

Key Security Indicators (KSIs)

- [Overview](#)
- [Taxonomy](#)
- [Guiding Principles](#)
- [KSI Example](#)
- [Notes and Agreements](#)

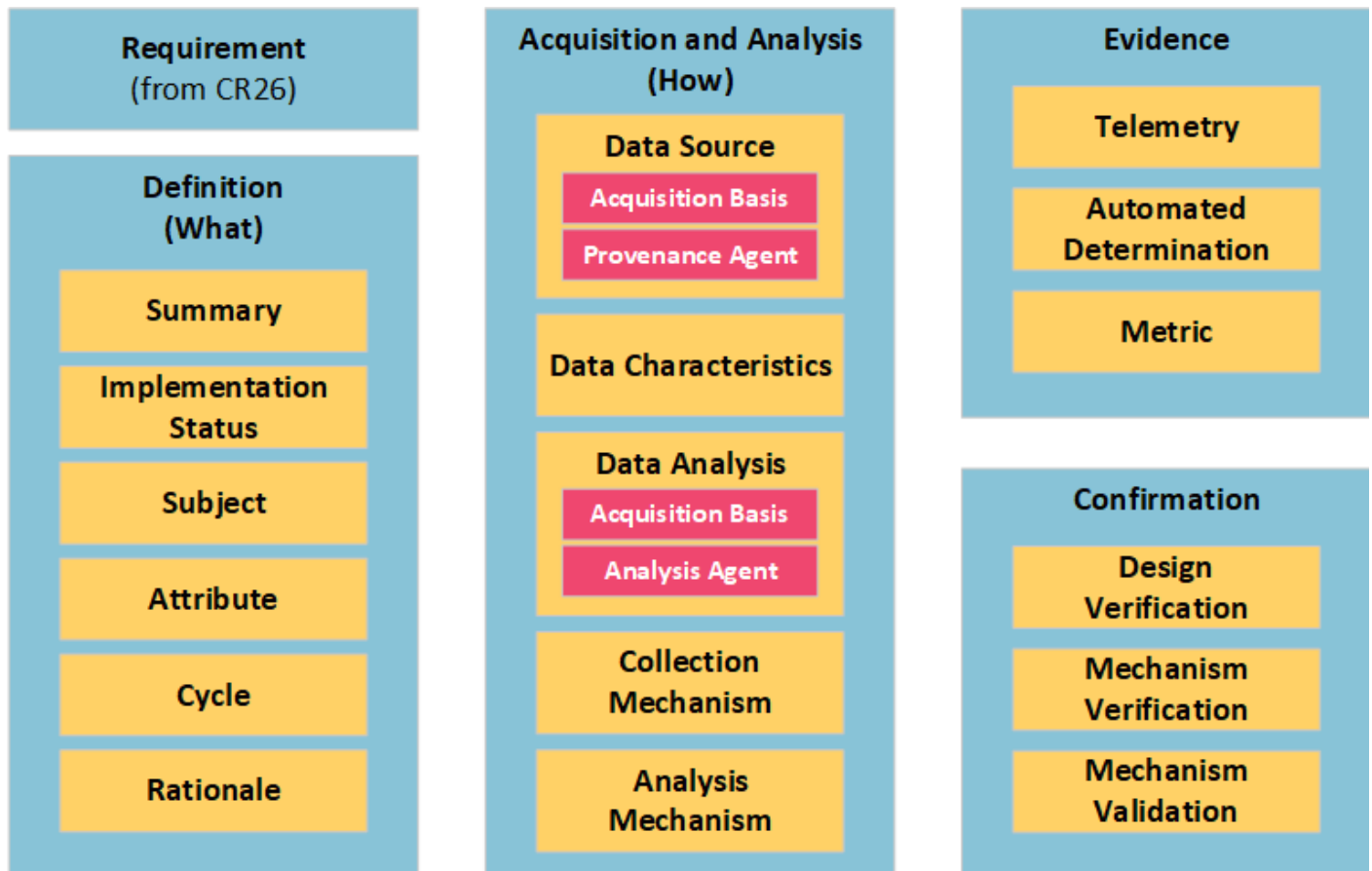
Overview

Links to the OSCAL Foundation's FedRAMP Technology Focus Group (TFG) FedRAMP KSI efforts:

- [Taxonomy](#)
- [Guiding Principles](#)
- [KSI Example](#)
- [Notes and Agreements](#)

Taxonomy

DRAFT - Please review and provide feedback. Self-register via Login to leave comments.



