TIO End-State Architecture

Architecture Overview and Viewpoints Pack

For Enterprise Architects, CIOs, Security and Data Architects, Transformation Leaders, and Solution Teams

Document Version 1.1 FINAL | TIO-KR-2026.08.0 | August 2026

Contents

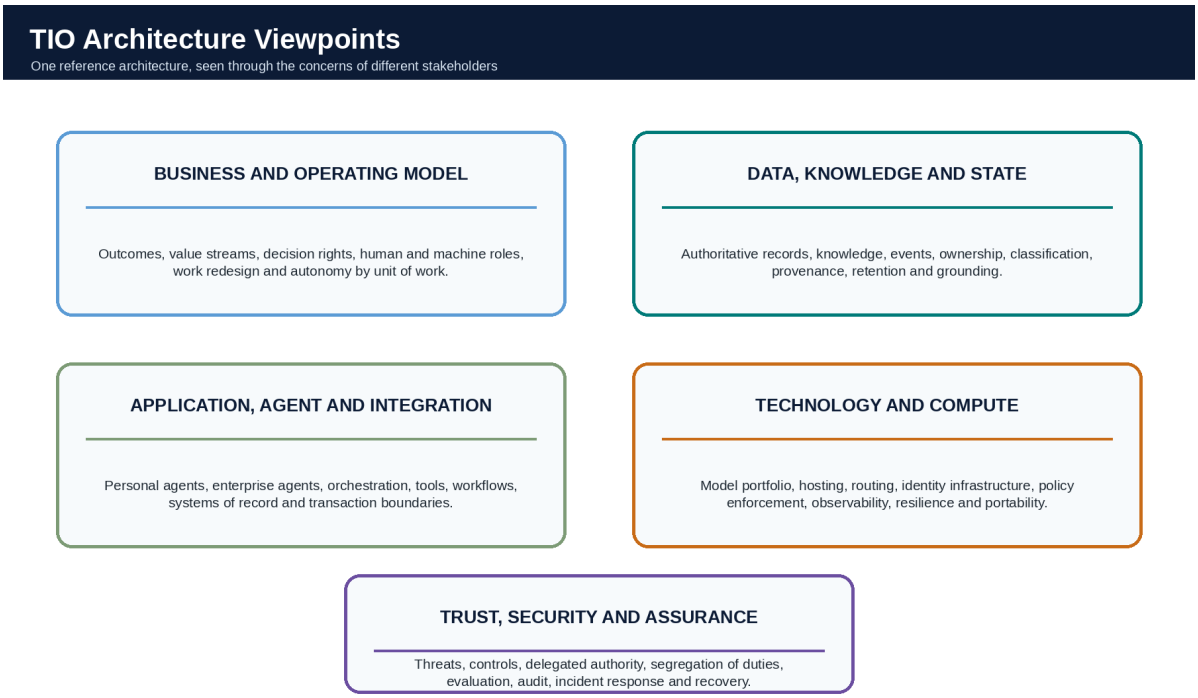
How to use this document

Use this pack with TIO-ESA-0101. The Blueprint explains the architecture to leaders. This document decomposes it into the concerns, building blocks, interfaces, requirements, and transition states used in architecture work.

01 Purpose and Stakeholder Concerns

One architecture, several legitimate views

The viewpoints decompose Alpha, the complete Sovereign Enterprise Intelligence System. Across every view, Alpha retains two co-equal foundations: the Intelligence Core and Enterprise Knowledge and State. The views do not create separate architectures; they expose different stakeholder concerns, building blocks, interfaces, and evidence needs.



Stakeholder	Primary concerns
CEO / Board	Enterprise direction, control, value, trust, accountability, resilience, and strategic dependency.
Business leader	Workflow ownership, customer or public outcome, Delegated Autonomy, exceptions, adoption, and value.
Enterprise architect	Boundaries, building blocks, interfaces, standards, decisions, transition states, and roadmap.
Data leader	Ownership, meaning, quality, access, provenance, authoritative state, flow, and retention.
CIO / Technology leader	Platforms, integration, identity, hosting, model portfolio, operations, portability, and cost.
Security / Risk / Privacy / Legal	Threats, delegation, data use, control evidence, incidents, rights, and residual risk.
People leader / Employee representative	Role change, skills, monitoring, fairness, accessibility, appeals, and trust.
Factory / Delivery team	Use-case design, contracts, evaluations, release, measurement, Evidence Gates, and scaling.

