NIST CSRC OSCAL Workshop Series
c1secure OSCAL Engine

An Enterprise Platform Perspective

C1SECURE IS A SERVICENOW-POWERED SECURITY + SERVICE PROVIDER

Our Team
Introduction

JJ Contessa
Chief Operating Officer
Chief Product Officer
JJContessa@c1secure.com

Todd Hughes
Sr. Security & Compliance
CISSP, CISA
THughes@c1secure.com

Vijay Addicam
Sr. Solutions Architect
Enterprise Platforms
VAddicam@c1secure.com

Steve Grogan
VP of Professional Services
FedCloud Express
SGrogan@c1secure.com

AGENDA

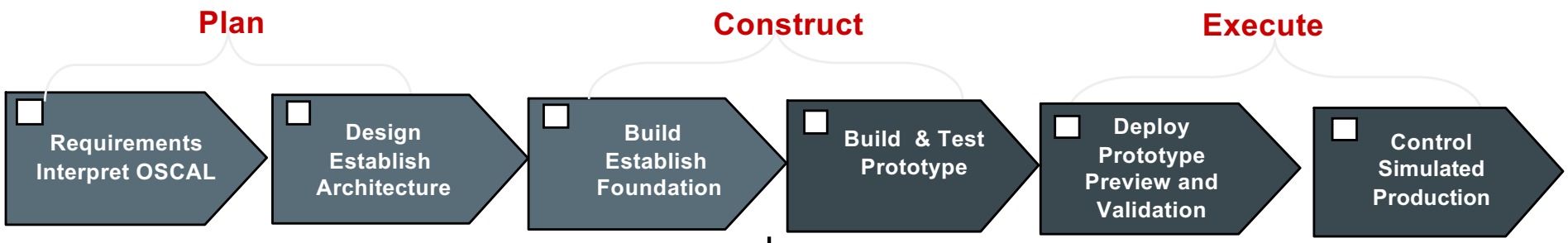
- **Objectives**
  - ➢ Vision, timing, and success measures
- **The Journey**
  - ➢ Challenges, progress, course of action
- **The OSCAL reporting landscape**
  - ➢ Interwoven dependencies
- **OSCAL Engine Architecture**
  - ➢ Intricate, Comprehensive, Highly Relational
- **Roadmap**
  - ➢ Expanding from foundations

1Secure

Objectives - Vision, Timing, Success Measures

- Automation of US Gov Regulatory reporting and continuous monitoring requirements
- Agnostic Plug and Play Application for Enterprise Security and Compliance platforms
- Early adoption “FedRAMP”- efficiencies and benefits targeted to Cloud Service Providers (CSP), Regulatory bodies (FedRAMP PMO, US GOV Agencies), and Third Party Assessor organizations (3PAO)
- CSP and FedRAMP PMO prototype - Q2’23
- NIST/GSA/FedRAMP PMO and 3PAO validation - Q4’23

The Journey – Q1’22 – Q3’23



- OSCAL relational model: POAM, SSP, Profile, Catalog using XML.
- Started with POAM and worked backward to SSP, Profile, and Catalog.
- Built data structure (150+ tables) for each assembly/sub-assemblies.
- Translation map: excel POAM template to OSCAL data schema.
- Created OSCAL output prototypes.
- Created SSP Digital Form (Sections 1-12) and designed automated control integration.
- UI process for management of metadata information.

- Architectural constructs implemented for SSP, PoAM in process.
- SSP prototype in Beta, with live CSP data in proof of value engagements (POV).
- 90% validation outbound (CSP) content and inbound (PMO) processing
- Collaborative previews in process with Stakeholders (CSP, PMO, and 3PAO)