We defined the following **DRAFT** KSI Taxonomy to align with CR26 terminology and Security Decision Record (SDR) schema fields. We expanded on this where necessary; expansions and departures from FedRAMP's literal language are noted at the bottom of this section.

Taxonomy elements are named in the singular; a KSI's Design may reference more than one instance of any element (e.g., multiple Data Sources reconciled by a single Data Analysis rubric).

The taxonomy of a KSI includes:

- **Requirement:** The required KSI as defined by the PMO in CR26. [^ksi]
- **Definition (What):** Explanation of measures and objectives demonstrating a KSI, provided by the CSP in the SDR. [^ksi-1] The definition includes:

- **Summary:** A brief description of the data collection.
- **Implementation Status:** Whether measures demonstrating the KSI exist. Where not fully implemented, this includes the reason and resulting risk to customers. [^{ksi-1}][^{ksi-3}][^{ksi-5}]
- **Subject:** The capability the KSI's claim is about.
- **Attribute:** The specific observable property of that Subject being examined.
- **Cycle:** The timing pattern governing when data is collected. Expressed either as a frequency, a trigger, or both. [^{ksi-2}][^{n-cycle}]
- **Rationale:** Why the measurement supports the KSI.
- **Acquisition and Analysis (How):**
 - **Data Source:** Where Evidence of an Attribute is found.
 - **Acquisition Basis:** Categorizes the nature of the Evidence as received, before Data Analysis is performed. See Guiding Principles: Measurement Basis.
 - **Provenance Agent:** Categorizes the actor that makes the data available ahead of its acquisition by the Collection Mechanism. See Guiding Principles: Agent Basis. [^{mgn}]
 - **Data Characteristics:** The format or other characteristics of the Evidence that impact Data Analysis.
 - **Data Analysis:** The correlation logic, thresholds, or other rubric applied to Telemetry to produce an Automated Determination. See Guiding Principles: Measurement Basis. [^{ksi-3}]
 - **Analysis Basis:** Categorizes the nature of the logic applied to produce the Automated Determination.
 - **Analysis Agent:** Categorizes the actor that performs the analysis. See Guiding Principles: Agent Basis. [^{mgn}]
 - **Collection Mechanism:** A description of the mechanism performing data acquisition, including the method used to acquire the evidence, such as an API call, a logging query, or a manual process performed by a human. [^{ksi-4}][^{n-mechanism}]
 - **Analysis Mechanism:** A description of the mechanism performing Data Analysis, whether automated, statistical, human, or Agentic AI. [^{ksi-4}][^{n-mechanism}]
- **Evidence:**
 - **Telemetry:** The actual data acquired by a Collection Mechanism from its Data Source, per the defined Cycle. Telemetry whose effective Measurement Basis Tier is Concrete corresponds to FedRAMP's defined term Deterministic Telemetry. [^{dtm}]
 - **Automated Determination:** The conclusion reached by applying Data Analysis to Telemetry. This is the KSI-aligned determination of the Subject's performance. [^{n-determination}]
 - **Metric:** A time-series summary of Telemetry and/or Automated Determinations for a KSI, retained and reported at the frequency required by the CSP's Certification Class. [^{kmt}]
- **Confirmation:** Confirmation, through objective evidence, that the Design and its Mechanisms can be trusted. [^{vrf}][^{vln}][^{n-confirmation}]
 - **Design Verification:** Confirms that the Attribute, as measured through Data Analysis, demonstrates the Subject's KSI claim. [^{ksi-3}]
 - **Mechanism Verification:** Confirms that the Collection Mechanism and/or Analysis Mechanism are built accurately and sufficiently, or that automation is not necessary

for the measure. [^ksi-4]

- **Mechanism Validation:** Confirms that the Collection Mechanism and/or Analysis Mechanism are operating and producing accurate results as intended. [^ksi-5]
-

Notes

[^ksi]: FedRAMP's defined term for the requirement itself is "Key Security Indicator," a type of FedRAMP Practice (FRD-FPR).

[^ksi-1]: SDR-CSX-KSI, item 1: "Explanation of measures (and their objectives) that demonstrate the Key Security Indicator, or an explanation of the reason and resulting risk to customers for not having measures available for that Key Security Indicator."

[^ksi-2]: SDR-CSX-KSI, item 2: "Explanation of the cycle for any measures that are implemented persistently (if applicable)."

