

How can architectural commitments remain true in running technology?

Capability Infrastructure Architecture



Simon Owen | Empower Your World | v2.0 FINAL

Start here

Capability Infrastructure is not a product architecture. It is the technology-independent technical substrate that makes WP06 commitments implementable, governable, interoperable, recoverable and replaceable across separately governed deployments.

Hold these ideas first

- Inherited meaning precedes implementation convenience.
- Every consequential action requires current authority, attribution and a declared Composition.
- Agents may exercise delegated authority but may not originate accountability.
- Protective routes remain available through degradation and recovery.
- No supplier, model, store, runtime or operator becomes the sole durable carrier of commitments.

A worked route through the architecture

Follow one consequential action through the Composition Manifest, control decision, Governed Capability Interface, execution, authoritative record and lineage. Then test correction, Agent delegation, federation, degradation, recovery, portability and replacement.

How to read this paper

- ORIENT: understand the public question and the architectural boundary.
- UNDERSTAND: follow the worked route, distinctions and failure conditions.
- EXPLORE: inspect the canonical structures, roles, relationships, lifecycle and controls.
- REFERENCE: use definitions, invariants, provenance and validation material for precision.

Status note. The frozen source architecture remains authoritative. These pages add orientation and explanation without silently replacing controlled definitions, decisions or accepted visuals.

Capability Infrastructure Architecture

The technology-independent technical realisation architecture for the WP06 suite

v1.0 FINAL: FROZEN CANONICAL ARCHITECTURE BASELINE

This is the frozen v1.0 canonical architecture baseline for WP06.10, approved for freeze on 23 September 2026 following Engineering Cycle 2, the final integration, governance and freeze-readiness review. It is identical in architectural content to the v1.0 freeze candidate. It preserves the frozen laws, invariants, constructs, visuals and terminology; records the closure of every integration action; adds Architecture Conformance (Section 23); and classifies the Research Validation Register conservatively. Every change is recorded in Appendix D. Research positions in Section 22 are not presented as proven.

Attribute	Value
Document	WP06.10 Capability Infrastructure Architecture
Version	v1.0 FINAL
Status	Frozen canonical architecture baseline, 23 September 2026. Freeze approved by the owner following Engineering Cycle 2: final integration-action closure, cross-paper boundary review, canonical terminology freeze, architecture conformance, research register reclassification and visual review (Appendix D.12)
Owner	Simon Owen
Date	23 September 2026
Series position	WP06.10 of WP06.0 to WP06.12
Purpose	The technology-independent technical realisation architecture that makes the commitments of the WP06 architecture implementable, governable, interoperable, recoverable and replaceable across separately governed deployments
Supersedes	WP06.10 v1.0 freeze candidate, v0.2 freeze candidate and v0.1 authoring draft (all 23 September 2026), each retained unchanged. WP06.10 also replaces the planned working title Platform, Integration and Technical Architecture still carried in the series tables of WP06.1 to WP06.8 v2.0 (IA-10.01)
Frozen inputs	WP06.0 to WP06.8 at v2.0, each a frozen canonical architecture baseline dated 21 September 2026; WP06.9 v1.0 FINAL and WP06.12 v1.0, each a frozen canonical architecture baseline dated 22 September 2026
Candidate input	WP06.11 v1.0 (22 September 2026) is recorded in its own document control as a candidate architecture baseline, not a frozen baseline; status re-verified on 23 September 2026. Dependencies on it are explicitly provisional, and no law, invariant, floor element or CC-3 or CC-4 obligation depends on it (IA-10.08; ED-10.05)
Input audit	File names, internal version, status, baseline date and supersedes metadata verified for every input on 23 September 2026 (Appendix D.4) and re-read in full for the Engineering Cycle 2 boundary review (Appendix D.9)

Attribute	Value
Formatting	FS-017 applied: every data table has a visible, labelled header row marked as a repeating Word header row; callouts carry no fake headers; 10 pt minimum for all text, including text inside visuals at printed size; alternative text, caption and body explanation for every visual
Change control	Frozen. Engineering Cycle 1 and Engineering Cycle 2 changes are recorded in Appendix D. Changes to this baseline require architecture review, a material contradiction, implementation evidence or a downstream proof obligation, and a new version. Dependencies on WP06.11 remain provisional until WP06.11 is frozen; their reconfirmation (IA-10.08) does not reopen this baseline unless it reveals a contradiction

CONTENTS

Section	Title
1	Purpose, ownership and reading guide
2	Why Capability Infrastructure matters
3	Canonical proposition
4	Architecture laws and Technical Realisation Invariants
5	Scope, boundaries and non-goals
6	Core architectural constructs
7	Technical realisation architecture
8	Federated control and execution model
9	Technical Responsibility Domains
10	Composition and the Composition Manifest
11	Governed Capability Interface
12	Semantic realisation, records and lineage
13	Distributed state and transaction integrity
14	Human-Agent architecture
15	Integration, federation and portability
16	Observability, degradation and continuity
17	Minimum Recoverable Capability State and recovery
18	Technical evolution, migration, renewability and replaceability
19	Quality attributes and the Minimum Infrastructure Floor
20	Failure modes and anti-patterns
21	Cross-paper integration
22	Validation, falsification and Research Validation Register
23	Architecture conformance
24; A to F	Architectural conclusion. Appendices: visual catalogue, glossary and terminology register, law and invariant traceability, decision record, manifest skeleton, scenario traces

WHY THIS PAPER EXISTS

1. Purpose, ownership and reading guide

The WP06 suite describes a Frontier Capability Organisation and the Capability Intelligence Platform that serves it. Eleven papers define what must be true: the platform proposition and boundary (WP06.1), the trust constitution (WP06.2), the semantic constitution (WP06.3), intelligence and judgement (WP06.4), lived journeys and Human Value (WP06.5), participation and propagation (WP06.6), Domains and the Domain Mesh (WP06.7), the operating model (WP06.8), requirements, controls and acceptance (WP06.9), evidence and assurance methods (WP06.11) and value exchange and economics (WP06.12).

None of those papers says how the commitments are made real in running technology. Each deliberately leaves that question open, and several explicitly defer it: WP06.3 states that it does not prescribe one database, graph product, API or physical schema and that WP06.10 will interpret its semantics technically; WP06.9 lists technical implementation as a non-goal and asks WP06.10 to adopt its register fields and traceability integrity rules as implementation requirements.

WP06.10 answers that deferred question. It defines the technical realisation architecture: the planes, responsibility domains, constructs, laws and integrity disciplines that any implementation must satisfy if it is to carry the WP06 commitments faithfully. It does so without choosing a technology, a vendor, a cloud or a product, because the commitments it carries must outlive every one of those choices.

WHAT THIS PAPER IS

The technology-independent technical realisation architecture that makes the commitments of the WP06 architecture implementable, governable, interoperable, recoverable and replaceable across separately governed deployments.

1.1 How to read this paper

Reader	Start with	Then read
Architect or design authority	Sections 3 to 7 (proposition, laws, scope, constructs, planes)	Sections 8 to 19 for the detailed disciplines; Section 23 for architecture conformance; Appendix C for law traceability
Engineer or implementer	Sections 6, 11 and 12 (constructs, Governed Capability Interface, semantic realisation)	Sections 13 to 18 for state integrity, Agents, federation, operations and evolution
Control owner or acceptance authority	Sections 4, 10 and 19 (laws, Composition Manifest, Minimum Infrastructure Floor)	Section 9 (TRD-08 and TRD-09), Section 21 for cross-paper integration and Section 23 for architecture conformance
Steward, sponsor or participant representative	Sections 2, 3 and 19 (why it matters, proposition, floor)	Section 14 (Human-Agent architecture) and Section 15 (portability and exit)
Researcher or reviewer	Section 22 (validation, falsification and Research Validation Register)	Appendix D (decision record and open items)

1.2 Normative language

The paper uses normative terms consistently with WP06.9. **Shall** marks an architectural obligation that an implementation must satisfy to claim conformance with WP06.10 (Section 23). **Should** marks a strong default that may be departed from only with a recorded reason. **May** marks a permitted option. A departure from a **shall** is not a design choice; it is an exception governed through WP06.9 exception, equivalence and compensating-control machinery.

Term	Meaning in WP06.10	Consequence of departure
Shall	Architectural obligation required for conformance	Exception under WP06.9; counts towards exception accumulation
Should	Strong default	Recorded rationale in the Composition Manifest
May	Permitted option	None
Candidate Canonical Pattern	Pattern adopted as the default realisation of a frozen law, pending implementation validation: the consistency classes of Section 13, the Agent memory classes of Section 14.6 and the Capability Information Disclosure View of Section 15.3.1	May be refined after validation; the law it realises does not change
Research position	Construct whose viability is not yet demonstrated (Section 22)	Must not be relied on as proven in design or acceptance decisions

1.3 Frozen inputs and ownership

WP06.10 inherits its meanings. Where this paper uses a concept owned elsewhere it uses that paper's definition unchanged and cites the owner. The table records what each paper owns and what WP06.10 does with it. Versions and statuses are those verified in Appendix D.4.

