Automating Compliance Processes with ibm.github.io/compliance-trestle/

ANCA SAILER
Distinguished Engineer
IBM Research

Agenda

- What is Trestle?
- Compliance Artifacts and Compliance as Code
- Trestle Applications
- Trestle and NIST Compliance as Code Standard:
  Open Security Control Assessment Language (OSCAL)

What is Trestle?

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

Trestle is an open-source for managing compliance artifacts as an automated workflow.

Trestle is a collaborative platform for the various compliance personas to orchestrate their individual aspects of the compliance artifacts via the interface of their choice. The automated workflow ensures their consistency and traceability.

Trestle is an opinionated implementation of the OSCAL NIST standard for compliance as code aiming for the compliance documentation to be maintained continuously up to date.

Compliance Artifacts & their Representation as code

*Regulatory compliance and Org **P**olicy controls are implemented as technical rules (aka **p**olicies) and tested via rule engines or checks based on evidence*

Regulatory Compliance and Org Policies

Example regulatory standards and certifications:

ISM & E8 (AU)

EU

GDPR (EU)

PCI DSS **Level 1**

HIPAA

NIST 800-53

Industry Specific Regulations
in PDF, Spreadsheet format

Regulation Specific:
Controls

e.g.,
NIST 800-53 Controls

System and Communication Protection (SC):
SC-7: Boundary Protection

System and Communication Protection (SC):
SC-28: Protection of Information at Rest

COMPLIANCE as CODE Controls

e.g., OSCAL-CATALOG of controls expressed in json, yaml, xml

OSCAL-PROFILE subset of controls

Technology Specific:

Technical Control Implementations

w/ associated

policy rules & test checks ID

procedures

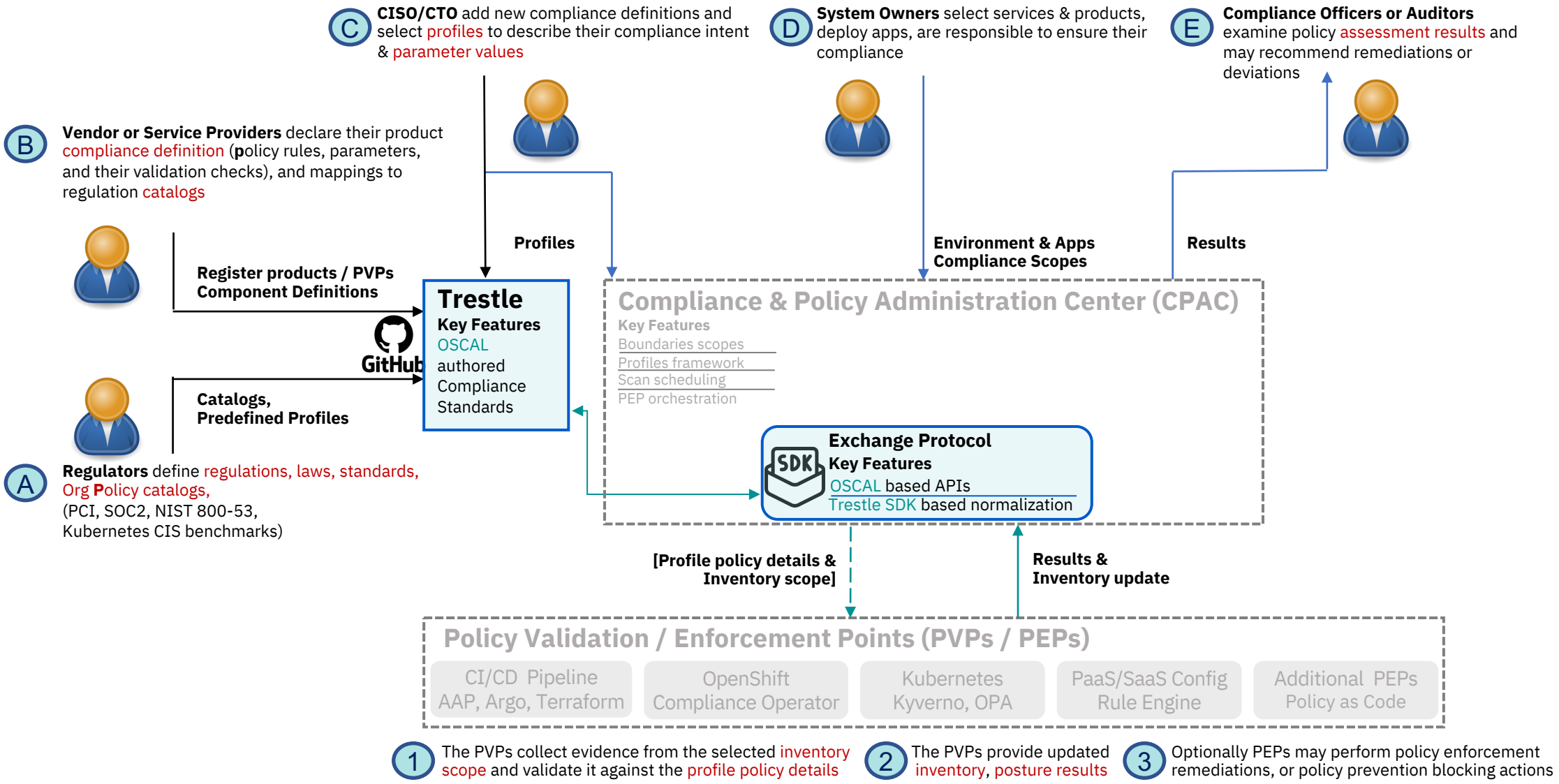
NETWORK SECURITY
Ensure Cloud Object Storage is enabled on *private endpoints*
Ensure Kubernetes ingress is enabled through Cloud Internet Services
Ensure VPC LBaaS is enabled through Cloud Internet Services

