSCAL artifacts (Transitioning from 3rd party content to OSCAL)

- In order for OSCAL to provide value a set of converters are required from various formats.
- Trestle contains transformers which can be used both as an SDK and a CLI (e.g.: <https://ibm.github.io/compliance-trestle/tutorials/task.tanum-to-oscal/transformation/>)
- Trestle conversion SDK is the basis for 3rd party conversions into IBM 'Security and Compliance Centre'
- Trestle OSCAL object model can easily be used to convert content:
 - Excel files
 - XML content
- Demos <https://github.com/IBM/compliance-trestle-demos/>



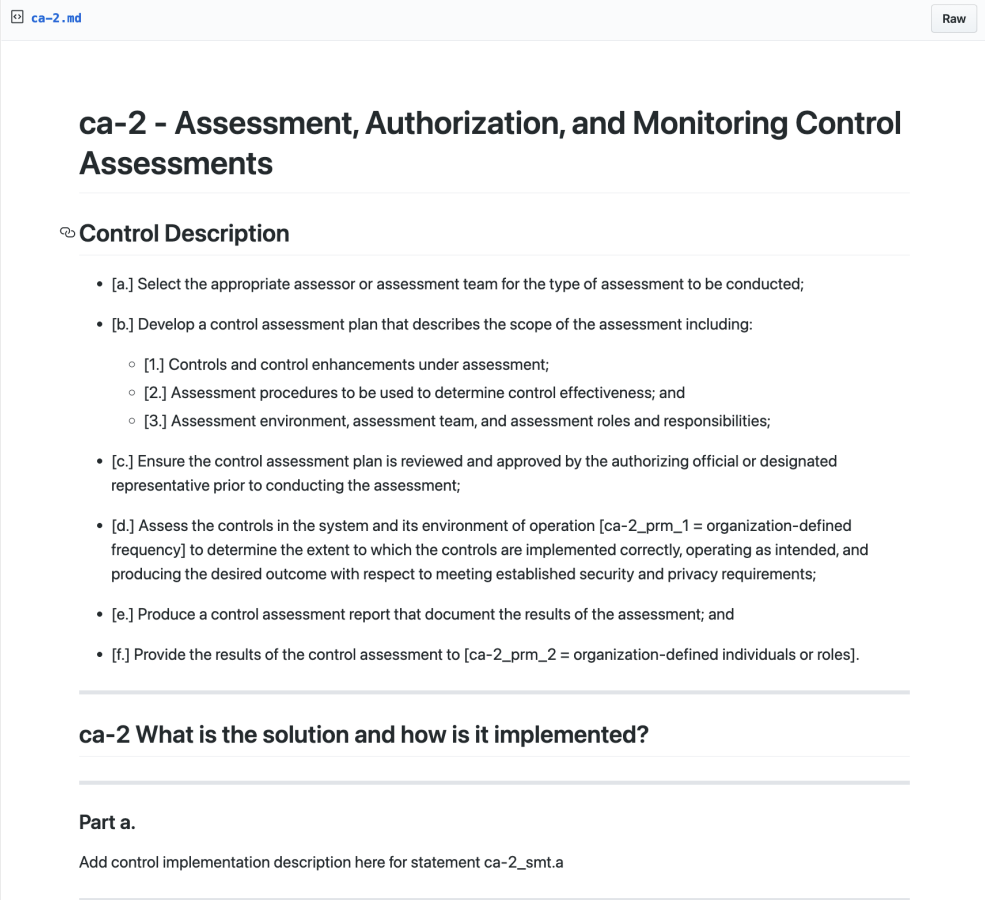
Content Authoring

Requirement: As a service team I would like to provide documentary artifacts to architecture / compliance / security only once.