Paper	Owns	WP06.10 treatment
WP06.1	Platform proposition, value chain, platform boundary	Realises the platform boundary technically; does not redraw it
WP06.2	Rights, trust, privacy, security principles, remedy, jurisdiction	Enforces the principles in the control plane and floor; does not restate or reinterpret them
WP06.3	Entities, relationships, events, states, lineage semantics	Realises persistence, projection, lineage and correction; does not redefine any semantic object
WP06.4	Signals, QuestionFrames, patterns, interpretation, intelligence	Provides data and analytics enablement (TRD-07); performs no interpretation
WP06.5	Lived journeys, Human Value	Makes journeys executable and accessible; does not design them

Paper	Owns	WP06.10 treatment
WP06.6	Participation, propagation, organisational and stewardship transition	Supports transition technically (migration, coexistence); does not define change method
WP06.7	Domains, Domain Mesh, lifecycle	Realises Domain boundaries, packs and compatibility; does not define Domains
WP06.8	Operating model, decision rights, roles	Binds technical authority to decision rights; does not allocate roles
WP06.9	Requirements, controls, acceptance, compliance, traceability	Provides control hooks, register realisation and trace queries (TRD-08); performs no acceptance
WP06.11	Evidence methods, assurance methods, confidence (v1.0 candidate baseline)	Emits evidence in method-ready form; makes no confidence judgement; dependencies provisional until WP06.11 is frozen
WP06.12	Value exchange, economics, participation economics	Records exchange events and exposes cost of floor and correction; sets no economic policy

WHY TECHNICAL REALISATION MATTERS

2. Why Capability Infrastructure matters

Architecture that cannot be implemented is aspiration. Implementation that is not governed by architecture quietly becomes the architecture. Both failures are common, and both are especially dangerous for a system whose purpose is to hold commitments to people over time.

Technology choices carry embedded assumptions: about who is a user, what a record is, when a transaction is complete, who may see what, and what happens when something goes wrong. When those assumptions are made silently by products, platforms or integration convenience, they override the commitments the organisation believed it had made. A right to challenge disappears because the workflow engine has no state for 'contested'. A correction does not reach the decisions that relied on the corrected fact because the analytics store keeps its own copy. An Agent acquires authority because a service account was the simplest way to connect it. A participant cannot leave with their evidence because the export was never designed.

2.1 Five recurring failures

Failure	How it occurs	What WP06.10 does about it
Implementation capture	A product's data model or workflow semantics silently redefine WP06 concepts	TR-L1 and TR-L2 through TRI-01 and TRI-02; semantic binding at every Governed Capability Interface (Section 11)

Failure	How it occurs	What WP06.10 does about it
Authority drift	Technical credentials stand in for authority; revocation does not propagate	Federated Control Plane (Section 8); authority freshness (Section 13.3); DelegationGrant realisation (Section 14)
Silent staleness	Decisions rely on projections whose age and source are invisible	Current-State Projection discipline (Section 12.4); consistency classes (Section 13)
Uncorrectable history	Corrections overwrite records or never reach dependants	Append-and-supersede records; correction propagation (Section 12.6)
Lock-in and stranded participants	Deployments, suppliers or originators cannot be left without loss	Capability Information Package, originator exit and replaceability (Sections 15 and 18)

2.2 Why technology independence is a requirement, not a preference

The WP06 commitments are meant to endure across changes of supplier, generation of technology, organisational form and jurisdiction. A commitment that is true only while one product is in use is not a commitment of the organisation; it is a feature of the product. Technology independence is therefore not an aesthetic preference for abstraction. It is the condition under which the organisation, rather than its suppliers, remains the author of its obligations.

INDEPENDENCE TEST

If replacing a technology would require the organisation to renegotiate what it has promised participants, the technology has become part of the architecture, breaching TR-L13 and TRI-02.

2.3 Why separately governed deployments

The WP06 ecosystem is not one system run by one operator. Communities, organisations, partners and Domains will run their own deployments, under their own accountable operators and often in different jurisdictions. Their participants will move between them, and value, evidence and opportunity will flow across them. A technical architecture that assumes a single operator, a single database or a single control authority would either fail in this setting or impose a hidden centre that contradicts WP06.2 and WP06.12. WP06.10 is therefore designed from the outset for federation among deployments that recognise one another without commanding one another.

3. Canonical proposition

CANONICAL POSITION

Capability Infrastructure is the enduring, governed technical substrate through which the WP06 commitments are realised. It shall make every consequential commitment implementable, every consequential action governable and attributable, every exchange interoperable, every Composition recoverable and every technical element replaceable, across separately governed deployments and without allowing any technology to redefine what the architecture means.

3.1 Foundational limitation

WHAT INFRASTRUCTURE CANNOT DO

Capability Infrastructure can enable, constrain, evidence and make challengeable legitimate FCO operation. It cannot make an illegitimate organisation legitimate by technical means, nor can it guarantee honesty, justice, competence, participation, remedy or institutional courage.

The limitation is stated because a technical architecture of this depth can be mistaken for a guarantee. Conformance with WP06.10 shows that the technical means required by the WP06 commitments exist and operate; it does not show that the organisation using them is acting legitimately, that its decisions are just, or that its people will use the routes it provides. Those questions belong to WP06.2, WP06.8 and WP06.9 and, ultimately, to the people and institutions involved. The limitation is traced into the non-goals (Section 5.3), failure modes (Section 20), validation (Section 22), conformance (Section 23) and conclusion (Section 24).

3.2 Five properties

The proposition has five properties, each a verb the architecture must make true. Together they define what it means for a technical estate to be Capability Infrastructure rather than merely a collection of systems.

Property	What must be true	Primary sections
Implementable	Every WP06 commitment has a technical realisation path that does not depend on a single technology	6, 7, 9, 11
Governable	Every consequential action is authorised, policy-checked, manifest-bound and attributable at the point it occurs	8, 10, 13, 14
Interoperable	Deployments and services exchange meaning, not merely data, through Governed Capability Interfaces	11, 12, 15
Recoverable	Every Composition can resume its constitutional obligations after disruption from a declared minimum state	16, 17
Replaceable	Every Capability Service, Agent, supplier and deployment can be replaced or exited without loss of commitments	15, 18

3.3 The architectural stance

WP06.10 takes four stances that shape every section that follows.

- **Realisation, not redefinition.** WP06.10 is downstream of every paper whose concepts it carries. When implementation pressure conflicts with an upstream meaning, the meaning prevails and the implementation changes.
- **Responsibilities, not products.** The architecture is expressed as planes, responsibility domains, services and interfaces defined by what they must guarantee. Any technology that provides those guarantees may be used; none is assumed.
- **Proportion, above a floor.** Technical rigour scales with consequence, reversibility and harm, consistent with WP06.9 Minimum Sufficient Compliance, but never below the Minimum Infrastructure Floor (Section 19).
- **Federation by recognition.** Deployments cooperate through explicitly declared, bounded federation terms. No Deployment acquires authority over another through hosting or technical position.

3.4 What the architecture is not

WP06.10 is not	Why	Where the concern sits
A Microsoft architecture or any vendor architecture	Vendor mapping would make commitments contingent on one supplier	Separate reference implementations, outside the WP06 suite
A reference implementation or solution design	Designs choose technologies and topologies; the architecture constrains them	Implementation projects, each with its own Composition Manifest
An MVP architecture	Minimum scope is a delivery decision; the Minimum Infrastructure Floor is the architectural minimum	Delivery planning above the floor
A cloud or product architecture	Hosting and product choices are replaceable	Deployment design
A change methodology	Transition behaviour is owned elsewhere	WP06.6
A semantic architecture	Meaning is owned elsewhere	WP06.3
A trust constitution	Rights and principles are owned elsewhere	WP06.2
A compliance architecture	Requirements, controls and acceptance are owned elsewhere	WP06.9

CANONICAL PRINCIPLE FOR AGENTS

Agents may exercise delegated authority.

Agents may not originate accountability.

Every consequential Agent action shall trace to a valid DelegationGrant, a Human Authority Holder and an identifiable human or legal Accountable Party.

CANONICAL LAW FOR DISTRIBUTED STATE (TR-L16)

Consistency shall be proportionate to consequence, reversibility and harm.

THE LAWS THAT BIND EVERY IMPLEMENTATION

4. Architecture laws and Technical Realisation Invariants

WP06.10 is governed by two related sets of statements. The seventeen **frozen architecture laws** (TR-L1 to TR-L17) are reproduced below exactly as frozen in the WP06.10 structural baseline. They are canonical and may be changed only through architecture review. The sixteen **Technical Realisation Invariants** (TRI-01 to TRI-16) are the operational rules through which this paper makes the laws implementable and checkable. Every invariant realises at least one law; no invariant may weaken, narrow or contradict a law.

The TR-L and TRI prefixes are distinct from the WP06.9 traceability integrity rules TR-01 to TR-08, which WP06.10 realises in TRD-08 but does not renumber.