2026.08 ALIGNMENT | Additional shared views

- Add the Work and Decision Map as the common business input to the Business, Data, Application and Agent, Technology,

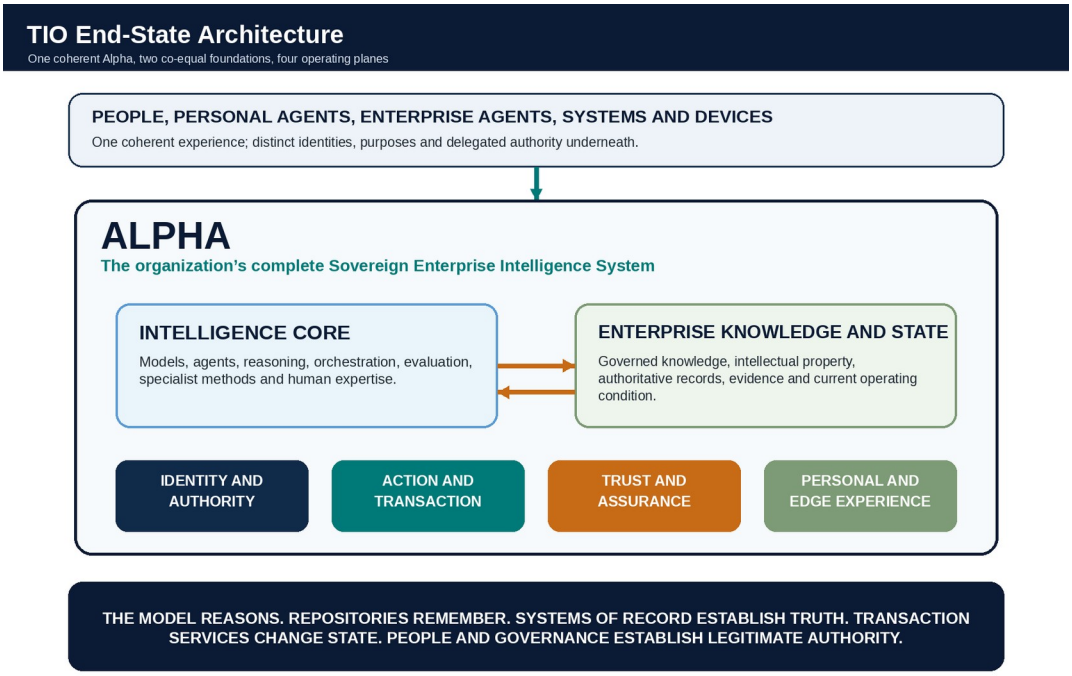
Stakeholder	Primary concerns

and Trust views.

- Use the Assurance and Operations lifecycle to connect architecture design to live ownership, monitoring, change, recovery, and retirement.
- Use Transition Architecture to describe temporary operating states, movement of work and authority, and explicit legacy outcomes.

02 Architecture Vision and Principles

The same core viewed through different concerns



Grounding principle
The model reasons. Repositories remember. Systems of record establish truth. Transaction services change state. People and governance establish legitimate authority.

Architecture principle	Implication
Alpha is the integrated capability	Do not design one model as the enterprise operating system.
Two co-equal foundations	Keep intelligence replaceable and enterprise truth governed.
Explicit operating planes	Identity, action, assurance, and edge experience remain visible in architecture decisions.
Enterprise Autonomy is the control outcome	Select sourcing and deployment according to required control outcomes.
Authority is bounded	Delegation attaches to work, purpose, time, data, tools, actions, and evidence.
Deterministic commit	Authoritative services validate and write material state.
Evidence drives Delegated Autonomy and transition	Delegated Autonomy changes through measured gates; each horizon creates reusable controls and capability.