DATA SECURITY
Ensure Cloud Object Storage is encrypted with *KYOK*
Ensure Block Storage is encrypted with *KYOK*
Ensure Database Postgres is encrypted with *KYOK*

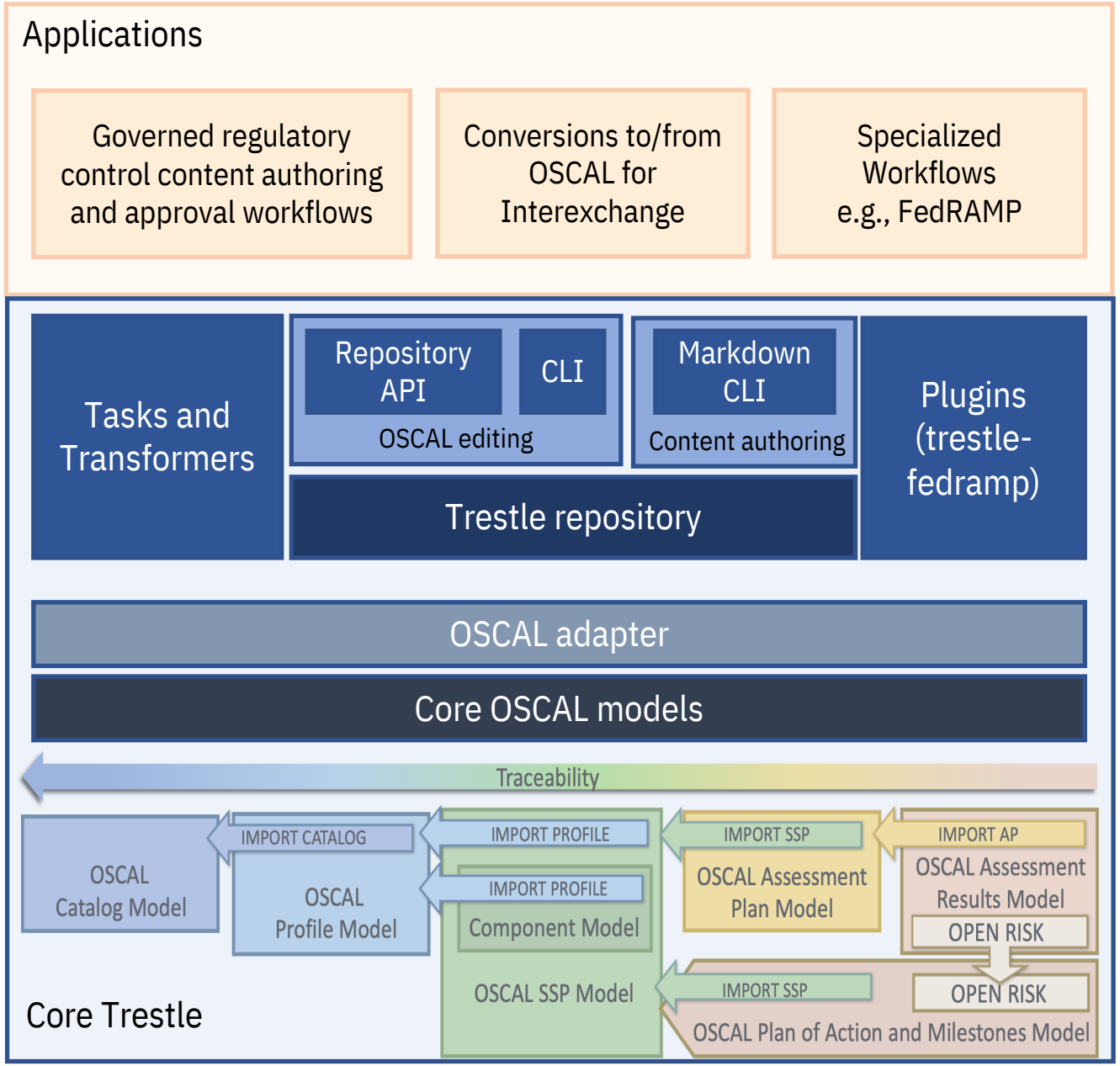
COMPLIANCE as CODE Rules
e.g., OSCAL-COMPONENT DEFINITION of mapping of controls to rules and *params* expressed in json, yaml, xml

