OSCAL Adoption
For Continuous Assurance & Beyond

Google Cloud CISO
Vikram Khare - Director Continuous Assurance Engineering
Valentin Mihai - Technical Lead
Agenda

Moving Towards Continuous Assurance
Adoption Challenges
Aligning The Data
Process and Systems Overview
Aspirational: Future Plans
Introductions

Vikram Khare
Continuous Assurance Engineering

Valentin Mihai
Technical Lead
Objective: Continuous Assurance

The Case for OSCAL

- OSCAL is an integral part of enabling continuous assurance.
  - Method for exchanging risk & controls data with customers & partners
  - Comprehensive taxonomy for GRC & CCM (Continuous Controls Monitoring) platforms
  - Tooling ecosystem built with OSCAL support can enable interoperability

Defining Continuous Assurance

- Continuous Assurance
  - Opinion: Continuous assurance is an umbrella term for industry buzzwords:
    - Compliance/Privacy/Security by Design
    - Policy as Code
    - Continuous Compliance
  - Tangible: Automation of assurance activities and the enablement of real time monitoring of controls based on objectively defined metrics
    - Treat compliance failures like systems downtime
Challenges for Adoption

Minor
- Timeline to support OSCAL automation
  - OSCAL builder tooling
  - Control on-boarding tooling
- Control data change management process
- Emerging standard
- Taxonomy adoption

Major
- 3P Software Challenges
  - Performance
  - Complexity with systems integrations
- Operationalization at scale
- Technical Debt: Gaps must be remediated immediately
Moving Towards Continuous Assurance

**Phase 1: POC**
Deliver a manual driven automation enable OSCAL generation from sheets.

**Phase 2: MVP**
Deliver tool that will provide a user friendly UI, and UUID persisted.

**Phase 3: Data Pre-Population**
Data pre-populated from GRC, asset inventory for vulnerability management, as well integration of validation rules.
Additional usability enhancements.

**Phase 4: Maturation**
Two-way integration with GRC, enhanced collaboration features, and format support.
Future items including external publication, ConMon support, etc.

Templates / Scripts

OSCAL Builder P0

OSCAL Builder P1

OSCAL Builder P2 + Future
Aligning The Data

Regulatory Decomposition
- Needed to change the way that regulations are decomposed for internal consumption and evaluation

Establishing a granular structure for defining controls
- Need the ability to draw a straight line from the regulatory requirements, through the control implementation, down to the individual control metrics

Refining the Asset Model
- Establish an asset taxonomy that aligns with current tooling, automation and management capabilities, but that can also align with a common data structure (how do we consume systems and component structures with our current asset mgmt systems)

Aggregating Data From Disparate Sources
- OSCAL definition of a control requires a higher level of granularity:
  - Complete rewrite of the GRC data model
  - Population of data from external source into centralized GRC
Example Requirement Breakdown

Scaling Requires:
- Diffusion of responsibility
- Granularity of requirements to facilitate automation

Anti Virus Control from FooRAMP

Title: [FooRamp] AC-1: Anti Virus Requirements for Cloud Service Providers

Description:
The provider has an antivirus program:
1. Scans are run on prod daily
2. AV findings are assessed and remediated within 24hrs
3. All incoming data is scanned

OSCAL Adopted Control Mapping

Requirement ID: AC-1a.1
Requirement Hierarchy: Access Control | Access Control Policy and Procedures
Title: CSP Has an AntiVirus Program

Description: The provider has an antivirus program:
1. Scans are run on prod daily

Requirement ID: AC-1b.1
Requirement Hierarchy: Access Control | Access Control Policy and Procedures
Title: CSP Has an AntiVirus Program

Description: The provider has an antivirus program:
1. All incoming data is scanned

Requirement ID: AC-1a.2
Requirement Hierarchy: Access Control | Access Control Policy and Procedures
Title: CSP Has an AntiVirus Program

Description: The provider has an anti-virus program:
1. AV findings are assessed and remediated within 24hrs
CONTROL-XXXX: CSP has an AV program

CONTROL-XXXX: AV scans run daily in prod

CONTROL-XXXX: All AV findings resolved in 24 hrs

CONTROL-XXXX: All incoming in data DCs is scanned daily

Cloud - US

Cloud - CA

Control Implementation Object in GRC

Control-Implementation-XXXX: CSP has an AV program that does the following:

Control-Implementation-XXXX: In NA DC, CSP runs daily scans using Company Foo x,y,z on all production systems

Control-Implementation-XXXX: AV scan results are sent to local NA AV-Sec teams, that work with dev, eng, and SRE to resolve any findings in 24hr, bugs are managed in US Issue Tracking System

Control-Implementation-XXXX: All files are uploaded to an FTP, and are then scanned and moved to prod. scans done by Company Bar

Component Model

Component-XXX

Company Foo

Endpoint Security Suite

Component-XXX

Company Bar

AntiVirus Scanner
CSP has an AV program

AV scans run daily in prod

All AV findings resolved in 24 hrs

All incoming in data DCs is scanned daily

CCM Metrics: % of scans, findings & incoming data measured based on risk appetite

Aggregate of CCM Metrics Determines:
- Red - down
- Yellow - warning
- Green - up

Real time monitoring at the system component level is weighted to determine the overall effectiveness.

Risk thresholds can be defined at more granular levels:
- Ex: 1 missed remediation of low risk AV finding in the 24hr SLO not as critical as failed AV scans
High Level Process

Intake
- Control Gap Identified
- Control Definition
- Reg-Control Mapping
- Control Maturity Review
- Internal Compliance Review
- Risk Identified

Existing Control Modified / Net New Control Created

Cataloging / Onboarding
- Control Creation / Modification
- Assurance Automation
- CCM Measurements

Continuous Assurance
- Audit Artifacts (OSCAL Package)
- Visualization (CRACL)
- Remediation / Incident Mgmt (CRE)
- Continuous Monitoring / Validation
- Alerting / Notification
Systems Overview

**Evidence Repository**
(archival + control evidence)

**Systems of Record**
(archival + control evidence) (Control signals, policies, risk data, third party services, customer commitments, contracts, etc.)

**Immutable Data Storage for Retention**

**GRC, CMDB, CCM, Threat, Risk & Loss Data**

**Visualization of Risk, Controls Data**

**End User Outputs**

**Input**

**OSCAL Outputs**
- SSP
- POAM
- Assessment Plan & Results

**Visualizations**
- Risk Assessment/ Risk Quantification
- Upstream / Alerting monitoring
- Control/ Threat Mapping and Modeling
Areas of Opportunity

1. Audit Toil Reduction
   ● Adoption Beyond US Public Sector
     ○ Expansion of OSCAL to include CCM
     ○ More regulatory bodies to adopt CCM metrics in place of manual audits & assessments
     ○ Participation / collaboration with regulators and standards body to establish data sharing architecture

2. Reg Analysis Toil Reduction
   ● Adoption of machine readable formats for compliance frameworks can greatly reduce time to analyze regs.
     ○ Conversion of existing regulations (banking, privacy regs) into machine readable formats
     ○ Aligning these formats with the different regulatory bodies
       ■ Potential to eliminate confusion on interpreting regulatory requirements

3. Integration of Controls with Broader IT Management & Security Operations
   ● Develop a mechanism to integrate CCM signals into security and incident response functions
   ● Incorporate control effectiveness coverage metrics into threat assessment practices
Thank you.