03 Business and Operating Model View

Outcomes, value streams, roles, and authority

Element	Target-state representation
Enterprise objectives	Growth, impact, service, productivity, resilience, trust, workforce, and regulatory outcomes.
Value streams	Customer, citizen, employee, supplier, operations, risk, finance, and management work supported by Alpha.
Capabilities	TIO Leadership, Data, Technology, Factory, and People capabilities required for the selected workflow and scale.
Business services	Search, advice, case support, planning, coordination, transaction preparation, controlled execution, monitoring, and learning.
Roles	Process owner, accountable executive, user, approver, data owner, agent owner, service owner, assurance reviewer, support and recovery.
Decision rights	Mandate, funding, data use, Delegated Autonomy, approval, commit, exception, incident, recovery, residual risk, and retirement.
Controls	Autonomy Envelope, Evidence Gates, policy, segregation, thresholds, monitoring, stop and appeal.
Measures	Baseline, value, quality, exceptions, adoption, customer or public outcome, risk, incident, cost, and recovery.

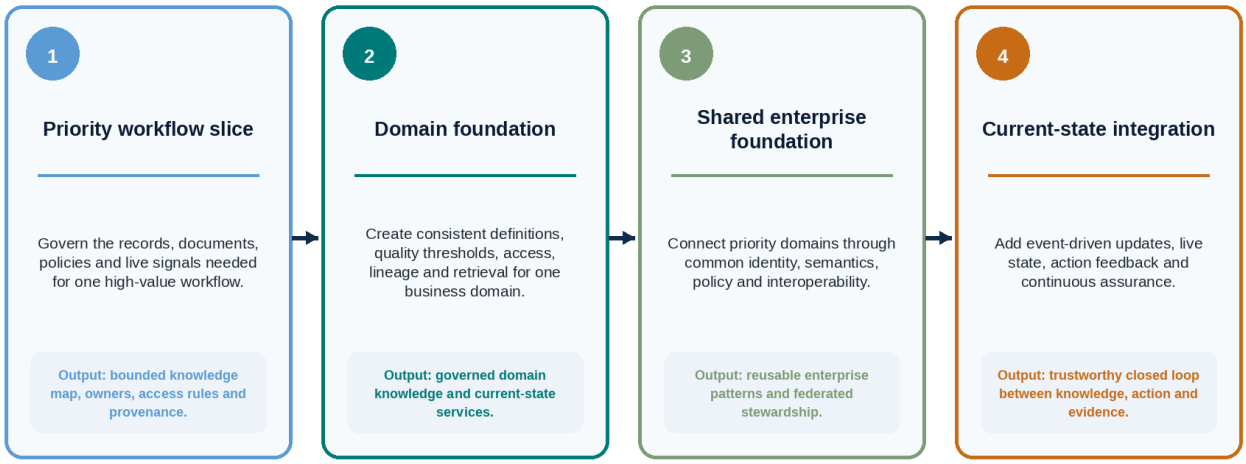
Example workflow: supplier invoice	Role and Delegated Autonomy
Receive invoice	Observe and classify automatically.
Match supplier, order, receipt, and tax	Prepare recommendation using authoritative records.
Resolve small known variance	Bounded autonomy within approved amount and case rules.
Approve payment	Named person or approved rules according to segregation and amount.
Release payment	Authoritative financial service commits; AI cannot bypass controls.
Monitor result	Assurance records exceptions, duplicates, supplier disputes, savings, and recoveries.

04 Data, Knowledge, and State View

Authoritative truth, governed context, provenance, and current state

Enterprise Knowledge and State: Partial-Credit Path

Start with the information needed for priority work; do not wait for perfect enterprise-wide unification



The hardest work is usually ownership, meaning, quality, access, provenance and current-state integrity—not the model connection itself.

Logical building block	Responsibilities
Source systems and repositories	Create and retain authoritative records, documents, messages, events, and sensor data.
Ownership and stewardship	Assign business meaning, quality, access, retention, correction, and acceptable-use decisions.
Classification and policy metadata	Sensitivity, purpose, jurisdiction, AI-use lane, retention, legal hold, and disclosure conditions.
Semantic layer	Definitions, taxonomies, entity relationships, rules, service commitments, and common language.
Knowledge and retrieval services	Index, search, graph, vector, structured query, relevance, provenance, freshness, and minimization.
Current-state and event services	Operational events, case status, capacity, approvals, inventory, incidents, and time semantics.
Lineage and provenance	Source, owner, version, transformation, retrieval, model/tool use, approval, transaction, and outcome.
Memory services	Personal, session, team, workflow, and enterprise memory with retention, correction, isolation, and deletion.

