

KSI Example

WORK IN PROGRESS

The OSCAL Foundation's FedRAMP TFG elected to focus on [\[KSI-IAM-AAM\] Identity and Access Management: Automated Account Management](#).

This is an example of how KSIs *could* be implemented in OSCAL. It does not necessary reflect exactly what should be collected or how.

KSI-IAM-AAM

The lifecycle and privileges of all accounts, roles, and groups are securely managed using automation.

The

- lifecycle and
 - privileges of
- all accounts, roles, and groups
- are securely managed
- using automation.

Related SP 800-53 Controls: AC-02 (02), AC-02 (03), AC-02 (13), AC-06 (07), IA-04 (04), IA-12, IA-12 (02), IA-12 (03), IA-12 (05)

Subjects

- Identity and Access Management (IAM) Process:
 - Document
 - **Automated Workflow**

Evidence

- For EVERY [account (human and machine) | role | group] , process artifacts (logs?) exist for that account's:
 - creation
 - privlige modification (requires some kind of manager approval)

- disablement; and
- deletion.
- **Creation** is triggered by an appropriate event:
- **privilege escalation** is triggered by an appropriate event
- **privilege reduction** is triggered by an appropriate event
- **disablement** is triggered by an appropriate event (offboarding, lack of use)
- **deletion** is triggered by an appropriate event

Appropriate Triggers Might Include

- external process (onboarding, offboarding, contractor onboarding)
- approval by authorized individual or role
- signing of some license agreement, RoB, etc.

Assumptions and Prerequisites

The automated workflow:

- produces logs for the following events:
 - account requests
 - approvals
 - privilege modification (escalation and reduction)
 - disablement
- The logs are sent to a centralized logging capability
- The log transmission and storage has a high degree of integrity and non-repudiation
- Any identities pre-dating the workflow and logs are validated as accurate.

Correlation

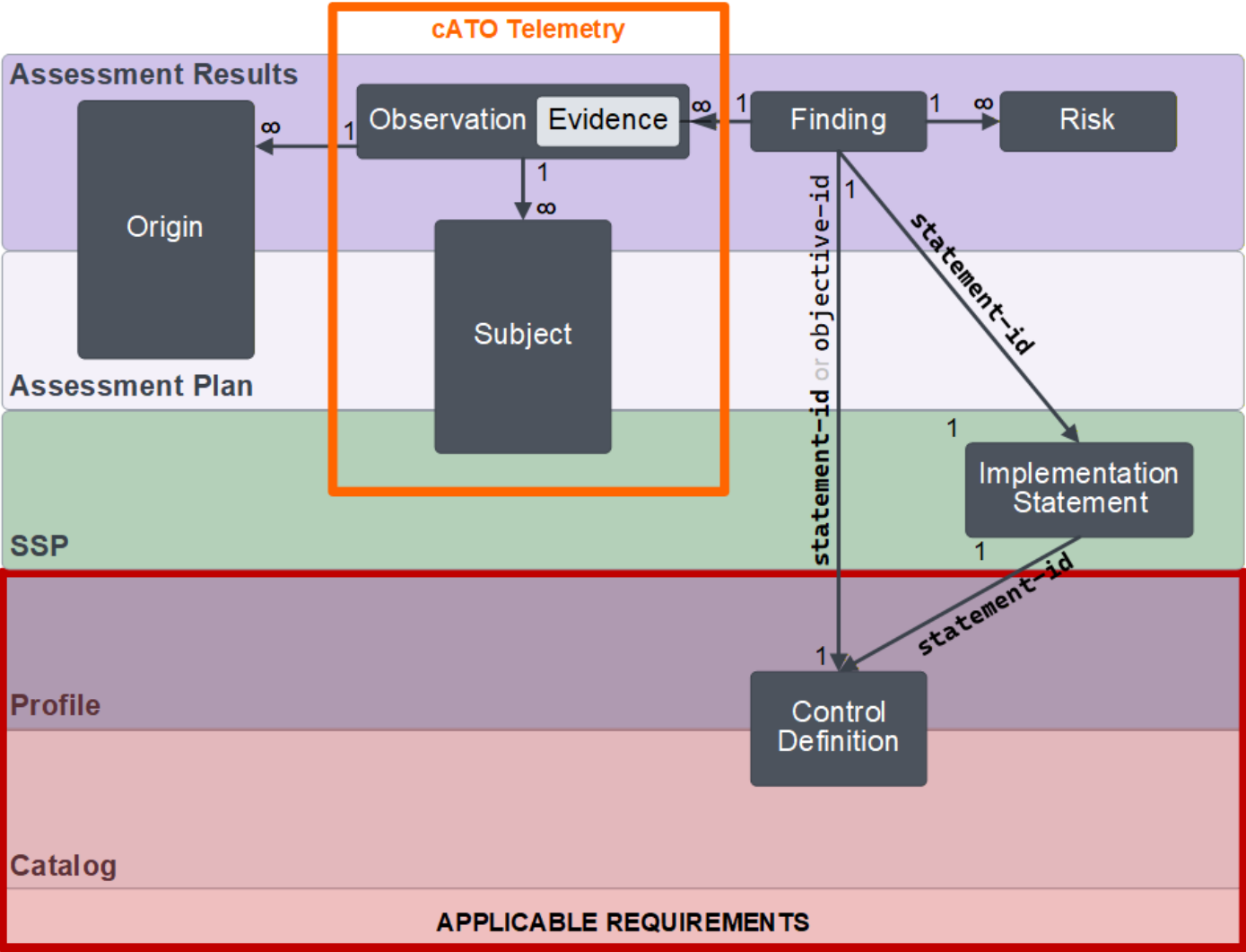
- ICAM system access (accounts, groups and privileges)
- Centralized Logging access

Questions to Answer

- What does telemetry look like, vs point-in-time?

OSCAL High-Level Concept

ORIGIN Who or what collected the evidence?	SUBJECT What was tested/inspected or who was interviewed?	OBSERVATION Result of an inspection, test or interview	FINDING Pass/Fail judgement for a control based on evidence	RISK Describes the risk(s) resulting from a failed finding
--	---	--	---	--



NOTES

Revision #2
Created 2026-08-20 19:42:19 UTC by Brian Ruf
Updated 2026-08-31 19:11:43 UTC by Brian Ruf