[^n-cycle]: **Expansion.** FedRAMP's rule text describes Cycle only in terms of a recurring frequency ("implemented persistently"); it does not distinguish frequency-based from trigger-based collection. We extend Cycle to cover both, since a triggering condition is, in our view, still an answer to "when is data collected," and FRD-PER (Persistently) already allows persistent activity to "occur irregularly" with "waiting periods between cycles" — a reading consistent with trigger-based collection, though not stated as such.

[^ksi-3]: SDR-CSX-KSI, item 3: "Verification that the measures demonstrate the Key Security Indicator, or that the reason for not having them is accepted."

[^ksi-4]: SDR-CSX-KSI, item 4: "Verification that the automation in place is accurate and sufficient to demonstrate appropriate measures for the Key Security Indicator, or that automation is not necessary for each measure."

[^n-mechanism]: **Departure.** SDR-CSX-KSI item 4 refers to "the automation in place," implying an automated mechanism. We do not require Collection Mechanism or Analysis Mechanism to be automated, since item 4 itself allows "automation is not necessary" as a valid answer — a mechanism can be a manual, human-performed process.

[^ksi-5]: SDR-CSX-KSI, item 5: "Validation that the measures are accurately produced and are in place and working as intended, or that the reason for not having them is valid."

[^n-determination]: **Departure.** FedRAMP's own term "Finding" (used in FRD-SDR and IVV-IAS-SUM) refers to the independent assessor's output, not the CSP's own automated conclusion. We use "Automated Determination" to avoid conflating the two. The assessor's own Finding, per IVV-IAS-SUM, is out of scope for this taxonomy, which models only the CSP's measurement chain under SDR-CSX-KSI.

[^kmt]: SDR-CSX-KMT requires historical metric data, scaled by Certification Class: a 30-day and up-to-one-year summary of each metric at Class B; the same plus all daily metric data up to one year at Class C; requirements exceeding Class B/C at Class D (specifics pending the 20x Phase 4 Pilot).

[^dtm]: FRD-DTM (Deterministic Telemetry): "Verifiable data collected directly from an authoritative source that represents a factual and reproducible observation of the attributes of a system." Its note states that probabilistic inferences, generative outputs, or predictive assessments "must not be used to generate deterministic telemetry" — consistent with this taxonomy's treatment of Agentic AI involvement as Inferential-tier under Measurement Basis.

[^vrf]: FRD-VRF (Verification): "Confirmation through objective evidence that specified FedRAMP Practices have been fulfilled for a cloud service offering."

[^vln]: FRD-VLN (Validation): "Confirmation through objective evidence that implemented security capabilities and related certification data are suitable for their intended FedRAMP Certification use and support the expected security outcomes for a cloud service offering."

[^n-confirmation]: **Departure.** We group Verification and Validation under "Confirmation" rather than FedRAMP's own term "assurance," since FedRAMP uses "assurance" for Certification Class and Type (FRD-CCL, FRD-CTY), a different concept. "Confirmation" is drawn from the shared opening language of FRD-VRF and FRD-VLN themselves. All three Confirmation elements are performed by the CSP, not an independent assessor — none of SDR-CSX-KSI's five items use the word "independent," unlike the base FRR layer (SDR-CSO-FRR) and Rev5 controls (SDR-CSF-CTF), which both explicitly require independent verification and validation as separate items.

[^mgn]: FRD-MGN (Machine-Generated): "Automatically produced by a computer process, application, or other mechanism without the intervention or manipulation of a human during production." This anchors the Automation category in Agent Basis; by exclusion, human involvement is the case FRD-MGN does not cover.

Guiding Principles

DRAFT - Please review and provide feedback. Self-register via Login to leave comments.

We defined the following **DRAFT** guiding principles in alignment with the [Taxonomy](#).

- **Data Analysis:** The Data Analysis *must* clearly define the intended result of data collection, either:
 - a *pass/fail* determination; or
 - a consistently quantifiable *degree of health*.
- **Measurement Basis:** Data Source and Data Analysis *must* distinguish Base, Derived, Interpretive and Probabilistic Measures, including those measures produced by Agentic AI.
- **Agent Basis:** Data Source and Data Analysis must identify the involvement of Automation, Statistical Model, Human, and/or Agentic AI; Telemetry and Findings inherit this classification from the Provenance Agent and Analysis Agent that produced them

Data Analysis

“ The Data Analysis *must* clearly define the intended result of data collection, either:

- a *Pass/Fail* determination; or
- a consistently quantifiable *Degree of Health*.