Logical building block	Responsibilities
Evidence repository	Evaluations, thresholds, Gate decisions, incidents, overrides, costs, and lessons.

Data contract question	Required answer
What information?	Sources, records, fields, classifications, exclusions, and derived data.
Whose authority?	Owner, requester, agent, purpose, legal basis or policy, and time.
How current?	As-of time, event time, update frequency, expiry, and stale-data behaviour.
How attributable?	Provenance, citations, transformation, confidence, and owner.
What may be inferred?	Approved combinations and prohibited sensitive or rights-affecting inference.
What may be remembered?	Session, cache, personal, team, enterprise, training, and deletion rules.
What may be changed?	Corrections, annotations, evidence, transactions, and authoritative write-back path.

05 Application, Agent, and Integration View

Components and interaction patterns

Component	Role
Personal agent host	Local or edge interaction, personal context, device authentication, and controlled enterprise delegation.
Enterprise experience layer	Conversation, forms, dashboards, notifications, approvals, accessibility, and user controls.
Alpha orchestration	Intent interpretation, workflow state, routing, context assembly, policy requests, tool coordination, and evidence capture.
Model and method router	Selects approved models, deterministic solvers, search, specialist agents, or people.
Agent registry	Owner, identity, purpose, version, capabilities, scopes, tools, status, and expiry.
Tool and action registry	Approved capabilities, schemas, owners, versions, risk, auth, rate, limits, and disable path.
Knowledge gateway	Purpose-bound retrieval across Enterprise Knowledge and State.
Policy decision and enforcement	Identity, purpose, data, action, amount, Delegated Autonomy, device, and risk decisions.
Workflow and transaction services	Long-running state, approvals, tasks, retries, idempotency, compensation, and commit.
Systems of record	Authoritative business state and durable records.
Event and integration services	Events, queues, APIs, service mesh, gateways, adapters, and lineage.
Observability and evidence	Logs, traces, metrics, evaluations, approvals, incidents, outcomes, and costs.

Integration pattern	Use
Request-response API	Synchronous retrieval, validation, calculation, and bounded actions.
Event-driven	Current-state updates, workflow triggers, monitoring, and decoupled processing.
Workflow orchestration	Long-running work, approvals, retries, compensation, deadlines, and human tasks.
MCP-style tool/context protocol	Focused resources and tools with host-controlled security boundaries and capability negotiation.
Agent-to-agent protocol	Collaboration between distinct agents with enterprise authentication, authorization, and task state.
Batch and document pipeline	Large-scale indexing, extraction, reconciliation, evaluation, and model preparation.
Human task queue	Specialist judgment, exception handling, approval, appeal, and recovery.

