COMPLIANCE RISK

The Latent Capability Problem

Regulatory Scope

Modern AI regulation targets system **capability**, not just deployed configuration. The EU AI Act Article 6 evaluates what a system can do, not merely what it currently does

Audit Limitations

Traditional compliance relies on documentation, configuration scans, and self-attestation. These methods cannot detect dormant capabilities embedded in hardware or system architecture

Hidden Risk

Regulated systems may contain unused or inactive capabilities that remain present and potentially activatable. Static audits fail to surface these latent risks reliably

Compliance Implication

Regulatory liability exists **prior to deployment**, independent of current configuration or intent. Capability presence may create compliance exposure under certain regulatory classifications

THE PROBLEM

Why traditional documentation fails modern AI compliance

Static artifacts

PDFs and spreadsheets cannot capture inherited capabilities or conditional system relationships

No traceability

Text-based reviews cannot reliably map system components to regulatory definitions

Self-attestation

Current approaches rely on manual interpretation without systematic verification methods

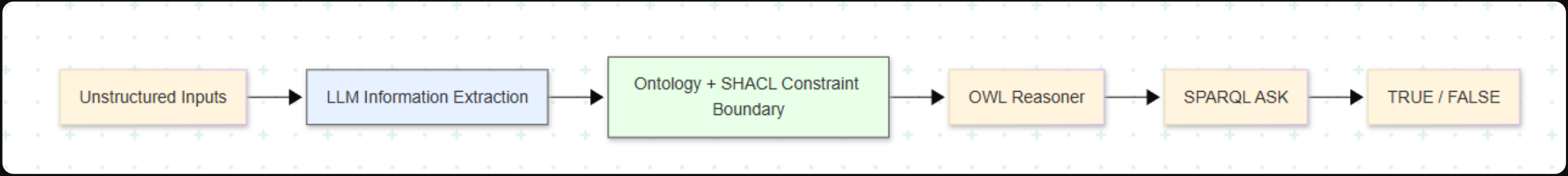
Documentation ≠ capability

Describing what is configured cannot support defensible claims about what the system can do

Latent risk

Compliance becomes documentation-heavy rather than verification-driven, hiding actual capabilities

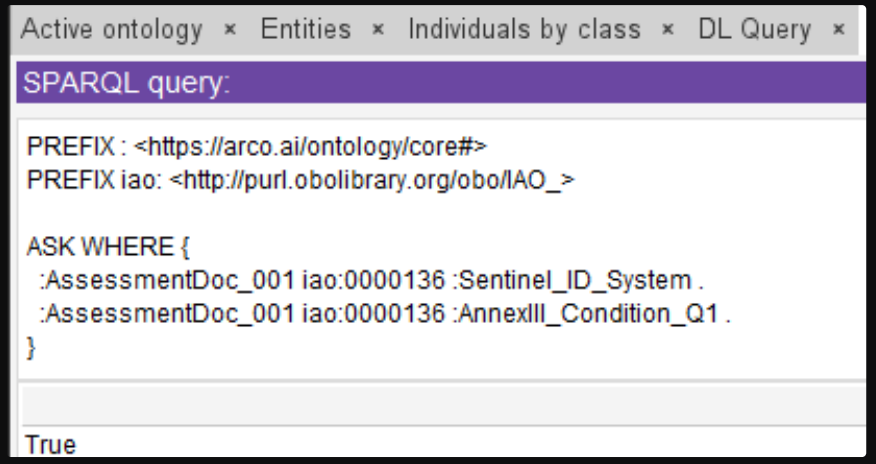
ARCO: Neuro-Symbolic Reasoning Approach



Architecture: ARCO separates information extraction from compliance reasoning. Language models parse unstructured sources (manuals, specifications, policy text). All compliance evaluation occurs within a formal ontology aligned with regulatory definitions. Reasoning is deterministic and logic-based, not probabilistic—ensuring inspectable, auditable outcomes. The ontology encodes regulatory concepts, system components, and capability relationships, determining whether regulated capabilities are present independent of current configuration.

Deterministic Outputs and Audit Traceability

Example: SPARQL ASK query evaluating Annex III high-risk condition against the Sentinel-ID system model.



Binary, Not Probabilistic

Compliance questions are evaluated using deterministic queries that produce TRUE or FALSE outputs—eliminating probabilistic uncertainty from final compliance determinations.

Traceable Reasoning Paths

Each result includes an inspectable reasoning path that links system components directly to specific regulatory clauses, supporting audit review and regulatory submission.

Independently Reproducible

Results can be independently verified by third-party reviewers, procurement evaluators, and auditors—ensuring transparency and defensibility throughout the compliance process.

Value and Scope Limitations

What This Does

Reduces audit ambiguity and improves traceability of compliance claims

Enables pre-deployment compliance assessment with inspectable evidence

Provides reproducible, verifiable compliance evidence.

Shifts compliance from static documentation to active verification

VS

What This Does Not Do

Does not automate legal judgment or regulatory decision-making

Does not replace auditors, regulators, or procurement review teams

Does not function as a generative AI product or system

Does not eliminate the need for human oversight and expertise

This proof-of-concept capability supports—but does not replace—procurement, audit, and regulatory review processes.