All KSI telemetry is gathered in support of a clear and specific result.

Pass/Fail

Most compliance frameworks seek to define clear pass/fail criteria against specific controls or requirements.

While Pass/Fail is still a preferred target for FedRAMP KSIs, it is not mandatory.

Degree of Health

FedRAMP KSIs open the door to other quantifiable metrics that can be analyzed to *indicate* a system's overall cybersecurity "health". Telemetry reflecting Degree of Health *should* include an unambiguous analysis mechanism whenever practical, such as thresholds.

In some instances, measurements *may* require organization-specific or system-specific "baselining" before thresholds can be defined. This *should* be conducted within a defined period of time and adjusted periodically as necessary.

Measurement Basis

“Data Source and Data Analysis *must* distinguish Base, Derived, Interpretive and Probabilistic Measures, including those measures produced by Agentic AI.

Categories

The Measurement Basis Categories are:

- **Concrete Measures:** Are quantitative without subjectivity.
 - **Base Measure:** A measure obtained by direct observation of a single attribute, requiring no computation or inference from other measures. (ISO 15939 term)
 - **Derived Measure:** A measure computed as a function of two or more Base and/or Derived Measures. (ISO 15939 term)
- **Inferential Measures:** May be quantitative or qualitative and have some element of subjectivity.
 - **Interpretive Measure:** A measure produced through human or Agentic AI judgment rather than deterministic computation or statistical inference — a qualitative assessment that cannot be fully reduced to a formula.
 - **Probabilistic Measure:** A measure produced by applying a statistical model, threshold, or algorithmic inference to underlying data, yielding a likelihood, score, or classification rather than a directly observed value.

Application

Measurement Basis applies to both Acquisition Basis and Analysis Basis.

- **Acquisition Basis:** The Measurement Basis classification of the data as received from the Data Source, before the KSI's own Data Analysis is applied.

- **Analysis Basis:** The Measurement Basis classification of the logic the KSI itself applies to produce the Finding.

A Finding's Acquisition Basis and Analysis Basis may differ from one another. For example, A Finding built on a Concrete Measure is still, in effect, an Inferential Finding if the underlying Data Source itself returned a Probabilistic value.

Both Acquisition Basis and Analysis Basis *must* be provided such that an Agency can filter based on their risk tolerance for Evidence based on Inferential Measures.

Agent Basis

“Data Source and Data Analysis must identify the involvement of Automation, Statistical Model, Human, and/or Agentic AI; Telemetry and Findings inherit this classification from the Provenance Agent and Analysis Agent that produced them

Categories

The Agent Basis Categories are:

- **Automation:** Deterministic, rule-based, automated mechanism.
- **Statistical Model:** Machine Learning, probabilistic, non-agentic mechanism.
- **Human:** Manual assembly, subjective analysis, judgement calls or similar activities performed by humans.
- **Agentic AI:** An autonomous or semi-autonomous AI system capable of independent action, tool use, or decision-making without direct human execution of each step

Application

Agent Basis applies to both Provenance Agent and Analysis Agent.

- **Provenance Agent:** Categorizes the actor that makes the data available ahead of its acquisition by the Collection Mechanism.
- **Analysis Agent:** Categorizes the mechanism that performs the analysis. See [Agent Basis](#) below for details.

Agencies need a way to filter Evidence based on strictly deterministic automation or less deterministic influences from humans, machine-learning and Agentic AI mechanisms.

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
 - privilege 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