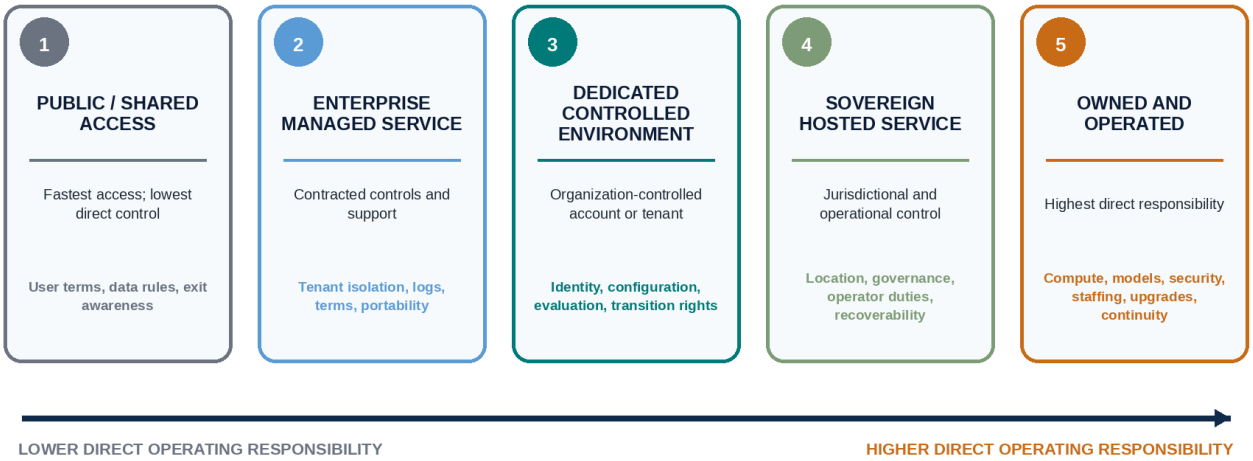
06 Technology and Compute View

Platforms, deployment, routing, observability, and resilience

Technology building block	Architecture concern
Model serving and APIs	Capability, data-use terms, latency, availability, security, version, and cost.
Organization-controlled model runtime	Accelerators, serving, scheduling, isolation, patching, capacity, performance, and support.
Routing and policy layer	Task, sensitivity, cost, reliability, location, and provider-selection rules.
Identity and secrets	Human and workload identity, federation, tokens, keys, vaults, attestation, revocation.
API gateway / service mesh	Authentication, authorization, rate limits, schemas, observability, egress, and service identity.
Data and knowledge platform	Storage, catalog, graph, vector, query, events, metadata, lineage, backup, recovery.
Workflow platform	State, timers, tasks, approval, retries, compensation, and audit.
Observability platform	Metrics, logs, traces, model and agent telemetry, data freshness, cost, incidents, and SLOs.
Security controls	Sandboxing, network isolation, content controls, DLP, supply-chain integrity, monitoring, response.
Resilience	Redundancy, diversity, failover, degraded modes, manual fallback, backup, restore, and testing.

Control, Ownership and Operating Responsibility

Ownership is one possible means of control, not the universal requirement



07 Trust, Security, and Assurance View

Threats, controls, evidence, and accountability

Threat-to-Control Model

Agentic systems need controls that answer named failure modes

Threat	Failure mode	Prevent	Detect	Respond / recover
Prompt or context injection	Untrusted content changes agent intent	Separate instructions from data; sanitize context; allowlisted tools; policy checks	Detect anomalous prompts and tool plans; log source and provenance	Pause workflow, revoke delegation, remove poisoned context
Tool poisoning or misuse	A tool, schema or description causes unsafe action	Signed registry; version pinning; narrow schemas; least privilege; sandboxing	Tool integrity checks; runtime policy; unusual-call monitoring	Disable tool, rotate credentials, reconcile affected transactions
Confused deputy	An agent acts with authority borrowed from another actor	Distinct identities; audience-bound tokens; per-client consent; purpose-bound delegation	Authorization telemetry; delegation chain review	Revoke chain, investigate, reauthorize explicitly
Retrieval or memory poisoning	False or malicious content enters working memory	Source allowlists; provenance; write controls; quarantine; human review	Freshness, anomaly and source-reputation checks	Remove entry, re-index, review dependent decisions
Excessive agency	Agent can execute more than the work requires	Autonomy Envelope; action limits; segregation of duties; approval thresholds	Exception rates, blast-radius monitoring, circuit breakers	Stop, rollback or compensate, downgrade autonomy
Cascading or partial failure	Multi-step action leaves inconsistent state	Idempotency; transaction boundaries; staged commit; compensation design	End-to-end tracing; reconciliation; timeout and retry limits	Compensate, restore authoritative state, reopen for human review
Supply-chain compromise	Model, code, plugin or provider is compromised	Due diligence; signed artifacts; isolation; SBOM; alternative provider path	Integrity monitoring; version drift; threat intelligence	Isolate, fail over, restore known-good version
Sensitive-information disclosure	Agent exposes data beyond purpose or authority	Data minimization; field-level access; output filtering; no implicit memory	DLP, access logs, canary data, exfiltration alerts	Contain, notify, delete, investigate and correct permissions

Trust boundary	Control questions
Person to personal agent	How is the person authenticated? What local information is used? What enterprise authority is delegated?
Personal agent to Alpha	Are agent identity, device posture, purpose, scope, audience, and duration verified?