4.1 Frozen architecture laws

Law	Name	Frozen statement
TR-L1	Inherited Meaning Before Mechanism	Implementation shall preserve the meanings owned by the canonical WP06 architecture. No technical choice may redefine, narrow, merge or silently extend an inherited concept.
TR-L2	Semantic Invariance, Operational Elasticity	Canonical meaning and constitutional protections shall remain stable while deployment topology, implementation mechanisms and operational arrangements may vary.
TR-L3	Explicit and Current Authority	Every consequential action shall identify and verify sufficiently current, scoped and revocable authority.
TR-L4	Human or Legal Accountability Preservation	Technical execution, automation or delegation shall never eliminate the identifiable human or legal Accountable Party.
TR-L5	Consequence-Bounded Autonomy	Autonomy shall be constrained by declared purpose, authority, information, consequence, evidence, containment and challenge.
TR-L6	Shared or Mappable Meaning, Distributed Custody	Interoperability shall require shared or explicitly mapped meaning, not common storage, common custody or central ownership.
TR-L7	Universal Consequential Lineage	Every consequential outcome shall remain reconstructable in proportion to its consequence, including relevant source, transformation, authority, decision, execution and correction lineage.
TR-L8	Separately Governable Responsibilities	Technical responsibilities may be modular and separately governed, but their dependencies, shared semantics and systemic consequences shall remain explicit.
TR-L9	Declared Composition	Every consequential runtime Composition shall have reconstructable identity, purpose, authority, services, interfaces, dependencies, controls and operating state.

Law	Name	Frozen statement
TR-L10	No Automatic Trust Inheritance	Trust, acceptance or conformance of a component shall constitute evidence for, but never proof of, trust, acceptance or conformance of a Composition, Deployment or Federation.
TR-L11	Portability Without Semantic or Constitutional Loss	Information shall move with sufficient meaning, provenance, authority, permission, restriction, correction and challenge context to prevent materially misleading or constitutionally deficient reuse.
TR-L12	Capability Before Infrastructure	Technology shall be operated, recovered, migrated and replaced in service of legitimate capability and the commitments owed to participants and affected parties.
TR-L13	Replaceability by Design	No provider, model, store, connector, runtime or operator shall become the sole durable carrier of meaning, authority, essential evidence, organisational memory or continuity.
TR-L14	Constitutional Availability	Protected participation, challenge, correction, containment, exit and remedy shall remain available during normal, degraded, partitioned and recovery operation.
TR-L15	Renewal Through Evidence and Learning	Material change, failure, challenge, elapsed time and new evidence shall be capable of triggering review, re-acceptance and technical renewal.
TR-L16	Consistency Proportionate to Consequence	The strength and freshness of state consistency shall be proportionate to consequence, reversibility and harm.
TR-L17	Minimum Infrastructure Floor	Proportionality may reduce implementation burden but shall not remove the technical means required to preserve constitutional protection, accountability, correction, portability or recovery.

4.2 Technical Realisation Invariants

The invariants retain the operational rules developed in the v0.1 authoring draft, reclassified so that they sit beneath the frozen laws. Each invariant names the laws it realises and the sections that specify it. Appendix C traces every law through its invariants to sections, Technical Responsibility Domains, floor elements and WP06.9 requirements.

Invariant	Name	Statement	Realises	Sections
TRI-01	Architecture precedes implementation	No technical choice shall redefine, narrow or silently extend a concept owned by another WP06 paper. Where implementation and meaning conflict, the implementation changes.	TR-L1, TR-L2	5, 11.4, 12.1

Invariant	Name	Statement	Realises	Sections
TRI-02	Technology independence	Every construct shall be realisable by more than one technology, and no commitment shall depend on the continued use of a single product, vendor, cloud, model or operator.	TR-L2, TR-L13	3, 7.5, 18
TRI-03	Governed interaction contracts	Consequential capability shall be invoked, and information exchanged, only through Governed Capability Interfaces, whether automated, human-mediated, offline or hybrid. Ungoverned side channels, shared credentials and direct store access are prohibited for consequential operation.	TR-L6, TR-L3, TR-L7	11
TRI-04	Nothing consequential runs unmanifested	Every consequential Composition shall operate under a valid, current Composition Manifest governed by the control plane. An element absent from the manifest shall not act at consequence within the Composition.	TR-L9, TR-L8	10
TRI-05	Control is logically separated from execution	Identity, authority, trust, policy and conformance decisions shall be logically distinct from execution and enforced at the point of execution. No execution component may grant itself authority. Physical separation is required only where consequence, security, scale, resilience or independence demands it.	TR-L3, TR-L8	7.5, 8
TRI-06	Authority is verified, fresh and revocable	Every consequential action shall be preceded by verification of authority fresh enough for its consistency class, and every grant shall be revocable with declared propagation.	TR-L3, TR-L5	8, 13.3, 14.3
TRI-07	Authoritative history precedes projection	Consequential history shall be appended and superseded, never silently overwritten. Current state is a derived, rebuildable projection that declares its freshness and lineage.	TR-L7, TR-L1	12
TRI-08	Correction propagates	A correction shall reach every projection, dependent decision, Agent memory, federated recipient and package holder that relied on the corrected item, within a declared window.	TR-L7, TR-L11, TR-L14	12.6, 15.3
TRI-09	Consequential actions are auditable	Every consequential action shall produce an attributable, tamper-evident record of who or what acted, under which authority, manifest and policy version, for which Accountable Party, with what effect.	TR-L7, TR-L4	11.2, 12.2, 16

Invariant	Name	Statement	Realises	Sections
TRI-10	Delegated Agency preserves accountability	Agents may exercise delegated authority. Agents may not originate accountability. Every consequential Agent action shall trace to a valid DelegationGrant, a Human Authority Holder and an identifiable human or legal Accountable Party.	TR-L4, TR-L5	14
TRI-11	Protective routes remain available; unverifiable consequential actions fail closed	Under degradation, partition, recovery or control-plane unavailability, protected participation, challenge, correction, containment, exit and remedy routes remain available, while consequential actions whose authority cannot be verified do not proceed, except under the Emergency and Protective Action pattern.	TR-L14, TR-L3	8.2, 13.8, 13.10, 16.3
TRI-12	Federation creates no hidden centre	No Deployment acquires authority over another except under explicitly declared and bounded federation terms. Hosting, technical position or ownership of shared infrastructure confers no authority.	TR-L6, TR-L10, TR-L13	8.3, 15.2
TRI-13	Portability is designed in	Capability information shall be able to leave a Deployment, and reach the participant it concerns as a package or Disclosure View, preserving meaning, provenance, custody, permission, restriction and correction context.	TR-L11	15.3, 15.4
TRI-14	Recoverability is declared and tested	Every Composition shall declare its Minimum Recoverable Capability State and demonstrate recovery to it before operating at consequence.	TR-L12, TR-L14	17
TRI-15	The Minimum Infrastructure Floor precedes proportional scaling	The floor elements F1 to F8 shall be met before proportional scaling is applied; proportionality may simplify how they are met but shall not remove them.	TR-L17	19
TRI-16	Replaceability and Renewal are designed properties	Every Capability Service, Agent, supplier dependency, operator and Deployment shall carry a declared exit, migration and replacement path, and material change, failure, challenge, elapsed time and new evidence shall be able to trigger review and renewal.	TR-L13, TR-L15, TR-L12	18

TR-L16 is realised directly by the consistency-class discipline of Section 13 rather than through a separate invariant. TR-L8 is realised through TRI-04, TRI-05 and the Capability Service declarations in Section 9.1; TR-L10 through TRI-12, rule CM-02 and the no-inheritance rules in Sections 6.2 and 15.2; TR-L12 through TRI-14, TRI-16 and the recovery sequence in Section 17.2.

PRECEDENCE

The frozen laws prevail over every invariant and every other statement in this paper. Where laws appear to pull in different directions, TR-L14 (Constitutional Availability) and TR-L4 (Human or Legal Accountability Preservation) take precedence over efficiency and convenience, and TR-L1 (Inherited Meaning Before Mechanism) takes precedence over all implementation convenience. An invariant found to conflict with a law is defective and is corrected, not applied. A conflict between laws that precedence cannot resolve is an architecture defect escalated for review rather than resolved locally.

4.3 How the laws and invariants are used

- **Design:** every Composition Manifest declares, in section M8, how each applicable law is satisfied and through which invariants (the law and invariant conformance statement; Appendix E).
- **Acceptance:** WP06.9 design and operational acceptance may cite a law or invariant as the architectural basis for an acceptance criterion; neither is itself an acceptance decision.
- **Challenge:** any participant, steward or control owner may challenge a technical arrangement on the ground that it breaches a law or invariant; the challenge is routed through TRD-09.
- **Evolution:** a change that would weaken conformance with a law or invariant is a material change under Section 18 and, under TR-L15, triggers re-validation of the manifest.

WHAT THIS PAPER GOVERNS

5. Scope, boundaries and non-goals

5.1 In scope

- The five technical planes and their relationship to the inherited constitutional and semantic foundation.
- The ten Technical Responsibility Domains and the Capability Services that realise them.
- The eleven core constructs: Capability Infrastructure, Capability Service, Composition, Composition Manifest, Deployment, Federation, Governed Capability Interface, Current-State Projection, Capability Information Package, Minimum Recoverable Capability State and Minimum Infrastructure Floor.
- Distributed state and transaction integrity: consistency classes, authority freshness, concurrency, compensation, stale state, reconciliation, partition handling and irreversible action.
- The technical realisation of Human-Agent Configurations: Agent identity, DelegationGrant enforcement, authority boundaries, memory classes, tool use, containment, replacement and escalation.
- Federation, interoperability and portability across separately governed deployments, including originator exit.
- Observability, degradation, continuity, recovery, migration, renewability and replaceability.
- Quality attributes and the Minimum Infrastructure Floor.
- The frozen architecture laws TR-L1 to TR-L17 and the Technical Realisation Invariants TRI-01 to TRI-16 that make them implementable.