- Based on an internal use case: Service teams are burdened by operational requirements
 - Particularly when multiple audits / reviews need to be conducted in parallel
- `trestle author`, combined with tests of OSCAL content, are used to enforce service teams follow templating.
 - Templates distributed by using ``git submodules`` for global consistency
- This allows CISO (as an example) teams to pull information from service teams confidently for reviews / audits / external documents.
- Allows service teams to manage all required artifacts in their VCS system and only have one system for approvals.
- Simplified demonstration using arc42 architecture templates.
 - <https://github.com/IBM/compliance-trestle-arc42-demo/>

Agile Authoring: SSP generation

- Requirement: As an a ‘system security plan’ author I need a workflow that allows me to have SMEs authors and reviewers edit and approve in parallel.
- ‘System security plans’ are complex documents requiring multiple users to edit and review
- Migrated SSP creation to per-control markdown in Github enterprise allowing users to edit individual files.
- Markdown provides an easy transformation path to oscal / HTML / other outputs.
- [trestle author ssp-generate](#) and `ssp-assemble` manage the workflow allowing information to be aggregated.
- CICD to validate that users content.
- Used for producing audited documentation currently.



The screenshot shows a markdown editor interface for a file named 'ca-2.md'. The main heading is 'ca-2 - Assessment, Authorization, and Monitoring Control Assessments'. Below this is a section titled 'Control Description' which contains a list of six items (a-f) detailing the assessment process. Item [a.] mentions selecting an assessor, [b.] mentions developing a plan with sub-points for controls, procedures, and environment, [c.] mentions review and approval, [d.] mentions assessing controls with a placeholder for frequency, [e.] mentions producing a report, and [f.] mentions providing results with a placeholder for roles. Below the list is a section titled 'ca-2 What is the solution and how is it implemented?' followed by a sub-section 'Part a.' and a placeholder text 'Add control implementation description here for statement ca-2_smt.a'.

ca-2 - Assessment, Authorization, and Monitoring Control Assessments

Control Description

- [a.] Select the appropriate assessor or assessment team for the type of assessment to be conducted;
- [b.] Develop a control assessment plan that describes the scope of the assessment including:
 - [1.] Controls and control enhancements under assessment;
 - [2.] Assessment procedures to be used to determine control effectiveness; and
 - [3.] Assessment environment, assessment team, and assessment roles and responsibilities;
- [c.] Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
- [d.] Assess the controls in the system and its environment of operation [ca-2_prm_1 = organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
- [e.] Produce a control assessment report that document the results of the assessment; and
- [f.] Provide the results of the control assessment to [ca-2_prm_2 = organization-defined individuals or roles].

ca-2 What is the solution and how is it implemented?

Part a.

Add control implementation description here for statement ca-2_smt.a

Catalog

Markdown

```

---
x-trestle-set-params:
  sc-7_prm_1:
    select:
      choice:
        - physically
        - logically
sort-id: sc-07
---

# sc-7 - \[System and Communications Protection\] Boundary Protection

## Control Statement

The information system:

- \[a.\] Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

- \[b.\] Implements subnetworks for publicly accessible system components that are {{ insert: param, sc-7_prm_1 }} separated from internal organizational networks; and

- \[c.\] Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

## Control guidance

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

```

OSCAL JSON

```

▼ catalog:
  uuid: "b954d3b7-d2c7-453b-8eb2-459e8d3b8462"
  ▶ metadata: {...}
  ▼ groups:
    ▶ 0: {...}
    ▼ 15:
      id: "sc"
      class: "family"
      title: "System and Communications Protection"
      ▼ controls:
        ▶ 0: {...}
        ▼ 6:
          id: "sc-7"
          class: "SP800-53"
          title: "Boundary Protection"
          ▼ params:
            ▼ 0:
              id: "sc-7_prm_1"
              ▼ select:
                ▼ choice:
                  0: "physically"
                  1: "logically"
          ▼ props:
            ▶ 0: {...}
            ▼ 1:
              name: "sort-id"
              value: "sc-07"
          ▶ links: [...]
          ▼ parts:
            ▼ 0:
              id: "sc-7_smt"
              name: "statement"
              prose: "The information system:"
              ▼ parts:
                ▼ 0:
                  id: "sc-7_smt.a"
                  name: "item"
                  ▶ props: [...]
                  ▼ prose: "Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;"
                ▶ 1: {...}