Define - Architect | **Construct – Test - Deploy** | **Monitor**

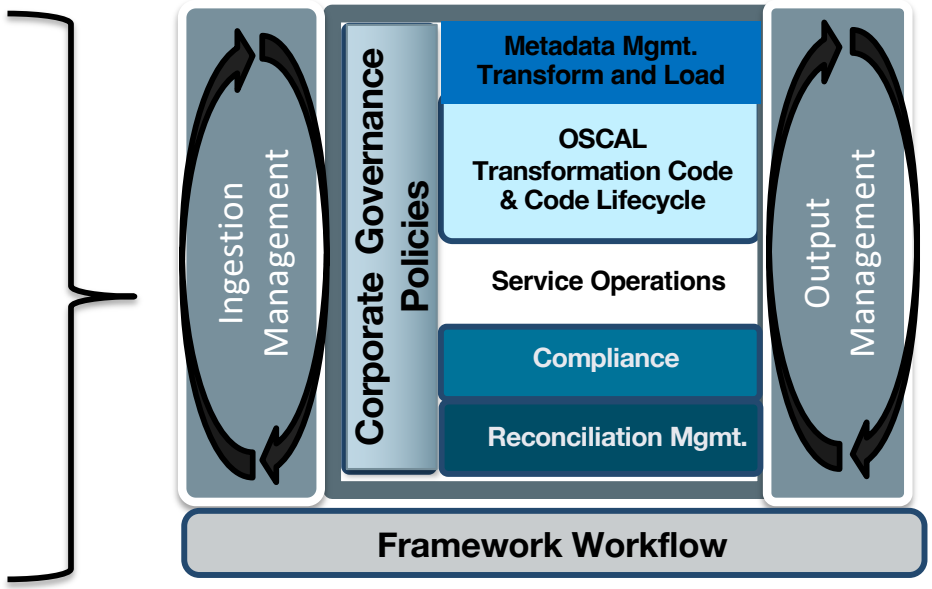
C1secure Innovation Framework Grounded in Structured Execution

OSCAL Engine Ecosystem

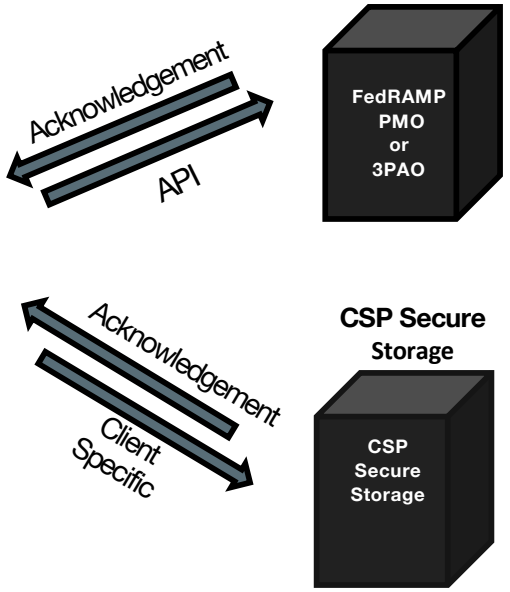
Sources

- **Digital**
  - Sec & Compliance Platform Metadata stores
  - POAM Excel Reports
  - SSP Digital forms
  - HTML
- **Manual**
  - Word Documents
  - Assessments
  - Audit reports