5.2 Ownership boundary with each paper

Boundary	Resolution
Semantics: WP06.3 and WP06.10	WP06.3 owns what an entity, relationship, event, state and lineage link means. WP06.10 owns how they are persisted, projected, versioned, exchanged and corrected. WP06.10 may add technical attributes (storage identifiers, integrity proofs, freshness markers) but never semantic attributes.
Trust: WP06.2 and WP06.10	WP06.2 owns rights, privacy, security principles, remedy and jurisdiction. WP06.10 owns the mechanisms that enforce them: identity validation, policy decision and enforcement, encryption boundaries, revocation and audit.
Compliance: WP06.9 and WP06.10	WP06.9 owns requirements, controls, acceptance and traceability rules. WP06.10 provides control hooks, operating evidence, register persistence and trace queries. A technical check is evidence for acceptance; it is never the acceptance. WP06.10 architectural conformance (Section 23) is evidence for WP06.9 acceptance and uses WP06.9 conformance states; it creates no acceptance decision, score or maturity level.
Assurance: WP06.11 and WP06.10	WP06.11 owns evidence and assurance methods and confidence statements. WP06.10 emits evidence with the provenance and completeness those methods require and records which method consumed it. Because WP06.11 v1.0 is a candidate baseline, every WP06.10 reference to its methods and vocabulary is provisional (IA-10.08); no law, invariant, floor element or CC-3 or CC-4 obligation depends on it.
Operating model: WP06.8 and WP06.10	WP06.8 owns decision rights and roles. WP06.10 binds technical authority to those decision rights through authority records and DelegationGrants; it does not decide who holds a right.
Domains: WP06.7 and WP06.10	WP06.7 owns Domain definition, the Domain Mesh and lifecycle. WP06.10 realises Domain boundaries as Participation Context and policy scopes, packages Domain capability as Compositions and enforces CompatibilityManifest constraints.
Intelligence: WP06.4 and WP06.10	WP06.4 owns signals, QuestionFrames, patterns and interpretation. WP06.10 provides governed data access, analytics environments and method-bound computation; it produces no interpretation of its own.
Transition: WP06.6 and WP06.10	WP06.6 owns participation, propagation and organisational and stewardship transition. WP06.10 provides coexistence, migration and parallel-running mechanisms that transition uses.
Economics: WP06.12 and WP06.10	WP06.12 owns value exchange and participation economics. WP06.10 records exchange events and makes the cost of the floor, correction and portability visible; it sets no price or economic rule.

5.3 Non-goals

Non-goal	Why it is excluded	Where the concern sits
Vendor or product selection	Selection is contingent and replaceable; the architecture must survive it	Reference implementations and procurement
Physical schemas and database design	Physical design is an implementation of WP06.3 semantics	Implementation projects under TRD-02
Topology, hosting and cloud design	Topology is a deployment decision within the constraints of this paper	Deployment designs
Delivery scope and MVP definition	Delivery sequencing is a project decision above the floor	Programme planning
Interpretation of law	WP06.10 enforces obligations imported through WP06.9; it does not interpret them	Qualified advisers
Evaluation of individual performance	Technical telemetry about people is not a performance instrument	Prohibited use under WP06.2; prohibited traversal under WP06.3
Manufacturing legitimacy	Technical architecture can enable, constrain, evidence and make challengeable legitimate operation; it cannot make an illegitimate organisation legitimate (Section 3.1)	WP06.2 trust constitution; the organisation's own governance

BOUNDARY TEST

If a technical design can only be justified by redefining an upstream concept, the design is out of bounds, however efficient it is. Raise the conflict through Appendix D rather than resolve it in code.

THE VOCABULARY OF REALISATION

6. Core architectural constructs

WP06.10 formalises eleven constructs. They are technical constructs: they describe how the architecture is realised, not what the organisation means. Each is defined once here and used unchanged throughout the paper. Where a construct relates to a semantic object owned by WP06.3, the relationship is stated so that the two cannot be confused.

Construct	Definition	Relationship to other papers
Capability Infrastructure	The enduring, governed technical substrate of Capability Services, Governed Capability Interfaces, records, control mechanisms and operational arrangements through which WP06 commitments are realised across one or more Deployments, and which can be inspected, challenged, recovered and replaced without loss of those commitments.	The whole of what WP06.10 governs; the platform boundary itself is owned by WP06.1
Capability Service	A bounded, separately governable unit of technical responsibility that realises obligations from one primary Technical Responsibility Domain, exposes its consequential operations through Governed Capability Interfaces, and declares its semantic, authority, consistency, evidence, degradation, dependency, ownership and replacement obligations.	May realise a WP06.3 Asset of type service; the Asset is the semantic object, the Capability Service is its technical realisation. Separately governable, with explicit dependencies and systemic consequences (TR-L8)
Composition	A declared, bounded arrangement of Capability Services, interfaces, policy bindings, records and human and Agent roles, assembled for a stated purpose within a Participation Context, whose behaviour and conformance are properties of the arrangement; the conformance of its parts is evidence for, never proof of, its own (TR-L10).	Realises a Capability Configuration (WP06.3) technically; the configuration is the semantic arrangement for action
Composition Manifest	The authoritative, versioned, human- and machine-readable declaration of a Composition, governed by the control plane, without which no element may act within the Composition (Section 10).	Distinct from the WP06.3 CompatibilityManifest, which a Composition Manifest references for Domain versions and dependencies
Deployment	A separately governed, operated instance of Capability Infrastructure under an identifiable accountable operator, jurisdiction and trust boundary, running one or more Compositions and exercising its own control plane.	The operator's organisational identity and decision rights are defined under WP06.8 and WP06.2
Federation	A governed and explicitly declared relationship among separately governed Deployments in which each retains its own authority while recognising defined identities, semantics, decisions, interfaces, obligations or trust states under bounded terms.	Types: Voluntary, Contractual, Mandated, Delegated and Emergency (Section 15.2). Hosting or technical position never creates authority (TRI-12)

Construct	Definition	Relationship to other papers
Governed Capability Interface	The declared contract through which capability is invoked or information is exchanged. It binds the interaction to identity, purpose, authority, semantics, consistency, evidence, lineage, correction, degradation, refusal, revocation and challenge obligations. Its implementation may be automated, human-mediated, offline or hybrid (Section 11).	Carries WP06.3 semantics; does not own them
Current-State Projection	A derived, rebuildable view of current state computed from authoritative events and records, carrying its as-of time, source lineage, consistency class and freshness bound; never itself the authoritative record.	A technical realisation that may serve a WP06.3 DomainView or other bounded projection
Capability Information Package	A self-describing, integrity-protected, portable bundle of records, evidence, lineage, permissions, semantic bindings and restrictions, with a Capability Information Disclosure View declaring custody, rights, transfer status and redaction for every element, that allows capability information to leave one Deployment and be received by another, or by the participant it concerns, without semantic or constitutional loss (TR-L11).	Canonical construct realising TR-L11 and TRI-13. Its Disclosure View is a Candidate Canonical Pattern, and long-horizon, cross-stack viability is research position RV-03. Does not imply that everything associated with a participant is owned by or exportable to them (Section 15.3)
Minimum Recoverable Capability State	The smallest set of authority state, commitments in flight, participant entitlements, authoritative records and lineage, and active configuration that must be recovered for a Composition to resume its constitutional obligations after disruption.	Defines what recovery must restore; projections and caches are excluded because they are rebuildable
Minimum Infrastructure Floor	The technical means that every Deployment and Composition shall retain whatever proportionality is applied (TR-L17): challenge route, accessible participation, authority record, correction capability, auditable consequential actions, continuity responsibility, portability and recovery.	Technical counterpart of the WP06.9 constitutional floor; research position for small-scale viability (RV-07)

6.1 How the constructs relate

The constructs form a single chain of realisation. A **Deployment** is the governed estate. Within it, **Capability Services** realise the responsibilities of the ten TRDs and are reachable only through **Governed Capability Interfaces**. Services are assembled into **Compositions**, each declared by a **Composition Manifest** that the Deployment's control plane validates, activates, suspends and retires. Compositions write authoritative events and records and read **Current-State Projections** derived from them. Deployments relate to one another through **Federation**, and capability information crosses those relationships, or returns to the

participant, as **Capability Information Packages**. Every Composition declares its **Minimum Recoverable Capability State**, and every Deployment meets the **Minimum Infrastructure Floor** before it scales. **Capability Infrastructure** is the name for the whole.