```



Profile	
Markdown	OSCAL JSON
<pre> --- x-trestle-set-params: sc-7_prm_1: select: choice: - physically - logically sort-id: sc-07 --- # sc-7 - \[System and Communications Protection\] Boundary Protection ## Control Statement The information system: - \[a.\] Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; - \[b.\] Implements subnetworks for publicly accessible system components that are {{ insert: param, sc-7_prm_1 }} separated from internal organizational networks; and - \[c.\] Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. # Editable Content <!-- Make additions and edits below --> <!-- The above represents the contents of the control as received by the profile, prior to additions. --> <!-- If the profile makes additions to the control, they will appear below. --> ## Control additional_fs_cloud_guidance The organization "service delivery" and "corporate" environments must be maintained as separate environments. That is, clear physical and/or logical boundaries separating the two environments must exist. </pre>	<pre> { "profile": { "uuid": "f2033a5f-afd9-4139-b8bd-fb28c9e86c62", "metadata": {}, "imports": { "0": {}, "1": { "href": "trestle://catalogs/NIST_800-53_rev4/catalog.json", "include-controls": { "0": { "with-ids": { "0": "ac-1", "1": "ac-2", "218": "sc-6", "219": "sc-7", "220": "sc-7.4" } } } } }, "merge": { "combine": { "method": "merge", "as-is": true }, "modify": { "set-parameters": { "0": { "param-id": "ac-1_prm_2", "values": { "0": "at least annually" } }, "1": {} } }, "alters": { "0": {}, "56": { "control-id": "sc-7", "adds": { "0": { "position": "after", "by-id": "sc-7_smt", "parts": { "0": { "id": "sc-7_additional_fs_cloud_guidance", "name": "additional_fs_cloud_guidance", "title": "additional_fs_cloud_guidance", "prose": "The organization \"service delivery\" and \"corporat </pre>

Component Definition									
Spreadsheet									
rule_name_id	Rule Description	NIST Mappings				Resource	Parameter	Values default , [alternatives]	
vpc_security_groups_inbound_no_ssh_port	Ensure Virtual Private Cloud (VPC) security groups have no inbound rules that specify source IP 0.0.0.0/0 to SSH port.	AC-4	CM-2	SC-7 (3)	SC-7 (5)	VPC	SSH Port ssh_port	22, []	
vpc_security_groups_inbound_no_rdp_port	Ensure Virtual Private Cloud (VPC) security groups have no inbound rules that specify source IP 0.0.0.0/0 to RDP port.	AC-4	CM-2	SC-7 (3)	SC-7 (5)	VPC	RDP Port rdp_port	3389, []	
vpc_no_default_security_group_rules	Ensure Virtual Private Cloud (VPC) has no rules in the default security group	AC-4	CM-2	SC-7 (3)	SC-7 (5)	VPC			



```

OSCAL JSON
{
  "component-definition": {
    "uuid": "11b9da4c-d461-4659-ba33-d147b207db37",
    "metadata": {
      "title": "Component definition for NIST Special Publication 800-53 Revision 4 profiles",
      "last-modified": "2022-05-17T18:14:01+00:00",
      "version": "1.0.2",
      "oscal-version": "1.0.2",
      "roles": [],
      "parties": [],
      "responsible-parties": []
    },
    "components": {
      "0": {},
      "27": {
        "uuid": "85c0ec18-76c7-4168-9868-542f595657c1",
        "type": "Service",
        "title": "VPC",
        "description": "VPC",
        "control-implementations": {
          "0": {
            "uuid": "8f6b28df-8156-4bb8-a30d-a7eb25611670",
            "source": "https://github.com/usnistgov/oscal-content/blob/master/nist.gov/SP800-53/rev4/json/NIST_SP-800-53_rev4_catalog.json",
            "description": "VPC implemented controls for NIST Special Publication 800-53 Revision 4. It includes assessment asset configuration for CIDC.",
            "set-parameters": {
              "0": {
                "param-id": "ssh_port",
                "values": {
                  "0": "22",
                  "1": {},
                  "2": {},
                  "3": {},
                  "4": {}
                }
              }
            },
            "implemented-requirements": {
              "0": {},
              "1": {},
              "2": {
                "uuid": "ee728d16-0d6d-4274-80db-1b32d1bafb0e",
                "control-id": "sc-7",
                "description": "sc-7",
                "props": {
                  "0": {
                    "name": "rule_name_id",
                    "ns": "http://ibm.github.io/compliance-trestle/schemas/oscal/cd/ibm-cloud",
                    "value": "vpc_security_groups_inbound_no_ssh_port",
                    "class": "scc_rule_name_id",
                    "remarks": "Ensure Virtual Private Cloud (VPC) security groups have no inbound rules that specify source IP 0.0.0.0/0 to SSH port."
                  }
                },
                "set-parameters": {
                  "0": {
                    "param-id": "ssh_port",
                    "values": {
                      "0": "22",
                      "1": {},
                      "2": {},
                      "3": {}
                    }
                  }
                },
                "responsible-roles": {}
              }
            }
          }
        }
      }
    }
  }
}

