iSOAF Reliance Assessment Model v1.1

Document type: Architectural Doctrine Note
Status: Public-facing architectural clarification
Scope: Conceptual model for explaining how iSOAF separates evidence, conclusions, reliance, and human decisions.

1. Purpose

The Reliance Assessment Model surfaces the core abstraction behind iSOAF. It explains how the framework reasons from operational evidence to reliance without becoming an operational decision-maker.

This is not a replacement for the Continuous Operational Assurance Methodology. It is an architectural clarification that makes the framework boundary more explicit.

2. Core doctrinal statement

> iSOAF does not validate whether a decision is correct. It validates whether the available evidence provides a sufficient basis for relying upon a conclusion within a defined assessment scope, while preserving accountability with the designated human authority.

3. Five-layer assurance progression

[LAYER 1: EVIDENCE]
Operational signals and provenance records whose integrity, origin, completeness, and currency are evaluated.

↓

[LAYER 2: ASSESSMENT]
The continuous activity performed on evidence to determine strength, relevance, consistency, and alignment with defined policy or governance expectations.

↓

[LAYER 3: CONCLUSION]
Assertions derived from assessed evidence, such as whether a control, recovery capability, policy condition, or operational claim remains supportable.

↓

[LAYER 4: RELIANCE]
Validation that the assessed evidence provides a sufficient basis for relying upon the conclusion within the defined assessment scope.

↓

================ EPISTEMIC BOUNDARY ================
Evidence-based validation ends here. Evidence may support reliance within scope, but it does not determine

broader organizational, legal, ethical, strategic, or risk-appetite judgments.

========== OPERATIONAL BOUNDARY ==========
Framework authority ends here. iSOAF does not determine what decision should be made and does not extend into autonomous remediation, closure, policy enforcement, or risk acceptance.

↓

[LAYER 5: DECISION]
Choices, policy enforcement, operational closure, or risk acceptance made under accountable human authority and outside the framework decision boundary.

4. Boundary definitions

Epistemic boundary

The epistemic boundary is the point at which evidence-based validation ends and human judgment begins. Beyond this boundary, decisions may incorporate factors that cannot be established from operational evidence alone, including strategy, legal obligations, ethics, risk appetite, organizational priority, and contextual judgment.

Operational boundary

The operational boundary is the limit of what the framework is authorized to do. iSOAF evaluates evidence, conclusions, and reliance. It does not perform autonomous remediation, operational closure, policy enforcement, or risk acceptance.

5. Design objectives

Accountability Preservation

The framework is designed to preserve accountability with the designated human authority by limiting its scope to evidentiary reliance assessment rather than operational decision-making.

Boundary Integrity

The doctrine establishes architectural and epistemic boundaries intended to prevent expansion from evidentiary validation into autonomous operational decision-making.

Domain Adaptability

The underlying assurance principles remain consistent across domains, while evidence models, thresholds, and governance requirements may be adapted to the context.

6. Domain consistency criterion

A doctrinal abstraction is considered stable when its assurance principles remain internally consistent across multiple operational domains without modification to the framework boundary.

The evidence, assessment methods, thresholds, and governance requirements may differ by domain. The assurance progression remains the same:

Evidence → Assessment → Conclusion → Reliance → Human Decision

7. Cross-domain illustration

Domain	Evidence	Assessment	Conclusion	Reliance	Human Decision
Cybersecurity	Firewall logs, configuration states, packet traces	Analysis against baseline traffic rules and enforcement expectations	Unauthorized inbound traffic is being blocked according to the defined policy	The evidence is sufficient to rely on the control status within the assessment scope	Maintain policy, adjust risk treatment, or require corrective action
Backup and Recovery	Backup logs, restore-test records, recovery timing evidence	Freshness, completeness, recoverability, and RTO/RPO alignment are evaluated	Recovery capability remains supportable under current conditions	The conclusion can or cannot be relied upon for operational closure	Close incident, keep incident open, escalate, or accept residual risk
Executive Governance	Access logs, separation-of-duty records, policy mappings, approval records	Evidence lineage and policy alignment are evaluated against governance requirements	Privileged access is restricted according to policy	Evidence is sufficient or insufficient to support executive sign-off	Certify, defer, escalate, or issue a corrective action plan
Smart Traffic / STOPS	Sensor telemetry, camera feeds, loop counts, congestion history	Drift and reliability are assessed against traffic-flow models and operating conditions	Routing adjustments are producing the expected operational effect	Evidence sufficiency determines whether the model can be relied upon	Override timing, approve changes, or defer capital decisions
Evidentiary Assurance	Source records, timestamps, chain-of-custody metadata, validation logs	Provenance, integrity, completeness, and independence are evaluated	The evidentiary record remains traceable and supportable	Reliance may be supported or withheld within the defined evidentiary scope	Legal, administrative, or governance authority determines the action

8. Implementation note

This model should be surfaced consistently across public documentation, runtime interpretation, training material, and future domain papers. It does not disclose scoring logic, proprietary implementation architecture, or internal orchestration mechanics. It defines the conceptual boundary of assurance.

Related Publications

- **iSOAF Executive White Paper v1.2** - establishes the governance assurance problem, public doctrine, strategic positioning, and documented historical validation outcomes.
- **Continuous Operational Assurance Methodology v2.1** - provides the generalized methodology for applying continuous operational assurance.
- **Evidence Provenance Reference v1.0** - defines the evidentiary properties that support assurance

and justified reliance.
- **Public Architecture Index** - defines the role and relationship of the synchronized publication suite.

Version 1.1 Synchronization Note

Terminology and cross-references were synchronized with the Executive White Paper v1.2 and Methodology v2.1. The model remains evidence-bounded and human-governed: it evaluates whether available evidence supports reliance within a defined assessment scope; it does not make operational decisions, accept risk, authorize closure, or perform remediation.