Construct	Is governed by	Governs or contains
Deployment	Its accountable operator under WP06.8; declared federation terms	Control plane, Compositions, Capability Services
Composition Manifest	The Deployment's Federated Control Plane	The Composition it declares
Composition	Its Composition Manifest	Capability Services, interfaces, Agent configurations, records
Capability Service	The manifests that include it; its service owner	Its Governed Capability Interfaces
Governed Capability Interface	The service contract and policy bindings	Every invocation and exchange across it
Current-State Projection	Its source records and declared freshness	Nothing: it is derived and replaceable
Capability Information Package	The permissions and restrictions it carries	The information it transports
Minimum Recoverable Capability State	The Composition Manifest (M9)	The recovery obligation
Minimum Infrastructure Floor	TR-L17, TRI-15 and the WP06.9 constitutional floor	Every Deployment and Composition

6.2 Construct discipline

- A construct shall not be used as a synonym for a semantic object. A Capability Service is not an Asset; a Composition is not a Capability Configuration; a Current-State Projection is not a DomainView. Each realises or serves the other.
- No construct confers authority. Authority comes only from authority records governed by WP06.8 decision rights and WP06.2 principles and verified in the control plane.
- No construct confers compliance. Under TR-L10, the trust, acceptance or conformance of a component is evidence for, but never proof of, that of a Composition, Deployment or Federation, consistent with the WP06.9 rule of no automatic inheritance.
- Every Capability Service has exactly one primary Technical Responsibility Domain for ownership and accountability and may declare contributing Technical Responsibility Domains whose obligations it also satisfies (Section 9.1).

THE SHAPE OF THE ARCHITECTURE

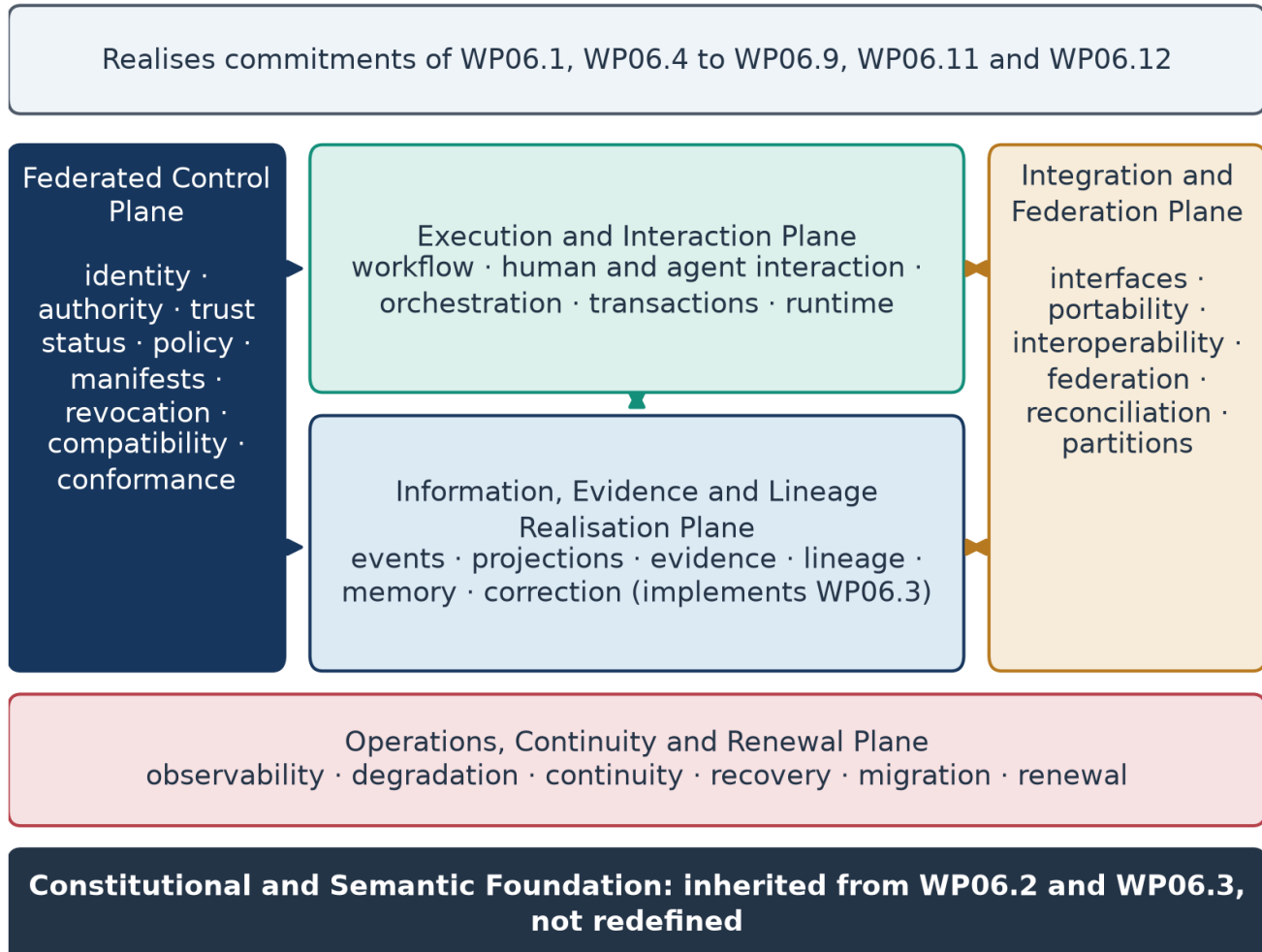
7. Technical realisation architecture

Capability Infrastructure is organised as five technical planes resting on an inherited constitutional and semantic foundation. A plane is a logical grouping of technical responsibility with a distinct integrity concern. Planes are not layers in a stack, tiers in a

deployment or products in a catalogue, and they need not be separately hosted (Section 7.5): one Capability Service may contribute to more than one plane, and one plane is realised by many services. What a plane defines is the guarantee its services must jointly provide.

VA-01 Technical Realisation Architecture

Five logical planes realise the WP06 commitments on an inherited foundation



Planes are logical responsibilities; physical packaging may vary (Section 7.5).

VA-01 Technical Realisation Architecture

7.1 Constitutional and Semantic Foundation

The foundation is inherited, not built. It consists of the trust constitution of WP06.2 (rights, trust, privacy, security principles, remedy and jurisdiction) and the semantic constitution of WP06.3 (entities, relationships, events, states and lineage semantics). WP06.10 does not redefine either. Every plane is obliged to respect the foundation, and every Governed Capability Interface binds its operations to it. Where a technical capability cannot honour a foundation principle, the capability is deficient; the principle does not bend.

FOUNDATION RULE

The foundation is referenced by every plane and owned by none of them. A technical plane that needs a new right, a new semantic object or a new lineage relationship raises it with the owning paper; it does not create it locally.

7.2 The five planes

Plane	Responsible for	Integrity concern	Characteristic failure
Federated Control Plane	Identity validation; authority validation; trust status; policy decisions; manifest governance; revocation; compatibility validation; conformance status	Whether an action is permitted, by whom, under which manifest and policy, now	Authority drift; stale revocation; self-granted permission
Execution and Interaction Plane	Workflow execution; human interaction; Agent interaction; orchestration; transaction execution; runtime operation	That permitted work is carried out as declared, with humans and Agents interacting through accessible, governed routes	Undeclared behaviour; inaccessible routes; ungoverned Agent action
Information, Evidence and Lineage Realisation Plane	Event storage; Current-State Projections; evidence realisation; lineage realisation; memory realisation; correction propagation	That WP06.3 meaning, history and lineage are faithfully persisted, projected and corrected	Overwritten history; invisible staleness; uncorrected dependants
Integration and Federation Plane	Governed Capability Interfaces; portability; interoperability; federation; reconciliation; partition handling	That meaning, authority and restriction survive every crossing between services and Deployments	Semantic loss in exchange; hidden centres; unreconciled divergence
Operations, Continuity and Renewal Plane	Observability; degradation; continuity; recovery; migration; renewability; replaceability	That the infrastructure keeps its commitments through disruption and change, and can be renewed or replaced	Silent degradation; unrecoverable state; lock-in

7.3 Plane obligations

Federated Control Plane

The Federated Control Plane decides; it does not execute. It holds or can verify the current state of identity, authority, trust status, policy, manifests, revocations, compatibility and conformance, and answers the question 'may this happen now?' for every consequential action. It is federated in two senses: each Deployment runs its own logical instance of the plane, referred to in this paper as that Deployment's control plane, under its own accountable operator; and control planes recognise one another's decisions only through declared federation terms. Section 8 specifies the plane in detail.

Execution and Interaction Plane

The Execution and Interaction Plane carries out work that the control plane has permitted. It runs workflows, hosts human interaction and Agent interaction, orchestrates services within a

Composition and executes transactions. It shall not decide authority for itself, shall not act outside a manifest, and shall present every consequential human interaction in an accessible form consistent with WP06.5 and the Supported Participation Principle of WP06.9. Agent runtime within this plane is governed by Section 14.

Information, Evidence and Lineage Realisation Plane

This plane implements WP06.3. It stores governed events, maintains authoritative records under append-and-supersede, derives Current-State Projections, realises evidence in method-ready form for WP06.11, realises lineage links, realises memory under the classes defined in Section 14.6 and propagates correction. It is the plane most exposed to implementation capture, because storage and analytics technologies carry strong assumptions about identity, time and mutability. Section 12 specifies it.

Integration and Federation Plane

This plane governs every boundary. It defines and enforces Governed Capability Interfaces, realises interoperability of meaning between services and Deployments, carries Capability Information Packages, operates declared federation terms, reconciles divergent state and handles network or organisational partition. Sections 11 and 15 specify it.