```

Component Definition

Markdown	OSCAL JSON
<pre> --- x-trestle-rules: - vpc_security_groups_inbound_no_ssh_port - vpc_security_groups_inbound_no_rdp_port - vpc_no_default_security_group_rules sort-id: sc-07 --- # sc-7 - \[System and Communications Protection\] Boundary Protection ## Control Statement The information system: - \[a.\] Monitors and controls communications at the external boundary of ... - \[b.\] Implements subnetworks for publicly accessible system component ... - \[c.\] Connects to external networks or information systems only ... <hr/> ## What is the solution and how is it implemented? <!-- Enter implementation details in the parts below. --> <hr/> ## Overall Control <hr/> ## Implementation a. The provider should ensure VPC security groups have no inbound rules ... <hr/> ## Implementation b. <hr/> ## Implementation c. The provider should ensure VPC has no rules in the default security group ... <hr/> </pre>	<pre> 27: uuid: "85c0ec18-76c7-4168-9868-542f595657c1" type: "Service" title: "VPC" description: "VPC" control-implementations: 0: uuid: "8f6b28df-8156-4bb8-a30d-a7eb25611670" source: "https://github.com/usnistgov/oscal-conte description: "VPC implemented controls for NIST Specia set-parameters: [...] implemented-requirements: 0: {} 1: {} 2: uuid: "ee728d16-0d6d-4274-80db-1b32d1bafb0e" control-id: "sc-7" description: "sc-7" props: 0: name: "rule_name_id" ns: "http://ibm.github.io/compliance-trestle/ value: "vpc_security_groups_inbound_no_ssh_port" class: "scc_rule_name_id" remarks: "Ensure Virtual Private C... 0.0.0.0/0 to S 1: {} set-parameters: 0: param-id: "ssh_port" values: 0: "22" statements: 0: statement-id: "sc-7_smt.a" uuid: "ee3034cc-f306-4578-85c7-49b98fc5f83f" description: "The provider should ensure VPC security 1: statement-id: "sc-7_smt.c" uuid: "ee3034cc-f306-4578-85c7-49b98fc5f83e" description: "The provider should ensure VPC has no r 3: {} 4: {} </pre>

Component Definition

Spreadsheet

rule_name_id	check_name_id	NIST Mappings					Resource	Check implemented
vpc_security_groups_inbound_no_ssh_port	check_vpc_security_groups_inbound_no_ssh_port	AC-4	CM-2	SC-7	SC-7 (3)	SC-7 (5)	VPC	yes
vpc_security_groups_inbound_no_rdp_port	check_vpc_security_groups_inbound_no_rdp_port	AC-4	CM-2	SC-7	SC-7 (3)	SC-7 (5)	VPC	yes
vpc_no_default_security_group_rules	check_vpc_no_default_security_group_rules	AC-4	CM-2	SC-7	SC-7 (3)	SC-7 (5)	VPC	no



