CLOUD NATIVE
COMPUTING FOUNDATION

OSCAL Compass

OSCAL-COMPASS
Open Security Control Assessment Language
Compliance Automated Standard Solution

OSCAL Compass

Towards standardization, digitization, and automation of compliance

- Direct contribution to a **CNCF open-source project**
- Opportunity for **big impact** – help us **move from CNCF sandbox to incubating**
- **Hands-on** skill development - practical applications of OSCAL concepts

Develop Your Skills

Compliance Automation & Contribution Essentials

- Open source **contribution workflows** for collaborative coding
- **Exposure to diverse** set of technologies
  - Git
  - Python
  - Go
- Application of **compliance** concepts
  - Automating compliance
  - OSCAL, standardized formats, and interoperability

Tools for Your Journey

Visit the Slam Backlog: A curated set GitHub Issues for the event https://github.com/orgs/oscal-compass/projects/11/views/1

Flexibility on Time and Tasks

- Different levels of contributions (small, medium, large)
  - Documentation improvement - *small*
  - Improvement to demos - *medium*
  - Adding new functionalities - *large*

Ready to Contribute?

Read our Documentation:
https://github.com/oscal-compass/community/blob/main/CODE_OF_CONDUCT.md
https://github.com/oscal-compass/community/blob/main/CONTRIBUTING.md