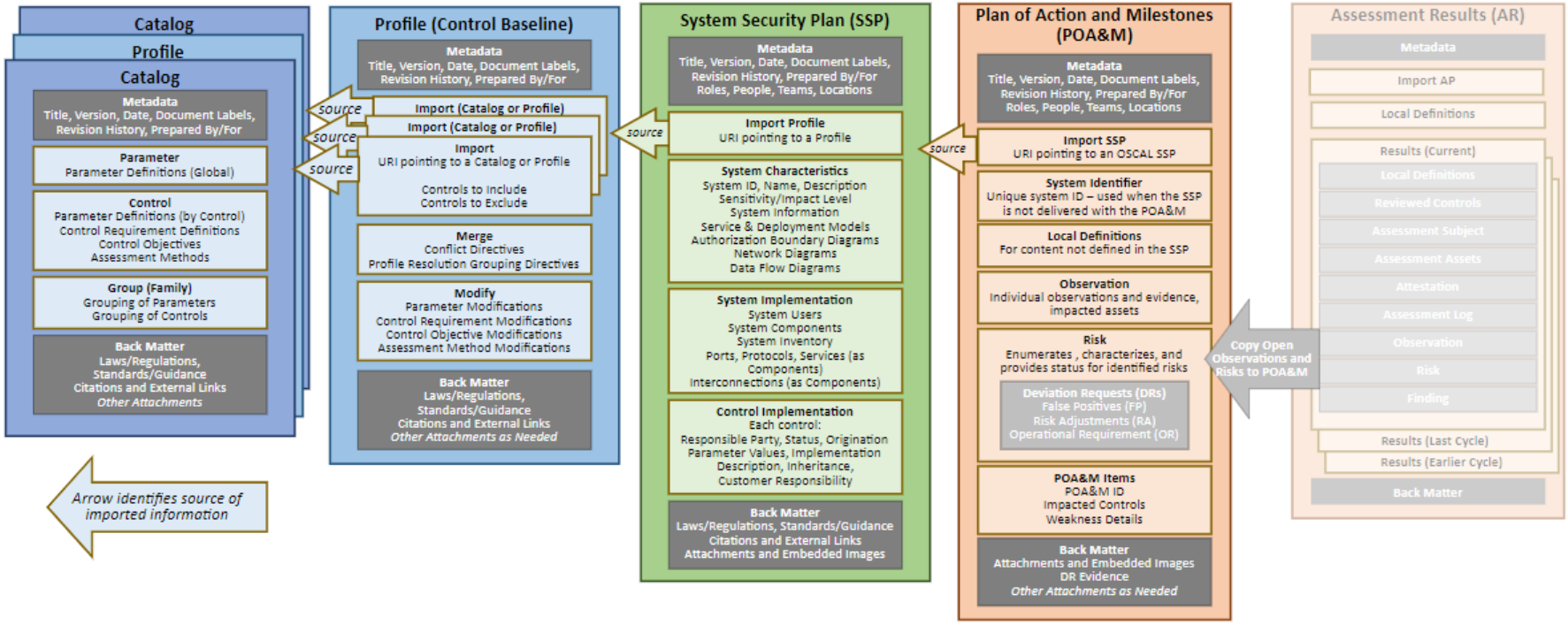
Ingest



OSCAL Reporting

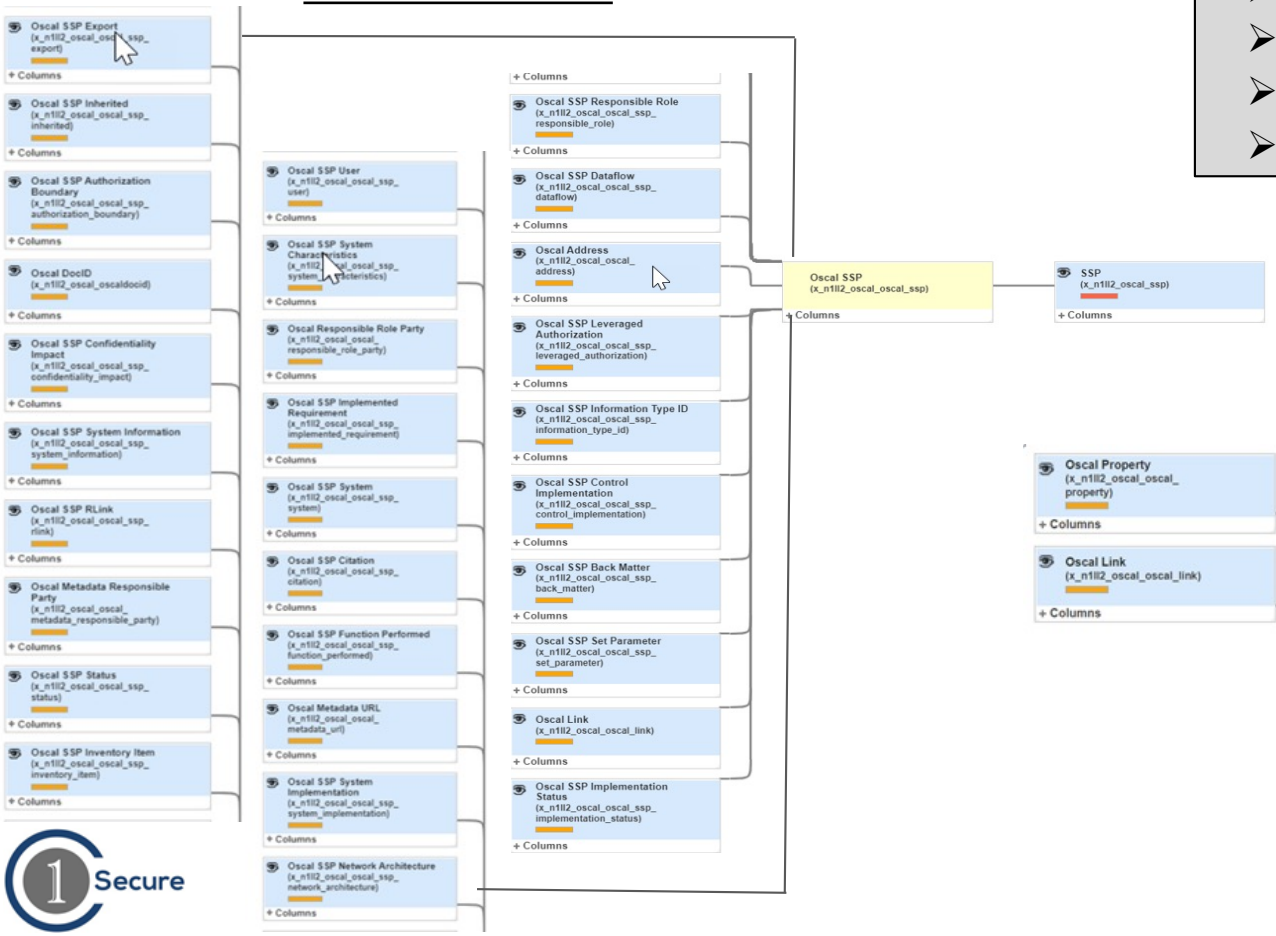


OSCAL Engine Architecture and Reporting Landscape



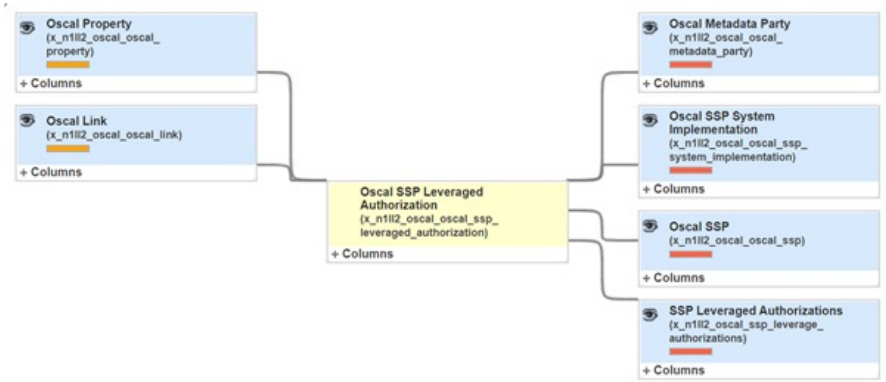
OSCAL Engine Architecture

SSP Relational Schema



- Sample Schema System Security Plan (SSP)
- Significant Metadata granularity
- Complex relational data model
- Diversified Data sources: Manual, Digital, 1>Many>1

SSP Leveraged Authorization



Challenges and Outcomes

REGULATORY REPORTING TAXONOMY – TRANSLATION TO RELATIONAL DATABASE SCHEMA COMPLIMENTARY WITH ENTERPRISE PLATFORMS.	**Architected 4-layer relational schema utilizing MariaDB, SQL, and SQL Databases.**
DATA SOURCE VARIABILITY AND WEIGHT - GRANULARITY, 1 > MANY > 1, EXISTING AND FUTURE STATE.	**Modification of Control Objectives, Supplemental guidance, and implementation details utilizing low code enterprise platform forms designer.**
MANAGEMENT OF EVIDENCE ARTIFACTS – CATALOGUE OF DOCUMENTS, DIAGRAMS, SCREENSHOTS ETC.	**Utilized back matter management capabilities with 2 options: Base 64-bit encoding or provisioning of Hyper-link to source repositories.**
OUTPUT VALIDATION – TOOLS UNDER DEVELOPMENT AND VALIDATION REMAINS EXTERNAL TO THE SOLUTION.	**Established recurring sessions with GSA and others to address Validation Tool errors and/or moving requirements.**
CONFIGURATION MANAGEMENT/CHANGE MANAGEMENT/SECURITY OPERATIONS SEAMLESSLY INTEGRATE BEST OF BREED ENTERPRISE PLATFORM CAPABILITIES.	**A unified platform for compliance, security, and IT operational workflows, management, reporting, etc.**

1 Secure

Roadmap

- GSA Automation Platform Integration – Q4’23
- Adoption of other OSCAL control catalogs
- Output Management Center - Translations to legacy artifacts (Word / Excel) – Q1’24
- POA&M Prototype – Q4’23
- StateRAMP & TX-RAMP – Q1'24
- Identify collaboration partners

THANK YOU

LET’S MAKE THE VISION A REALITY