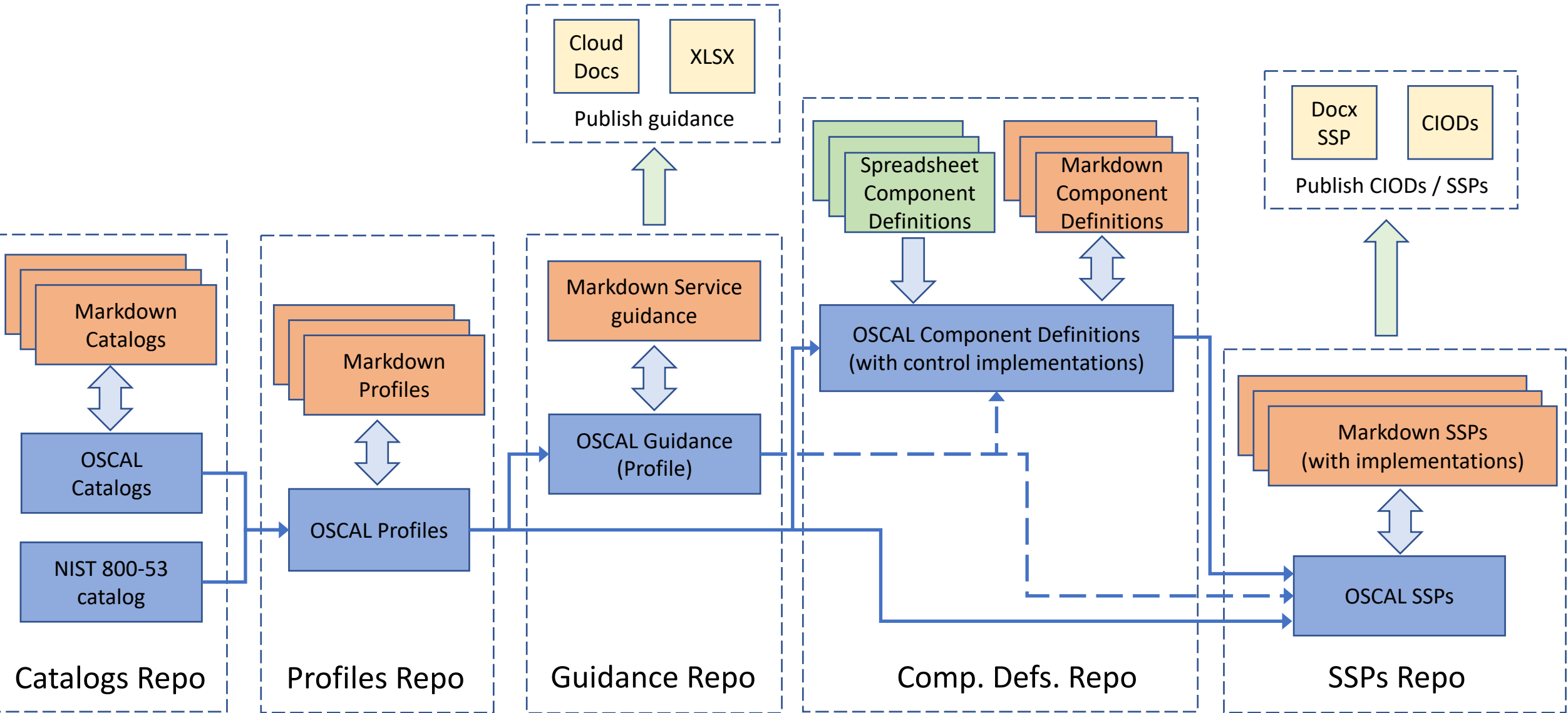
OSCAL JSON

```

component-definition:
  uuid: "11b9da4c-d461-4659-ba33-d147b207db37"
  metadata:
    title: "Component definition for NIST Special Publication 800-53 Revision 4 profiles"
    last-modified: "2022-05-17T18:14:01+00:00"
    version: "1.0.2"
    oscal-version: "1.0.2"
    roles: [...]
    parties: [...]
    responsible-parties: [...]
  components:
    0: {}
    6:
      uuid: "943f6235-3ae9-4237-97d6-e67d20e46802"
      type: "Validation"
      title: "TOOLCHAIN"
      description: "TOOLCHAIN"
      control-implementations:
        0:
          uuid: "6531a82b-5788-455e-a6b4-7b383bc13802"
          source: "https://github.com/usnistgov/oscal-content/blob/master/nist.gov/SP800-53/rev4/json/NIST_SP-800-53_rev4_catalog.json"
          description: "TOOLCHAIN checks for NIST Special Publication 800-53 Revision 4. It includes assessment asset configuration for ICID."
          implemented-requirements:
            0:
              uuid: "6e22190f-d9fd-48a7-896a-ec0be0244659"
              control-id: "sc-7"
              description: "sc-7"
              props:
                0:
                  name: "rule_name_id"
                  ns: "http://ibm.github.io/compliance-trestle/schemas/oscal/cd/ibm-cloud"
                  value: "vpc_security_groups_inbound_no_ssh_port"
                  class: "scc_rule_name_id"
                  remarks: "link100"
                1:
                  name: "check_name_id"
                  ns: "http://ibm.github.io/compliance-trestle/schemas/oscal/cd/ibm-cloud"
                  value: "check_vpc_security_groups_inbound_no_ssh_port"
                  class: "scc_check_name_id"
                  remarks: "link101"
                2: {}
                3: {}
              responsible-roles: [...]
            1: {}
  