Trust boundary	Control questions
Alpha to knowledge	Are source, classification, purpose, minimization, freshness, provenance, inference, retention, and response schema enforced?
Alpha to model	Is the model approved for the task, data, environment, performance, and provider conditions?
Alpha to tool	Is the tool registered, versioned, integrity-checked, least-privileged, and policy-enforced?
Tool to authoritative service	Does the downstream service independently validate identity, authority, business rules, and state?
Agent to agent	Is the delegation chain preserved and can sub-delegation be controlled or prohibited?
System to evidence	Can every material outcome be reconstructed and challenged?

08 Cross-View Contracts

Interfaces that protect the architecture boundaries

Contract	Minimum content
Intent contract	Requested outcome, requester, role, context, priority, deadline, and acceptable result.
Knowledge contract	Purpose, sources, fields, classification, freshness, provenance, inference, retention, response schema.
Delegation contract	Principal, agent, delegator, scopes, audience, amount, time, conditions, sub-delegation, revocation.
Model contract	Approved model/version, task, data, environment, evaluation status, limits, provider terms, fallback.
Tool contract	Owner, capability, schema, version, auth, allowlisted operations, limits, integrity, failure and disable.
Action contract	Operation, business rules, approval, idempotency, transaction boundary, commit, evidence, recovery.
Event contract	Event type, producer, schema, time, ordering, delivery, replay, sensitivity, consumer, retention.
Evidence contract	What must be measured, logged, retained, protected, reviewed, and linked to the outcome.
Recovery contract	Stop trigger, authority revocation, rollback or compensation, reconciliation, continuity, approval to resume.

09 Architecture Building Blocks

Reusable logical capabilities and solution choices

Architecture Building Block	Example Solution Building Blocks
Enterprise interaction and personal-agent host	Enterprise assistant, mobile/desktop agent host, browser extension, accessibility interface.
Alpha orchestration and workflow state	Agent orchestration platform, workflow engine, task queue, event processor.
Model and method routing	Model gateway, policy router, deterministic solver service, specialist agent catalog.
Knowledge gateway	Search, vector retrieval, graph query, structured query, document service, provenance layer.
Identity and delegated authority	Identity provider, workload identity, OAuth/OIDC, policy engine, token exchange, consent and delegation service.
Tool and action registry	API catalog, MCP servers, function registry, service catalog, schema and risk metadata.
Policy enforcement	API gateway, service mesh, authorization service, data policy, action policy, rate and amount controls.
Authoritative transaction services	ERP, CRM, HR, payments, case management, inventory, workflow commit services.
Evaluation and assurance	Test harness, red team, model evaluation, policy tests, observability, evidence repository.
Resilience and recovery	Failover, queue, manual fallback, backup/restore, compensation service, incident orchestration.

Solution Building Blocks are illustrative and client-specific. TIO defines the required capability, boundary, control, and evidence before selecting a platform or vendor.

