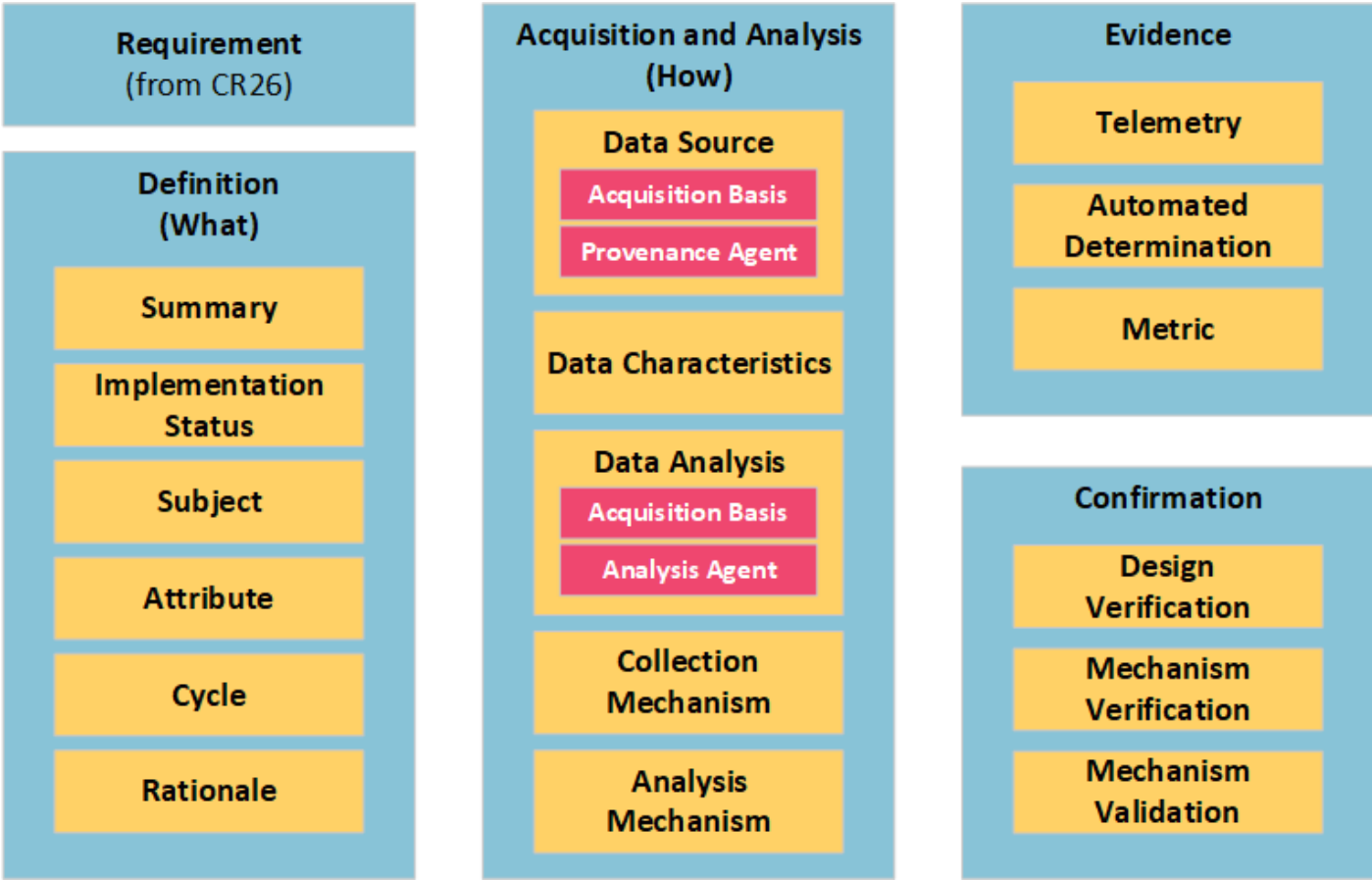


Taxonomy

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.

Revision #10

Created 2026-09-21 12:23:10 UTC by Brian Ruf

Updated 2026-09-29 14:13:40 UTC by Brian Ruf