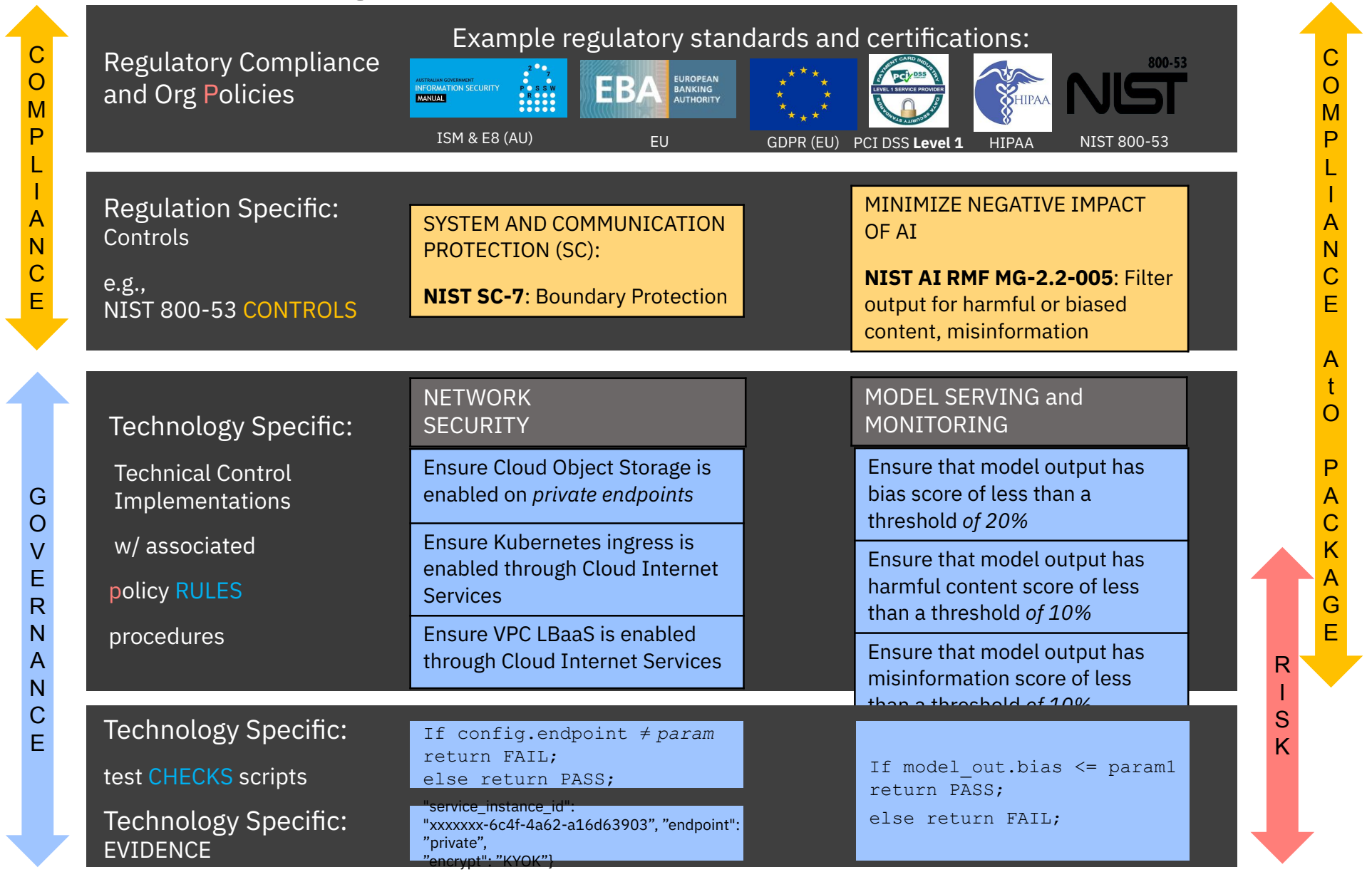
Connect with the Community

- Join the CNCF Slack channel - #oscal-compass-trestle-agileauthoring-c2p
  - CNCF Slack Workspace Access
- Office Hours
  - OSCAL Compass maintainers will hold daily office hours during the event

Background

Compliance Artifacts and their Representation as code

Regulatory compliance and Org Policy controls are implemented as rules (technical, operational, financial, data, or AI) and tested via rule engines or checks based on evidence

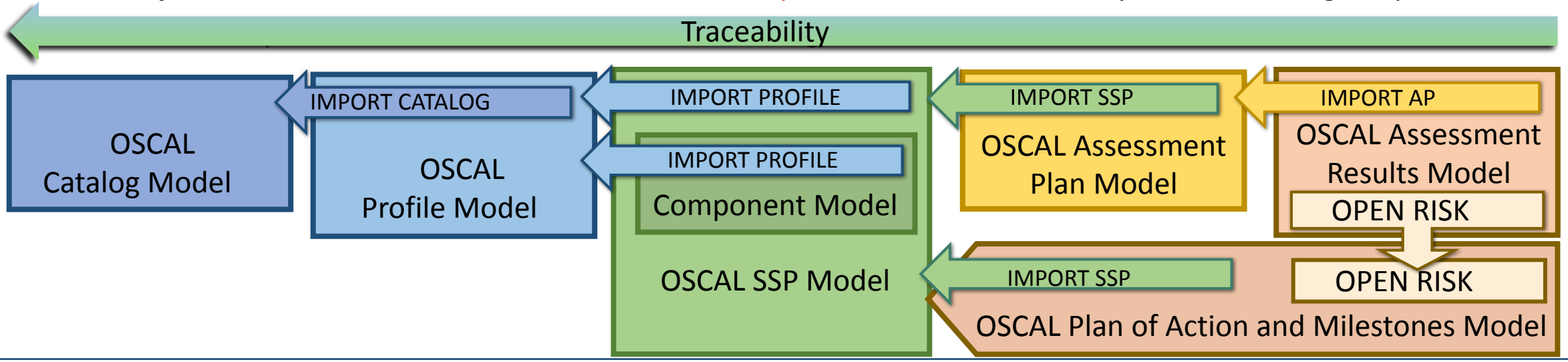


What is OSCAL?

Credit: NIST

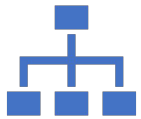
OSCAL is the result of NIST and FedRAMP collaboration

- **OSCAL provides** a common machine-readable language, expressed in XML, JSON and YAML for:
  - multiple compliance and risk management frameworks (e.g., SP NIST 800-53, ISO/IEC 27001&2, COBIT 5)
  - software and service providers to express implementation guidance against security controls (Component definition)
  - system owners to share how security controls are implemented in an actual environment (System Security Plans [SSPs])
  - sharing security assessment plans (System Assessment Plans [SAPs])
  - sharing security assessment results/reports (System Assessment Results [SARs])
  - sharing plans of actions for remediations and mitigation
- **OSCAL provides** a framework for automated traceability from selection of security controls through implementation and



OSCAL, Trestle, Agile Authoring, Compliance-to-Policy

https://pages.nist.gov/OSCAL/
https://github.com/oscal-compass
https://github.com/oscal-compass/compliance-trestle
https://oscal-compass.github.io/compliance-trestle/



OSCAL is a NIST framework & language **for managing compliance artifacts as code end-to-end**

From selection of security controls through implementation and assessment

To plans of actions for remediations and mitigation

TRESTLE is an **opinionated implementation of the OSCAL standard**

Allows editing and manipulation of OSCAL documents while making sure the schemas are enforced

