Traceability and Evidence

Return to Terms and Definitions

Discussion

Traceability and Evidence support review, reconstruction, accountability, conformance assessment, and defensibility. Traceability connects elements across conceptual, logical, implementation, deployment, and evidence layers. Evidence records information supporting claims about behaviour, configuration, interpretation, execution, governance, or review.

Traceability and Evidence remain distinct but closely related. Traceability identifies relationships. Evidence supports claims. A traceability relationship may connect an evidence item to the claim, artefact, Node, Communication Endpoint, Data Structure Definition, Runtime Plane, or execution condition that it supports.

Definition

relationships and recorded information supporting review, reconstruction, accountability, and defensibility

Source

Informed by SIP-RA traceability, audit, review, and reproducible processing concerns; aligned with FDIS-RA provenance, auditability, defensibility, comparability, and evidence concerns; adapted from FX Demo Reference Architecture material on persistence, provenance, audit, replay, release audit, and acceptance evidence.

Note

Logs may contribute to evidence, but evidence includes more than logs. Evidence may include captured messages, deployment records, configuration records, test outputs, provenance records, release decisions, review findings, and scenario results.

Example

A test result may provide evidence that a deployed Node published a Data Structure Instance through a Communication Endpoint. At the same time, traceability links that evidence to the relevant concept, logical element, implementation artefact, and deployment artefact.