10 Non-Functional Requirements

Architecture quality attributes and evidence

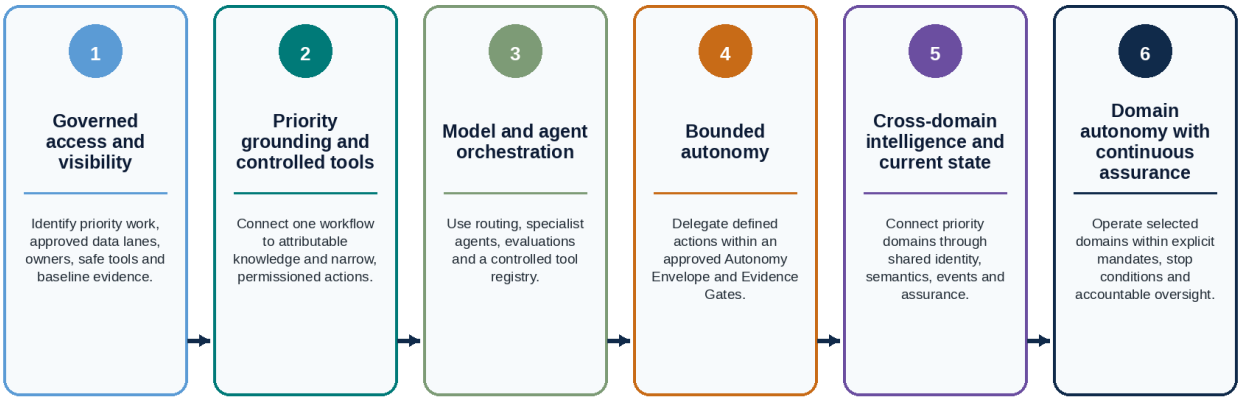
Attribute	Example requirement pattern
Security	Every request is authenticated and authorized per resource, purpose, action, and current conditions.
Privacy	Only the minimum information required for the approved purpose is processed, retained, and disclosed.
Reliability	Defined workflow success and exception thresholds are met on representative and perturbed cases.
Latency	P50/P95/P99 service targets align to the work and are measured end to end.
Availability	Mission-essential workflows have defined SLOs, degraded modes, and failover.
Recoverability	RTO/RPO, rollback, compensation, reconciliation, and manual restoration are tested.
Auditability	Material decisions and actions can be reconstructed from identity, source, model, tool, approval, transaction, and outcome evidence.
Portability	At least one alternative can pass the acceptance suite through documented contracts.
Operability	Named teams have runbooks, monitoring, support, patching, capacity, and incident responsibilities.
Scalability	Capacity and rate controls support forecast demand without unbounded cost or blast radius.
Accessibility	Interfaces meet the needs of intended users across disability, language, device, and work context.
Cost control	Budgets, unit costs, consumption limits, provider changes, and value measures are visible.

11 Transition Architectures

How the target state becomes a sequence of usable states

Progressive Realization Path

The end state is built through bounded operating slices, not a single transformation project



Progress is uneven by design. An organization may operate at advanced autonomy in one bounded domain while remaining at "recommend" or "prepare" for rights-affecting decisions.

Transition state	Architecture focus	Exit evidence
T1 Visibility	Inventory current AI uses, identities, data lanes, tools, owners, risks, and dependencies.	Named ownership, approved lanes, current-state map.
T2 Controlled assistance	Grounded search, analysis, drafting, and preparation through approved sources and tools.	Quality, source, access, user and cost evidence.
T3 Orchestration	Routing, agent registry, tool registry, workflow state, evaluations, and observability.	Contract conformance, regression, support and failure evidence.
T4 Bounded action	Approved low-consequence actions through deterministic services.	Envelope, Gate pass, exceptions, incidents, recovery.
T5 Cross-domain state	Priority domain events, semantics, lineage, reconciliation, and shared evidence.	Current-state integrity and continuity evidence.
T6 Domain autonomy	Defined domain operates within executive mandate and continuous assurance.	Sustained outcomes, independent review, residual risk, periodic reauthorization.

12 TOGAF ADM Crosswalk

How an EA team can use the TIO material

TOGAF ADM area	How TIO ESA contributes
Preliminary / Architecture Capability	0001, 0004, 0005, 0008 define evidence, governance, validation, and source controls.
Phase A: Architecture Vision	0101, 0301, and 0401 establish purpose, stakeholders, target-state hypothesis, principles, and value.
Phase B: Business Architecture	0103 and the Business View define outcomes, roles, decision rights, work, Delegated Autonomy, and management rhythm.
Phase C: Information Systems Architecture – Data	Data View defines Enterprise Knowledge and State, ownership, contracts, provenance, and transition path.
Phase C: Information Systems Architecture – Application	Application/Agent View defines components, services, interfaces, orchestration, workflows, and systems of record.
Phase D: Technology Architecture	Technology View and 0102 define models, hosting, identity, integration, observability, resilience, and portability.
Phase E: Opportunities and Solutions	Building blocks, deployment archetypes, and Evidence Gates support option and sourcing decisions.
Phase F: Migration Planning	Transition architectures and progressive realization provide sequencing and exit evidence.
Phase G: Implementation Governance	0103, 0201, contracts, policy, Gate decisions, and 0106 govern delivery and evidence.
Phase H: Architecture Change Management	ADRs, evidence triggers, model/provider change, incidents, evaluations, and release controls govern evolution.
Requirements Management	NFRs, contracts, threats, control outcomes, Evidence Gates, and client adaptation requirements operate across phases.