```

SSP	
Markdown	OSCAL JSON
<pre> --- x-trestle-props: control-origination: - Shared (Service Provider and Customer Responsibility) implementation-status: - implemented responsible-roles: - Customer sort-id: sc-07 --- # sc-7 - \[System and Communications Protection\] Boundary Protection ## Control Statement The information system: - \[a.\] Monitors and controls communications at the external ... - \[b.\] Implements subnetworks for publicly accessible ... - \[c.\] Connects to external networks or information systems only through ... ## Control guidance Managed interfaces include, for example, gateways, routers, firewalls ... ## What is the solution and how is it implemented? <!-- Please leave this section blank and enter implementation details in the parts below. --> ## Overall Control In IBM platform deny by default is implemented for all public ingress/egress traffic with network policies in place to specifically allow approved traffic. ## Implementation a. ## Implementation b. ## Implementation c. </pre>	<pre> system-security-plan: uuid: "b2d1ec5f-03b6-4974-b6d8-12f10b168050" metadata: {} import-profile: {} system-characteristics: {} system-implementation: {} control-implementation: description: "This is the control implementation for the" implemented-requirements: 0: {} 238: uuid: "c79f6597-7353-4888-918b-e443846b93dd" control-id: "sc-7" props: 0: name: "control-origination" ns: "https://fedramp.gov/ns/oscal" value: "Shared (Service Provider and Customer Resp" 1: {} responsible-roles: [] statements: 0: statement-id: "sc-7_smt.a" uuid: "552c1d98-7c23-49f2-b7c7-fbaebc76331f" by-components: 0: component-uuid: "85c0ec18-76c7-4168-9868-542f595657c1" uuid: "043ae214-fc07-4849-b19e-a232fc1125e8" description: "The provider should ensure VPC security gr" 1: {} 2: {} 3: {} 4: {} 1: {} 2: statement-id: "sc-7_smt.c" uuid: "a9d8b32a-55f7-4792-9288-8dad558a5c66" by-components: 0: component-uuid: "85c0ec18-76c7-4168-9868-542f595657c1" uuid: "33f59425-b088-4b3e-afc5-6972e1d1224e" description: "The provider should ensure VPC has no rul" 1: {} 2: {} 3: {} 4: {} by-components: 0: component-uuid: "a5f624b7-604a-46e4-ba8a-64eed50e0d29" uuid: "043ae214-fc07-4849-b19e-a232fc1125e8" description: "In IBM platform deny by default is impleme" 239: {} </pre>

Agile Authoring Repo Organization



GRC Framework