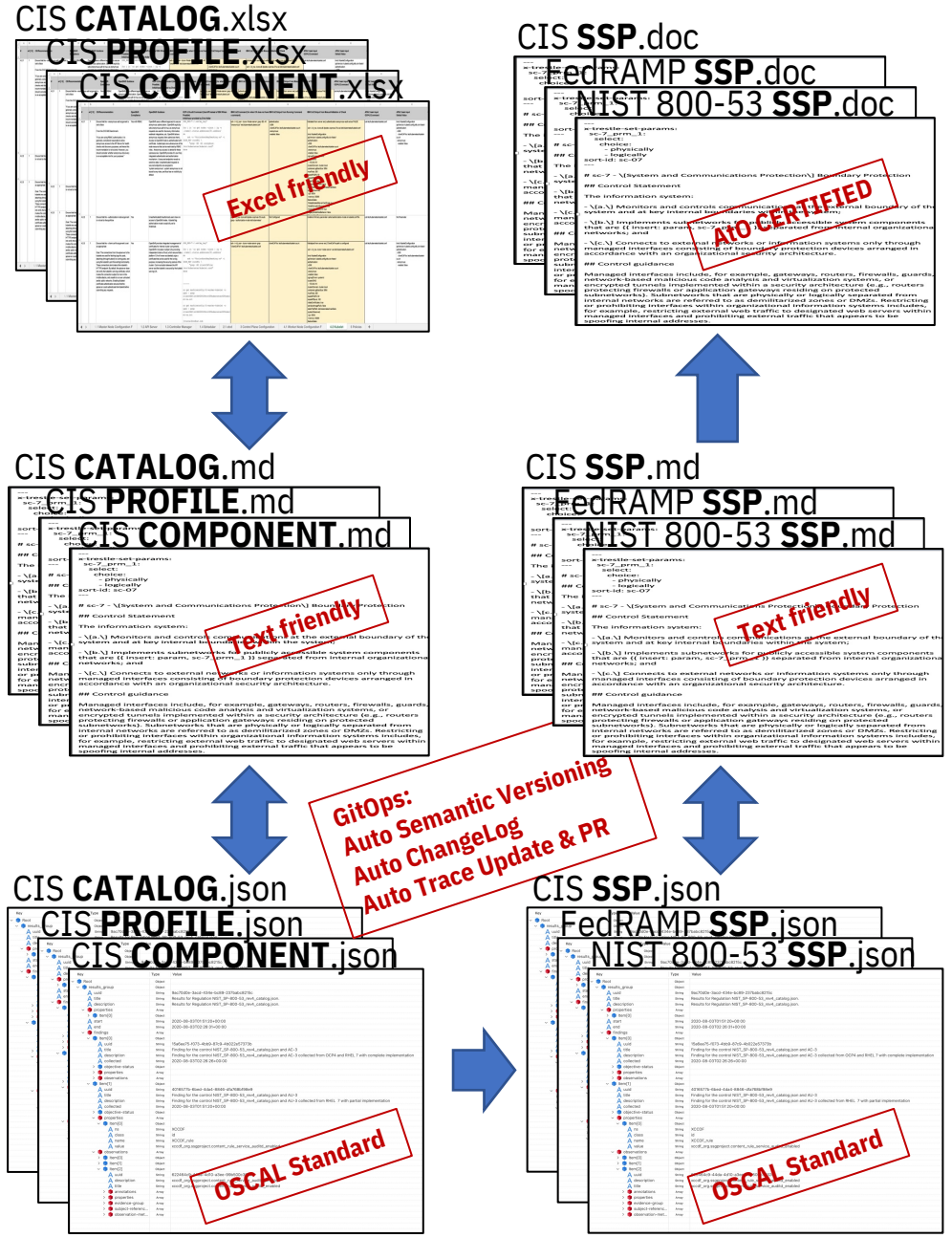
COMPLIANCE as CODE Results
e.g., OSCAL-ASSESSMENT RESULTS with observations, findings and risks

Compliance Personas and Roles



Compliance-Trestle – NIST Open Security Control Assessment Language (OSCAL) & Applications





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

Blogs:

Compliance Part 1: Personas and Roles

Compliance Part 2: Trestle SDK

Compliance Part 3: Artifacts and Personas

Thank you!