Operations, Continuity and Renewal Plane

This plane keeps the infrastructure honest over time. It observes behaviour and degradation, maintains continuity responsibility, executes recovery to the Minimum Recoverable Capability State, runs migration and supports renewal and replacement. Sections 16 to 18 specify it.

7.4 Cross-plane rules

Rule	Statement
XP-01	Every consequential action touches at least three planes: control (decision), execution (action) and information (record). An action that cannot be traced across all three is not auditable under TRI-09.
XP-02	No plane may bypass another. Execution may not write authoritative records except through the interfaces of the Information, Evidence and Lineage Realisation Plane; integration may not grant authority except through the Federated Control Plane.
XP-03	Degradation in one plane shall be visible to the others. A control plane that cannot verify authority shall signal the Execution and Interaction Plane, which shall apply TRI-11.
XP-04	Every plane's responsibilities shall be replaceable without replacing all others. Plane independence means replaceability and responsibility separation, not mandatory one-plane-per-product deployment (TR-L13; TRI-16).
XP-05	Logical separation of control, execution, information, integration and operational responsibilities is mandatory. Physical separation into different products, processes, services, stores, networks or teams is not mandatory unless consequence, security, scale, resilience or independence requires it (TR-L8; TRI-05).

7.5 Logical and physical separation

WP06.10 prescribes responsibilities, not a technical style. Rule XP-05 makes the logical separation of responsibilities mandatory while leaving their physical packaging to the Deployment. Conforming implementations may use any of the forms below, provided the logical obligations remain visible, enforceable, testable and replaceable.

Implementation form	Conforms when
Modular monolith	Plane and TRD responsibilities are separate modules with declared interfaces, and the control decision cannot be bypassed from execution code
Distributed services	Each service declares its primary TRD, interfaces and dependencies, and cross-service calls use Governed Capability Interfaces
Human and digital hybrid processes	Human steps carry the same applicable interface obligations and are recorded (Section 11.1)
Event-driven components	Events are governed, attributed and bound to WP06.3 semantics; consumers declare freshness
Shared infrastructure	Sharing confers no authority (TRI-12) and each party's obligations remain separately visible and replaceable
Independently hosted federated services	Federation terms declare what is recognised and how recognition is withdrawn (Section 15.2)

- **Append-and-supersede** is mandatory for consequential historical integrity. **Full event sourcing** is one optional implementation pattern, not a requirement.
- **Current-State Projections** need not imply command-query separation or any particular storage architecture; they require only the projection rules of Section 12.4.
- **Policy decision and enforcement** must be logically distinct but may coexist physically in smaller or lower-consequence Deployments, with explicit compensating controls declared in the manifest.
- **Plane independence** means that a plane's responsibilities can be replaced without replacing the others; it does not require one plane per product.

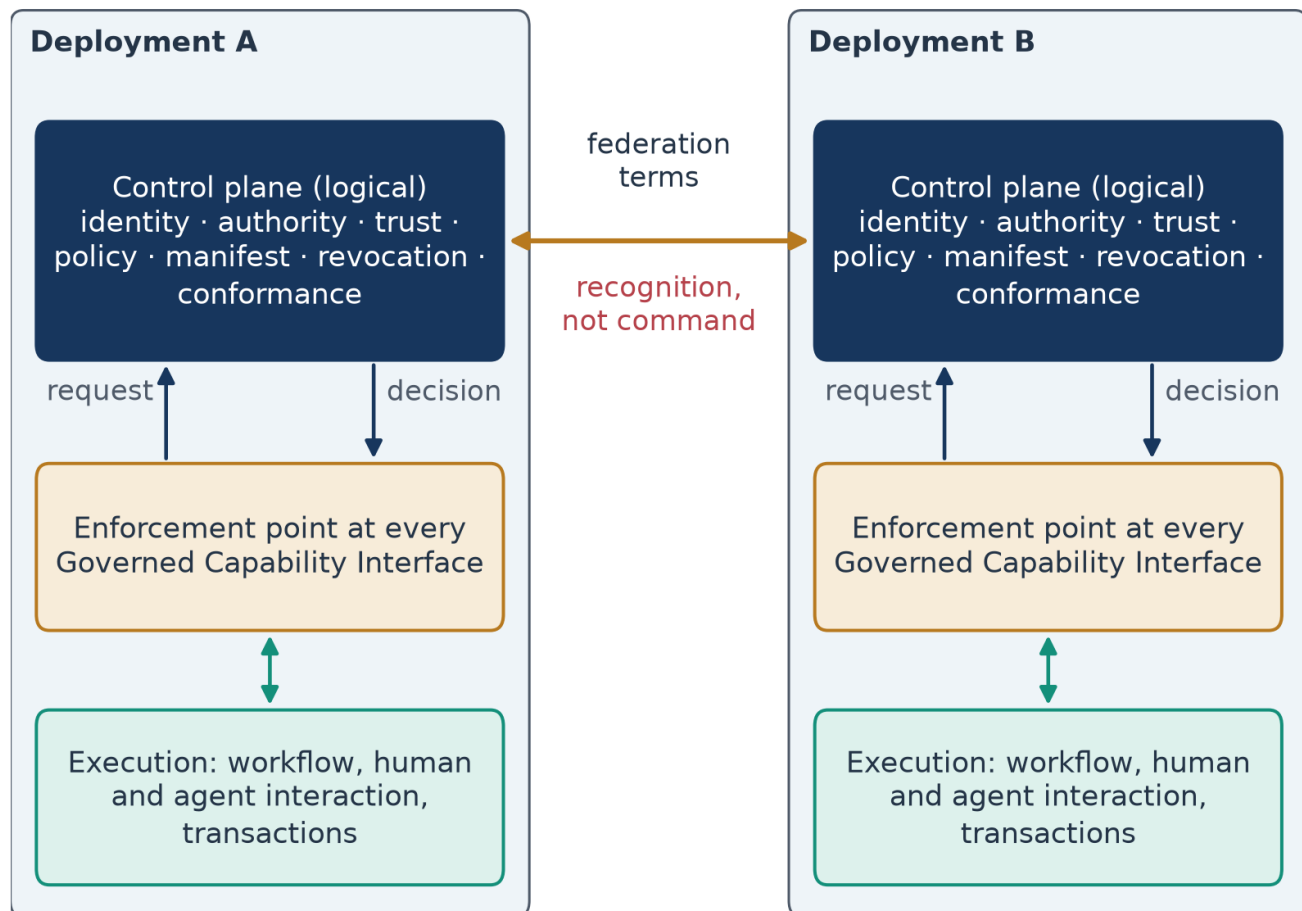
WHERE DECISIONS ARE MADE

8. Federated control and execution model

The separation of control from execution is the central structural decision of WP06.10 (TR-L3; TRI-05). The separation is logical: it may be realised within one component or across many, provided execution cannot decide its own authority (Section 7.5). It exists because the questions 'is this permitted?' and 'do it' have different integrity requirements, different owners and different failure consequences. When they are combined in the same component, the component becomes judge of its own authority, and authority drifts towards whatever is technically convenient.

VA-02 Federated Control and Execution Model

Each Deployment decides in its own control plane; enforcement happens at execution



VA-02 Federated Control and Execution Model

8.1 Control plane responsibilities

Responsibility	What the control plane decides or holds	Upstream owner of the rule
Identity validation	Whether a human, organisation, Agent or Deployment is who it claims to be, within a Participation Context	WP06.2 (principles); WP06.3 (identity semantics)
Authority validation	Whether the actor holds a current AuthorityGrant or DelegationGrant that covers this action, scope and consistency class	WP06.8 (decision rights); WP06.3 (grant semantics)
Trust status	The current trust standing of actors, services and federated Deployments, including suspensions and containment	WP06.2
Policy decisions	Whether policy permits the action given purpose, context, permission and restriction	WP06.2 (policy principles); WP06.9 (requirements)

Responsibility	What the control plane decides or holds	Upstream owner of the rule
Manifest governance	Which Composition Manifests are Draft, Validated, Active, Suspended, Superseded or Retired	WP06.10 (Section 10)
Revocation	Which grants, credentials, manifests and federation recognitions have been withdrawn, and whether withdrawal has propagated	WP06.2; WP06.8
Compatibility validation	Whether services, interfaces, Domain Packs and federated peers are compatible at declared versions	WP06.7 (CompatibilityManifest); WP06.10 (Section 11.6)
Conformance status	Whether a Composition currently meets the Minimum Infrastructure Floor and its declared law conformance; linked to WP06.9 Acceptance Records	WP06.9 (acceptance); WP06.10 (floor)

8.2 Decision and enforcement

Every Governed Capability Interface contains an enforcement point. For each consequential invocation the enforcement point assembles a decision request (actor, action, target, Participation Context, purpose, manifest, requested consistency class) and obtains a decision from the control plane. The decision is one of five outcomes.