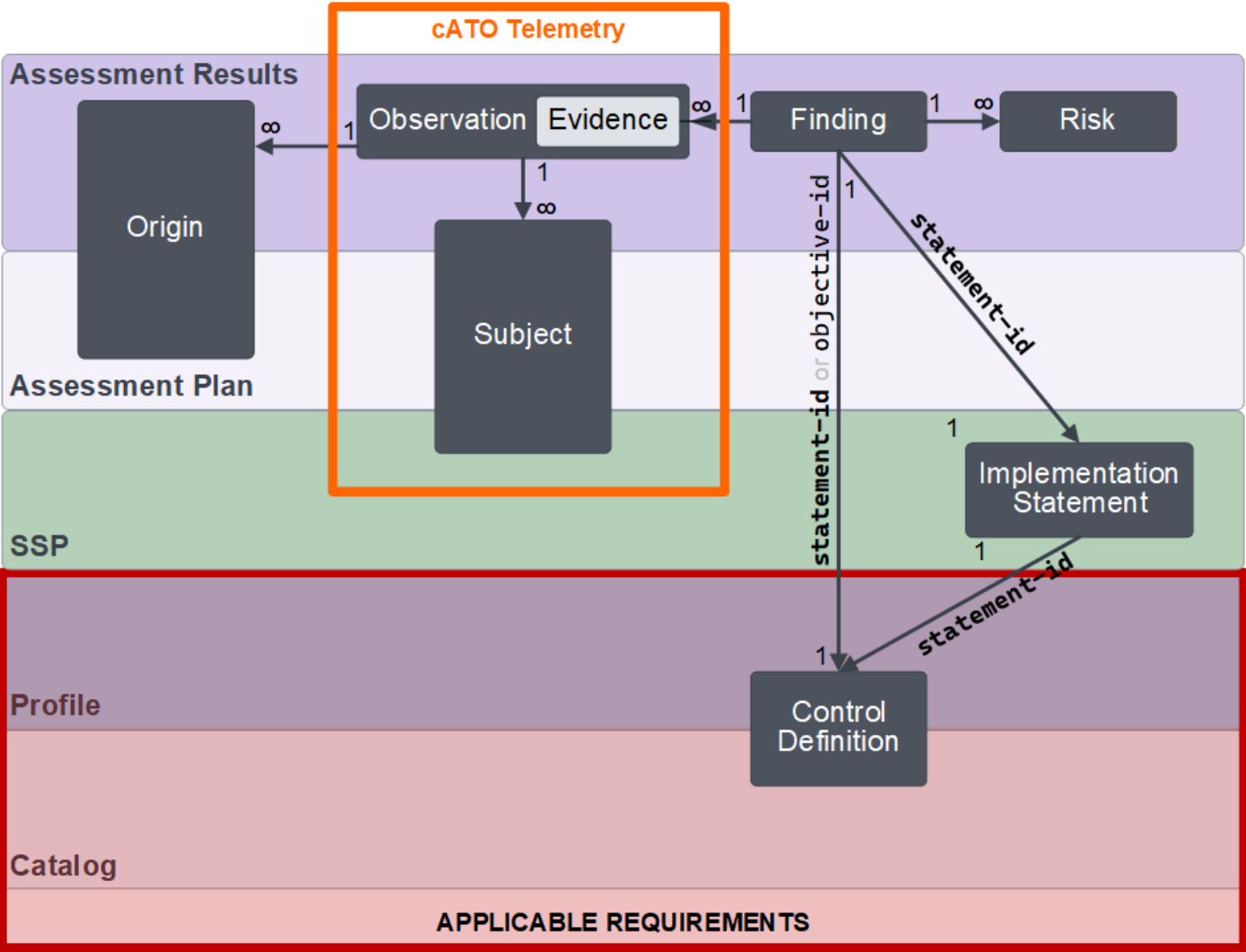
- ICAM system access (accounts, groups and privileges)
- Centralized Logging access

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

Notes and Agreements

As the OSCAL Foundation's FedRAMP Technology Focus Group (TFG) reaches agreements as to the path forward, they are captured here. This is a work in progress. Once the group reaches an appropriate milestone, this will be consolidated and re-organized into more consumable guidance.

DRAFT - Please review and provide feedback. Self-register via Login to leave comments.

See [Taxonomy](#)

See [Guiding Principles](#)

KSI Approach

- **KSI Statement Analysis**

- Identify KSI goal(s)

- **KSI Data Requirements:**

- **Intent:** *A simple, unambiguous status.* Typically Pass/Fail
- **Decision Point:** Sampling or full coverage?
- Identify evidence to collect in support of KSI goal(s)
- Define evidence interpretation
 - Evidence type (count, true/false, setting)
 - Collection frequency
 - Evidence fidelity
 - Correlation
 - Thresholds
 - Could be more granular than just pass/fail
 - Example: Satisfactory, Degraded, Critical

- **Organizational Considerations:**

- **Action Triggers:** Define the triggers for that system/org
 - Define required action(s) when triggered

- **KSI Technical Collection Approach**

- Identify all evidence source/component
 - Identify the source format(s)
- Define centralized evidence collection target
- Define the automation required to acquire evidence from each source/component and deliver to centralized collection target

- **Decision Point:** Evidence delivered *raw* or *normalized*?

- **KSI Technical Interpretation Approach**

- Apply data requirements/thresholds to produce *Findings*
 - Findings are continuously updating as new data is received and analyzed
- Raise action triggers when appropriate