Provides an SDK

AGILE AUTHORING is a **collaborative platform** enabling various compliance personas to orchestrate their individual aspects of the compliance artifacts via an interface of their choice

Trestle-based GitOps automated workflow

Ensures artifacts consistency and traceability

COMPLIANCE_TO_POLICY is a GitOps extension as a pluggable bridge to normalize the policy administration in the policy validation tools

Bridge between compliance-as-code and policy-as-code

Keep up with Compass and Trestle

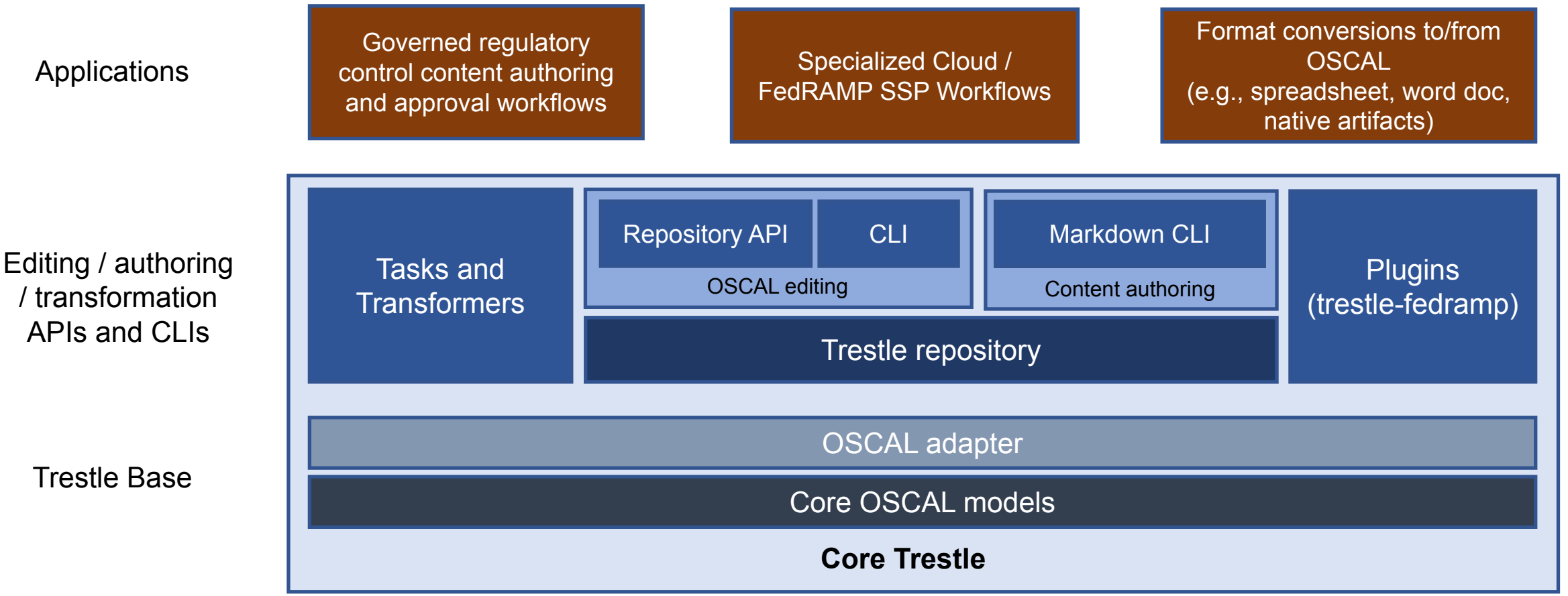
- Community calls
  - OSCAL Compass community calls - https://docs.google.com/document/d/1XTYM7xnWlIqd-8Nn5-qtgvgk8kH3NSmYle5yZvaS7qs/edit#heading=h.6pq38r2red0n

- Github organization
  - oscal-compass - https://github.com/oscal-compass

- Blogs
  - Personas and Roles
  - Trestle SDK
  - Artifacts and Personas
  - Topologies of Compliance Policy Administration Centers
  - A Lack of Network Boundaries Invites a Lack of Compliance
  - Compliance to Policy for Multiple Kubernetes Clusters

Project Deep Dive

Trestle Architecture



Compliance-to-Policy (C2P) and plugin architecture

- Flexibility in choice of policy engines and compliance framework
- Community-driven plugin extension