

SunStone Secure

“OSCAL - A “FastTrack” to Agency Contracting”

Robert Ficaglia - CTO

Robert@SunStoneSecure.com

Mats Nahlinder – CEO

Mats@SunStoneSecure.com



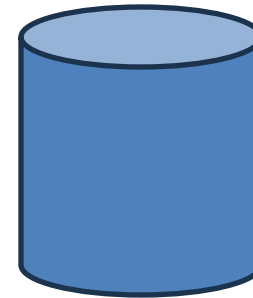
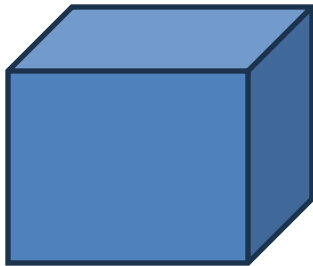
SunStone
Secure By Design

A Different View

Supplier

Marketing 101

Client



Product-Centric Marketing

Customer-Centric Marketing

-Selling what we have

-Selling what the client needs

- OSCAL is great for CSPs
- Many OSCAL centric tools vendors

- Agencies have not adopted OSCAL
- 3PAOs are not using OSCAL

Define what the value proposition upstream is
Why should Agencies adopt OSCAL?

Procurement Problem

- Hard to evaluate the compliance level of a product and how well they perform
- FedRAMP High/Moderate/Low
- Readiness and maturity of the vendor

Many times the true nature of the vendor is not revealed until one start working with them

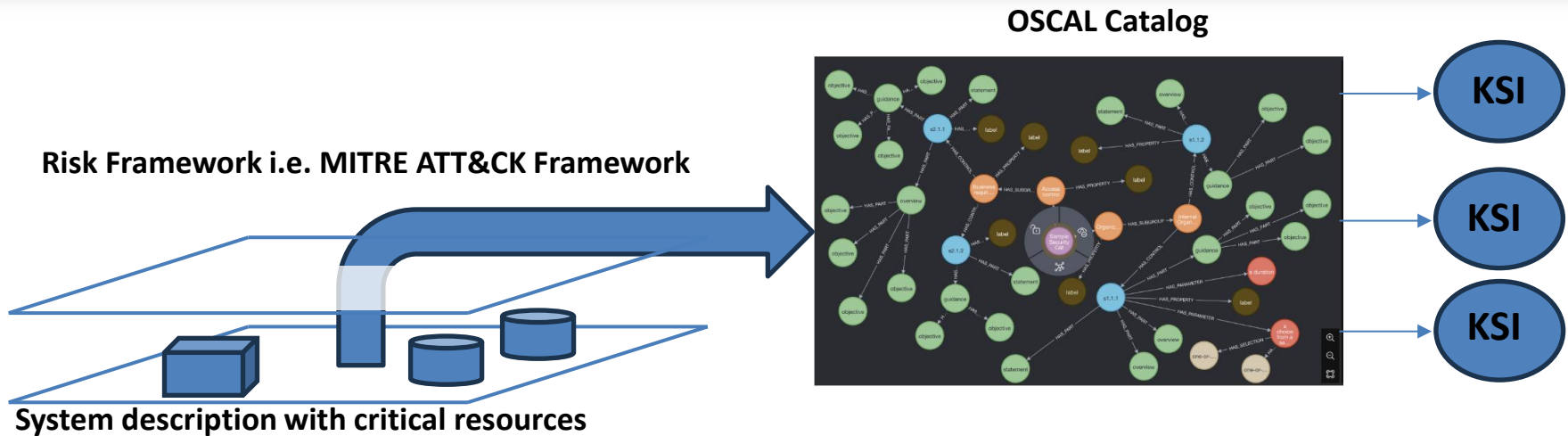
Procurement Approach

- Risk based security posture definition
- Efficiency of supplier's solution
- Security posture defined and known prior to decision
- Risk tiering of vendors
- Bridging gap between sourcing and onboarding
- Traceability of risk and control gaps

Agency OSCAL Purchasing Process

- Agency to define Security posture
- Agency to express RFP in OSCAL and KSIs
- CSP to provide KSI values as a measure of how efficient the system is
- CSP to respond with OSCAL catalog populated, test results, and corresponding evidence
- Agency to test and model defined risks.
- Agency to make an educated decision

Agency RFP Generation

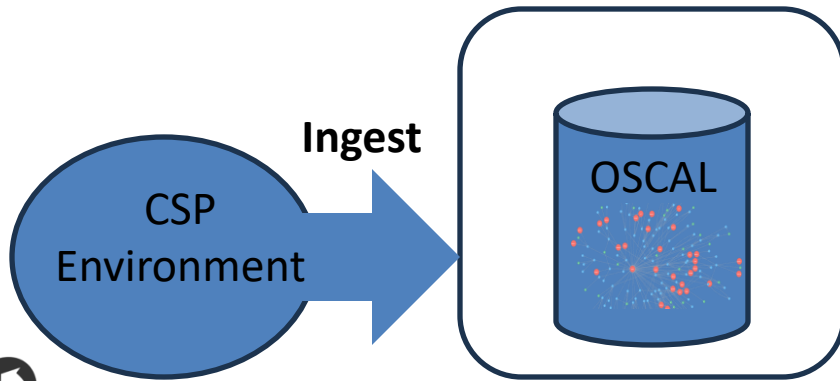


- KSIs used to performance benchmark vendors
- OSCAL Catalog used to:
 - Define security posture
 - Understand implementation
 - Readiness and completeness of system

CSP Response

- Automated testing
- Traceability
- Map risks to sourcing decision
- On boarding prior to purchase

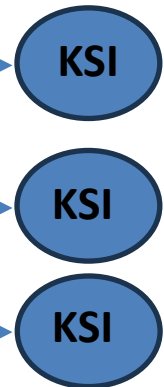
Artemis
Digital Twin



CSP RFP Response Test Control Workbook, SAP & SAR

Test	Result	Evidence	

OSCAL Catalog



Agency use of Digital Twin

With the Agency using the Digital Twin

- Attack scenarios can be simulated
- Vendors security efficiency can be measured and validated against identified and defined risks.

Test drive the system before you buy!

OSCAL Enabled Purchasing

- **Streamline Vendor Selection and Approval**

Automate due diligence tasks and reduce time-to-contract without sacrificing governance.

- **Align Procurement with Compliance and Security**

Make risk and regulatory context visible during sourcing—not after contracts are signed.

- **Reduce Third-Party Risk Exposure**

Catch high-risk or non-compliant vendors before onboarding and integrate controls into contracts.

- **Ensure Audit-Ready Procurement Workflows**

Document decisions, approvals, and controls across each step in the S2P lifecycle.