Decision	Meaning	Execution behaviour
Permit	Authority, policy, manifest and conformance all satisfied at the required freshness	Proceed; record decision reference with the action
Permit with obligations	Permitted subject to stated obligations, for example notification, additional evidence or a hold period	Proceed only while meeting obligations; record obligation fulfilment
Escalate	The decision requires a human with authority, typically for CC-4 actions or Agent actions above the grant ceiling	Hold the action; route to a Human Authority Holder through TRD-06 or TRD-09
Deny	Not permitted	Refuse; return a reason the actor can understand and a challenge route (F1)
Indeterminate	The control plane cannot decide at the required freshness, for example during partition	Apply TRI-11: protective routes proceed; consequential actions do not

NO SILENT DENIAL

A denial or indeterminate decision affecting a person shall always carry a human-readable reason and a challenge route. A technically correct refusal that leaves the participant without explanation or recourse breaches the Minimum Infrastructure Floor.

8.3 Why the control plane is federated

A single global control plane would be the simplest design and the wrong one. It would place authority over every Deployment in the hands of whoever operates it, contradicting TRI-12, WP06.2 jurisdiction principles and the WP06.12 warning against dependency engineered as a revenue strategy. WP06.10 therefore requires each Deployment to operate its own logical control plane, which may run on shared infrastructure provided its decisions remain the Deployment's own, and to recognise others only under declared federation terms (Section 15.2) that state what is recognised (identities, trust status, revocations, conformance), for which purposes, with what freshness, and how recognition is withdrawn.

Federation element	What is declared	Withdrawal of recognition
Identity recognition	Which identity assertions from the peer are accepted, for which actor classes and contexts	Revocation notice; assertions no longer accepted after the declared window
Trust status exchange	Which trust and containment states are shared and how quickly	Peer marked unrecognised; cross-Deployment actions default to Indeterminate
Revocation propagation	Maximum propagation time for revocations by consistency class	Recognition suspended if propagation guarantees are not met
Conformance disclosure	Which floor and conformance states are disclosed to the peer	Peer treats the Composition as non-conformant
Decision reliance	Whether and when one Deployment may rely on the other's policy decision	Reliance ceases; local decision required

8.4 Control plane integrity

- **Separation:** the operators of a control plane shall not be the sole operators of the execution services it governs for CC-3 and CC-4 actions; where full separation is impractical at small scale, the combination is declared and compensated, consistent with WP06.9 separation rules. Policy decision and enforcement may coexist physically in smaller or lower-consequence Deployments, with explicit compensating controls (Section 7.5).
- **Self-governance:** changes to the control plane's own policies, manifests and trust anchors are themselves consequential actions, recorded, authorised and challengeable.
- **Availability:** control plane unavailability shall not remove protective routes (TRI-11). The Minimum Infrastructure Floor requires that challenge, exit and remedy intake can be recorded locally and processed when the control plane returns.
- **Observability:** every decision is recorded with its inputs, policy version and freshness, so that a decision can be reconstructed and challenged after the fact.

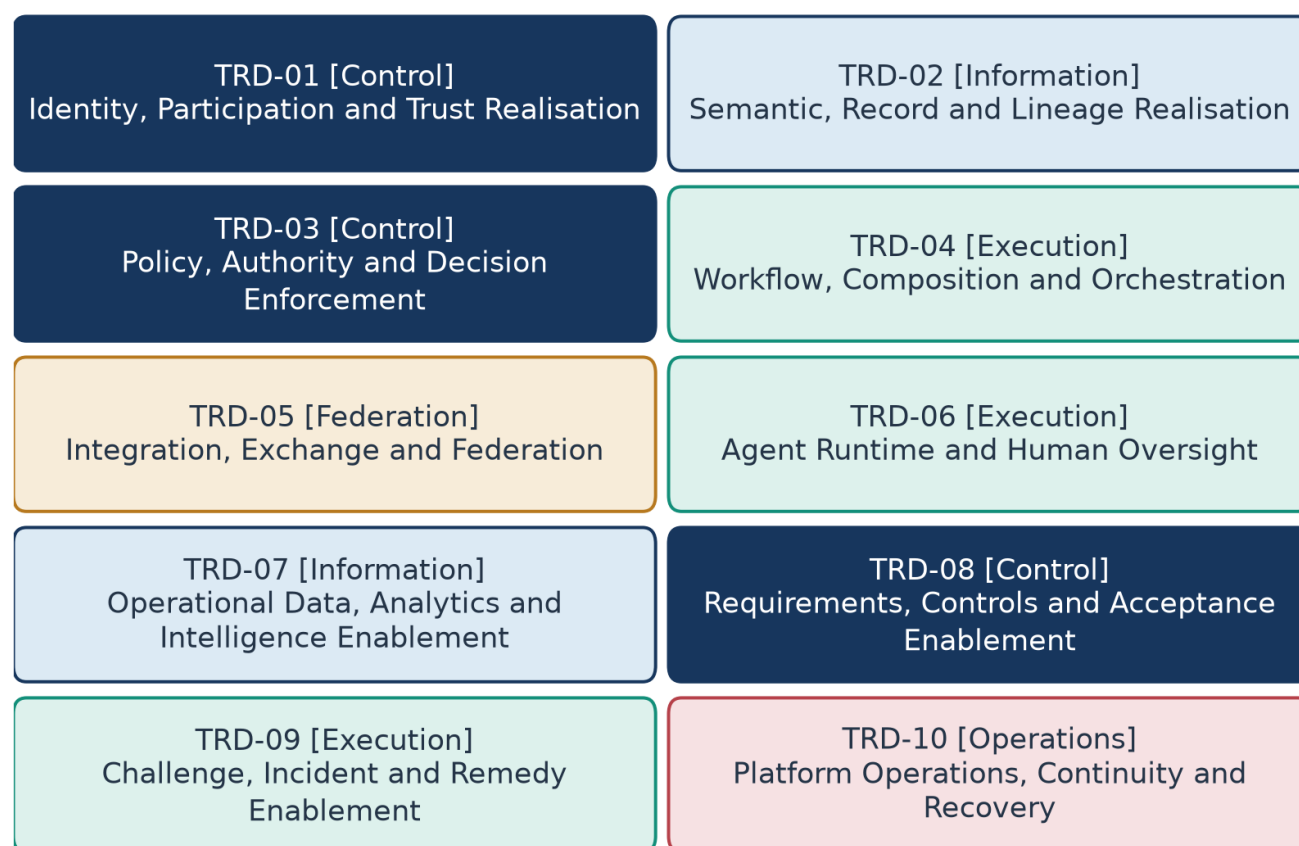
WHO IS RESPONSIBLE FOR WHAT, TECHNICALLY

9. Technical Responsibility Domains

The ten Technical Responsibility Domains (TRDs) allocate technical responsibility. Each TRD is a coherent area of technical obligation that can be owned, resourced, assured and replaced. Every Capability Service has exactly one primary Technical Responsibility Domain for ownership and accountability and may declare contributing Technical Responsibility Domains whose obligations it also satisfies. Services are separately governable, with explicit dependencies and systemic consequences (TR-L8). TRDs are not organisational units; WP06.8 decides who owns them (IA-10.03).

VA-03 Technical Responsibility Domains

Each Capability Service has one primary TRD and may declare contributing TRDs



Labels in brackets name the primary plane: Control, Execution, Information, Federation or Operations.

Colour repeats the label and is never the only signal.

VA-03 Technical Responsibility Domains

TRD	Name	Primary plane	Principal responsibilities	Upstream sources	WP06.9 Control Domains served
TRD-01	Identity, Participation and Trust Realisation	Control	Identity for humans, organisations, Agents and Deployments; Participation Context realisation; accessible participation routes; trust status	WP06.2; WP06.3 identity family; WP06.5	CD-01
TRD-02	Semantic, Record and Lineage Realisation	Information	Event and record persistence; Current-State Projections; lineage; correction propagation; memory realisation	WP06.3	CD-03
TRD-03	Policy, Authority and Decision Enforcement	Control	Authority records; policy decision and enforcement; revocation; decision recording	WP06.2; WP06.8	CD-04; CD-08
TRD-04	Workflow, Composition and Orchestration	Execution	Workflow execution; Composition assembly; manifest-bound orchestration; transactions and compensation	WP06.5; WP06.6; WP06.7	CD-06
TRD-05	Integration, Exchange and Federation	Federation	Governed Capability Interfaces; declared federation terms; Capability Information Packages; reconciliation; partition handling	WP06.1; WP06.7; WP06.12	CD-07; CD-01
TRD-06	Agent Runtime and Human Oversight	Execution	Agent identity; DelegationGrant enforcement; tool mediation; memory governance; containment; escalation; replacement	WP06.3; WP06.8; WP06.9 (CO-05)	CD-04; agentic controls
TRD-07	Operational Data, Analytics and Intelligence Enablement	Information	Governed analytical access; method-bound computation; signal and pattern data supply; traversal enforcement	WP06.4; WP06.11	CD-03
TRD-08	Requirements, Controls and Acceptance Enablement	Control	Register realisation; control hooks and operating evidence; trace queries; integrity checking	WP06.9	CD-08

TRD	Name	Primary plane	Principal responsibilities	Upstream sources	WP06.9 Control Domains served
TRD-09	Challenge, Incident and Remedy Enablement	Execution	Challenge intake and tracking; incident detection and containment support; remedy tracking; contamination tracing	WP06.2; WP06.9 (FR-15, FR-16)	CD-09
TRD-10	Platform Operations, Continuity and Recovery	Operations	Observability; degradation detection; continuity; backup and recovery to MRCS; migration; replacement	WP06.8; WP06.9 (FR-16)	CD-09; CD-06

9.1 Capability Service declarations

Because services are separately governable rather than independent, each Capability Service declares the following in manifest section M2. The declaration makes dependencies and systemic consequences explicit, as TR-L8 requires.

