Identity Continuity Under Interruption — Compliance Checklist

For architecture, design review, and procurement reference use

This checklist is derived from the SISMIQ Continuity Requirements. It is intended to support architectural assessment of whether a system preserves identity continuity under interruption.

Each item should be answerable **Yes / No / Unknown** based on current system design and documentation.

Section A — Interruption Assumptions

1. Does the system explicitly account for telemetry, sensing, or observation being degraded, delayed, reordered, or unavailable during normal operation?
2. Are interruption conditions treated as a first-class operating mode rather than solely as error cases?
3. Is system correctness defined independently of continuous observation?

Evidence examples: architecture assumptions, operating environment definitions, failure mode analyses

Section B — Identity Authority

4. Is there a clearly defined identity authority for each tracked entity?
5. Is the identity authority association between identity and persistent internal state explicitly maintained during interruption?
6. Is identity authority preserved across interruption without requiring reinitialization?
7. Is loss of telemetry insufficient by itself to revoke identity authority?

Evidence examples: identity lifecycle documentation, authority handoff logic, state diagrams

Section C — Persistent Internal State

8. Does the system maintain a persistent internal state for each entity that remains addressable during interruption?

9. Is this internal state addressable independent of continuous external observation?
10. Can downstream components reference entity state during interruption without instantiating a new identity?

Evidence examples: state models, internal representations, interface contracts

Section D — Downstream Identity Control

11. Are downstream subsystems explicitly prevented from instantiating new identities during interruption?
12. Is identity creation gated on explicit authority revocation rather than inferred loss of observation?
13. Are duplicate identity instances detectable or prevented by design?

Evidence examples: subsystem constraints, creation guards, duplicate detection logic

Section E — Recovery and Re-Association

14. Upon telemetry restoration, does the system perform validated re-association before resuming identity authority?
15. Is restored telemetry evaluated against preserved internal state before overwriting, replacing, or superseding it?
16. Are incorrect or ambiguous re-associations explicitly handled?

Evidence examples: recovery flows, validation gates, reconciliation logic

Section F — Distributed and Heterogeneous Execution

17. Do identity continuity guarantees apply across distributed components and execution domains?
18. Can identity authority survive transitions between edge, cloud, or hybrid environments?
19. Are asynchronous execution and delayed consistency explicitly accounted for?

Evidence examples: distributed architecture diagrams, synchronization assumptions, handoff mechanisms

Section G — Reset and Reinitialization Discipline

20. Is identity reinitialization treated as an external failure handling action, not a continuity mechanism?
21. Are reset cascades explicitly identified and architecturally mitigated?
22. Is system correctness preserved when resets occur out of order or partially?

Evidence examples: failure recovery documentation, reset policies, safety analyses

Interpretation Guidance

- A “No” or “Unknown” does not indicate a defect; it indicates unexamined architectural risk.
- Systems operating under interruption may satisfy these requirements through deterministic, probabilistic, hybrid, or heuristic approaches.
- This checklist does not prescribe implementation methods.
- Interpretation may require architectural context; uncertainty indicates a need for further examination, not immediate remediation.

Related Reference Material

SISMIQ Continuity Requirements (SCR)
Canonical architectural requirements for identity continuity under interruption.

Identity Failure Chain Under Interruption
Explanatory overview of common identity failure modes in interruption-prone systems.

Architectural Note: Identity Continuity Under Interruption
Contextual discussion of architectural implications and design tradeoffs.

Procurement / RFP Language Pack
Specification-ready language for solicitations and contracts.

For architectural interpretation questions related to this checklist:

contact@sismiq.io