This crosswalk is an aid, not a claim that TIO replaces or reproduces the TOGAF Standard. The Open Group material remains the authoritative source for TOGAF and ArchiMate.

13 Use in Enterprise Architecture Practice

A practical sequence for architecture teams

1. Use 0101 and 0401 to establish the architecture vision and executive decisions.
2. Use 0103 to confirm mandate, accountability, control position, human authority, and initial scope.
3. Use this viewpoints pack to compare current and target states by stakeholder concern.
4. Use 0105 to record decisions, alternatives, consequences, and review triggers.
5. Use contracts and NFRs to guide solution design and procurement without prescribing one vendor stack.
6. Use transition architectures and 0201 to sequence bounded workflow slices and Delegated Autonomy.
7. Use 0106 to record independent review and field evidence before strengthening validation claims.
8. Feed outcomes, incidents, recoveries, provider changes, and client lessons into architecture change management.

TIO architecture discipline
The executive architecture should stay simple. Complexity belongs in controlled viewpoints, contracts, decisions, tests, and transition plans—not in unexplained framework language.

14 Source Notes

Standards and TIO sources supporting the viewpoints

Ref	Source	Location
E1	Moonshot AI, Kimi K3 Tech Blog: Open Frontier Intelligence, July 2026	https://www.kimi.com/blog/kimi-k3
E2	Open Source Initiative, The Open Source AI Definition 1.0	https://opensource.org/ai/open-source-ai-definition
E3	NIST AI 100-1, Artificial Intelligence Risk Management Framework 1.0	https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10
E4	NIST AI 600-1, Generative Artificial Intelligence Profile	https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence
E5	NIST SP 800-207, Zero Trust Architecture	https://www.nist.gov/publications/zero-trust-architecture
E6	NIST SP 800-207A, Zero Trust for Cloud-Native Applications	https://csrc.nist.gov/pubs/sp/800/207/a/final
E7	NIST NCCoE, Software and AI Agent Identity and Authorization Concept Paper, 2026	https://www.nist.gov/news-events/news/2026/02/new-concept-paper-identity-and-authority-software-agents
E8	NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems	https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final
E9	Model Context Protocol, Architecture Specification	https://modelcontextprotocol.io/specification/2025-06-18/architecture
E10	Model Context Protocol, Security Best Practices	https://modelcontextprotocol.io/docs/tutorials/security/security_best_practices
E11	Google, Agent2Agent Protocol: A New Era of Agent Interoperability	https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/
E12	The Open Group, How ArchiMate and the TOGAF Standard Complement Each Other	https://help.opengroup.org/hc/en-us/articles/32115987894930-How-the-ArchiMate-Language-and-the-TOGAF-Standard-Complement-Each-Other
E13	Regulation (EU) 2024/1689, Artificial Intelligence Act	https://eur-lex.europa.eu/eli/reg/2024/1689/oj
E14	Canada, Personal Information Protection and Electronic Documents Act	https://laws-lois.justice.gc.ca/eng/acts/P-8.6/
E15	CISA and UK NCSC, Guidelines for Secure AI System Development	https://www.cisa.gov/news-events/alerts/2023/11/26/cisa-and-uk-ncsc-unveil-joint-guidelines-secure-ai-system-development
E16	OWASP GenAI Security Project, Securing Agentic Applications	https://genai.owasp.org/2024/12/15/announcing-the-owasp-llm-and-gen-ai-security-project-initiative-for-securing-agentic-applications/
T1	TIO Leadership Domain Guide, Version 1.0 FINAL	Internal TIO Library
T2	TIO Factory Domain Guide, Version 1.0 FINAL	Internal TIO Library

Ref	Source	Location
T3	TIO Capability Guide: Data Access, Version 0.1 FINAL	Internal TIO Library
T4	TIO Capability Guide: Data Flow, Version 0.1 FINAL	Internal TIO Library
T5	TIO Capability Guide: Transformation, Version 0.1 FINAL	Internal TIO Library
T6	TIO Delivery Ecosystem Research Standard, Version 1.0	Internal TIO Library