Declaration	Content
Primary TRD	The one TRD accountable for the service's ownership and assurance
Contributing TRDs	Other TRDs whose obligations the service also satisfies, with the obligations named
Service owner	The accountable owner under WP06.8
Technical dependencies	Services, stores, models, connectors, runtimes and operators the service relies on
Shared controls	Controls operated jointly with other services or parties, with the WP06.9 control owner
Systemic consequences	Effects on other services, Compositions or Deployments if the service degrades, fails or changes
Interfaces exposed and consumed	Governed Capability Interfaces with contract versions
Continuity dependency	What the service needs to continue, and what depends on its continuity
Replacement path	How the service can be replaced without loss of commitments (TR-L13)

9.2 TRD specifications

TRD-01 Identity, Participation and Trust Realisation

Realises the identity and participation family of WP06.3 (Human, Account, Organisation, ParticipationContext, Actor, AgentIdentity, ParticipationRoute) and the trust principles of

WP06.2. It establishes who or what is acting, in which Participation Context, and through which accessible route.

- Distinct, non-reusable identifiers for every human, organisation, Agent and Deployment; identifiers do not encode mutable meaning (WP06.3 modelling principle).
- Participation Context as the primary security, ownership and policy boundary, as WP06.3 cross-paper invariants require.
- Supported and accessible participation routes, including assisted, alternative-format and advocate routes that achieve the same outcome (WP06.9 Supported Participation Principle).
- Trust status for actors and federated peers, including containment states set by TRD-06 and TRD-09.

GUARDRAIL

Identity shall never be inferred from behaviour, and participation shall never be taken as evidence of capability, consistent with WP06.3 prohibited traversals.

TRD-02 Semantic, Record and Lineage Realisation

Implements WP06.3 technically. It is the custodian of authoritative history.

- Governed event storage and authoritative records under append-and-supersede (Section 12).
- Current-State Projections with declared freshness and lineage.
- Lineage links for every derived object, including derived-from, supersedes, resulted-in and learned-from.
- Correction propagation and CorrectionRecord realisation.
- Memory realisation, including OrganisationalMemoryRecord persistence and the Agent memory classes of Section 14.6.

GUARDRAIL

No semantic attribute may be added, merged or dropped for storage convenience. Physical design choices are recorded in the Composition Manifest so that they can be challenged.

TRD-03 Policy, Authority and Decision Enforcement

Realises the decision half of the control plane. It maintains authority records bound to WP06.8 decision rights, evaluates policy, enforces decisions and records them.

- Authority records for AuthorityGrants and DelegationGrants, with scope, validity, conditions and revocation state.
- Policy decision service and enforcement points at every Governed Capability Interface.
- Revocation with declared propagation windows by consistency class.
- Decision records sufficient to reconstruct any decision (inputs, policy version, freshness, outcome).

GUARDRAIL

Capability, seniority, service account or technical access never substitutes for authority. The WP06.3 invariant that Capability never creates Authority by itself is enforced here.

TRD-04 Workflow, Composition and Orchestration

Carries out declared work. It assembles Compositions from their manifests, executes workflows and transactions, orchestrates services and handles compensation.

- Manifest-bound assembly: only manifest-declared services, interfaces and roles participate.
- Workflow states that include contested, paused, held and compensated conditions, so that WP06.2 and WP06.9 routes are representable in execution.
- Transaction execution by consistency class, including compensation for CC-2 and holds for CC-3 and CC-4 (Section 13).
- Journey execution support for WP06.5 journeys and WP06.6 transitions without redefining them.

GUARDRAIL

A workflow engine's native states shall not limit the states a journey requires. Where a technology cannot represent a required state, the gap is a deficiency recorded against the manifest.

TRD-05 Integration, Exchange and Federation

Governs every crossing between services and between Deployments.

- Definition, publication, versioning and deprecation of Governed Capability Interfaces.
- Declared federation terms of every type and their technical enforcement.
- Capability Information Package production, verification and receipt.
- Reconciliation and partition handling across Deployments (Sections 13.7, 13.8 and 15.6).

GUARDRAIL

Exchange preserves meaning, provenance and restriction or does not occur; lossy exchange is recorded as a restriction on what the recipient may claim.

TRD-06 Agent Runtime and Human Oversight

Realises Human-Agent Configurations technically and keeps Agents within delegated authority.

- Agent identity bound to operator, model and configuration version.
- DelegationGrant enforcement at every Agent action and tool invocation.
- Tool mediation through Governed Capability Interfaces only.
- Memory class enforcement, containment ladder, escalation and replacement (Section 14).

GUARDRAIL

No Agent may hold a credential that bypasses TRD-03. An Agent that can act without a decision request is outside the architecture.

TRD-07 Operational Data, Analytics and Intelligence Enablement

Supplies WP06.4 intelligence and WP06.11 methods with governed data and computation, without interpreting.

- Governed analytical access that honours permission, purpose and Participation Context.
- Method-bound computation: no high-consequence metric is computed for decision use without the approved Method Pack required by WP06.3.
- Technical prevention of prohibited traversals, not merely documentation of them (WP06.3 semantic conformance question).
- Provenance and completeness markers that allow WP06.11 methods to assess evidence visibility and bias.

GUARDRAIL

Analytics stores are projections. They shall not become shadow authoritative records, and they receive corrections like any other projection.

TRD-08 Requirements, Controls and Acceptance Enablement

Realises the WP06.9 machinery technically, responding to WP06.9 integration action IA-05.

- Persistence of the Requirement, Control and Acceptance Registers with the fields defined in WP06.9 Section 14.
- Continuous checking of the WP06.9 traceability integrity rules TR-01 to TR-08 where tooling permits, with defects raised as Degradation Events.
- Control hooks: interfaces through which technical, agentic and hybrid controls report operating evidence.
- Trace queries in both directions, from commitment to profile and from control to commitment.

GUARDRAIL

TRD-08 records acceptance; it never performs it. Agent logs and automated checks are evidence, not acceptance, consistent with WP06.9 anti-capture safeguards.

TRD-09 Challenge, Incident and Remedy Enablement

Makes challenge, incident and remedy real in running systems.

- Challenge intake available on every consequential route, including during degradation, partition and recovery (F1; TR-L14; TRI-11).
- Incident detection, containment support and Containment Consequence Assessment recording.
- Decision contamination tracing using lineage, supporting WP06.9 Decision Contamination Review.
- Remedy tracking to completion, including residual harm records that cannot be closed as resolved.

GUARDRAIL

A challenge route that depends on the system being challenged, with no alternative, does not satisfy the floor.

TRD-10 Platform Operations, Continuity and Recovery

Keeps the infrastructure running, observable, recoverable and replaceable.

- Observability across all planes, including degradation signals mapped to WP06.9 Degradation Events.
- Continuity responsibility: a named accountable party for every Composition's continuity (F6).
- Recovery to the Minimum Recoverable Capability State and recovery testing.
- Migration and replacement execution (Section 18).

GUARDRAIL

Operational telemetry about people is not performance evidence and is subject to WP06.2 prohibited use.

9.3 TRD and plane matrix

The matrix shows how each TRD relates to each plane. 'Primary' marks the plane in which the TRD's services have their primary responsibility; a service's own primary TRD is declared separately (Section 9.1).

TRD	Control	Execution	Information	Federation	Operations
TRD-01	Primary	Contributes	Contributes	Contributes	Observed
TRD-02	Consumes	Consumes	Primary	Contributes	Observed
TRD-03	Primary	Enforced in	Records to	Recognised by peers	Observed
TRD-04	Consumes	Primary	Records to	Invokes	Observed
TRD-05	Consumes	Contributes	Contributes	Primary	Observed
TRD-06	Consumes	Primary	Records to	Invokes	Observed
TRD-07	Consumes	Serves	Primary	Consumes	Observed
TRD-08	Primary	Hooks into	Records to	Discloses	Observed
TRD-09	Consumes	Primary	Records to	Coordinates	Observed
TRD-10	Observes	Observes	Observes	Observes	Primary

HOW CAPABILITY IS ASSEMBLED

10. Composition and the Composition Manifest

Capability is delivered by arrangements, not by components. A journey, a Domain Pack, a Community's operating environment or a partnership pathway is a Composition: a declared arrangement of Capability Services, interfaces, policy bindings, records and human and Agent roles assembled for a purpose within a Participation Context. The Composition, not any of its parts, is what participants experience, what WP06.9 profiles as an object and what must be recovered after disruption.

10.1 Composition rules

Rule	Statement
CM-01	Every Composition has exactly one current Composition Manifest in Active state before it acts at consequence (TR-L9; TRI-04).
CM-02	A Composition's behaviour and conformance are assessed as a whole. Under TR-L10, the trust, acceptance or conformance of a component is evidence for, never proof of, that of the Composition (consistent with WP06.9 no automatic inheritance).
CM-03	Every element that acts within a Composition, including every Agent and every external service, is declared in its manifest. Undeclared elements are refused at the enforcement point.

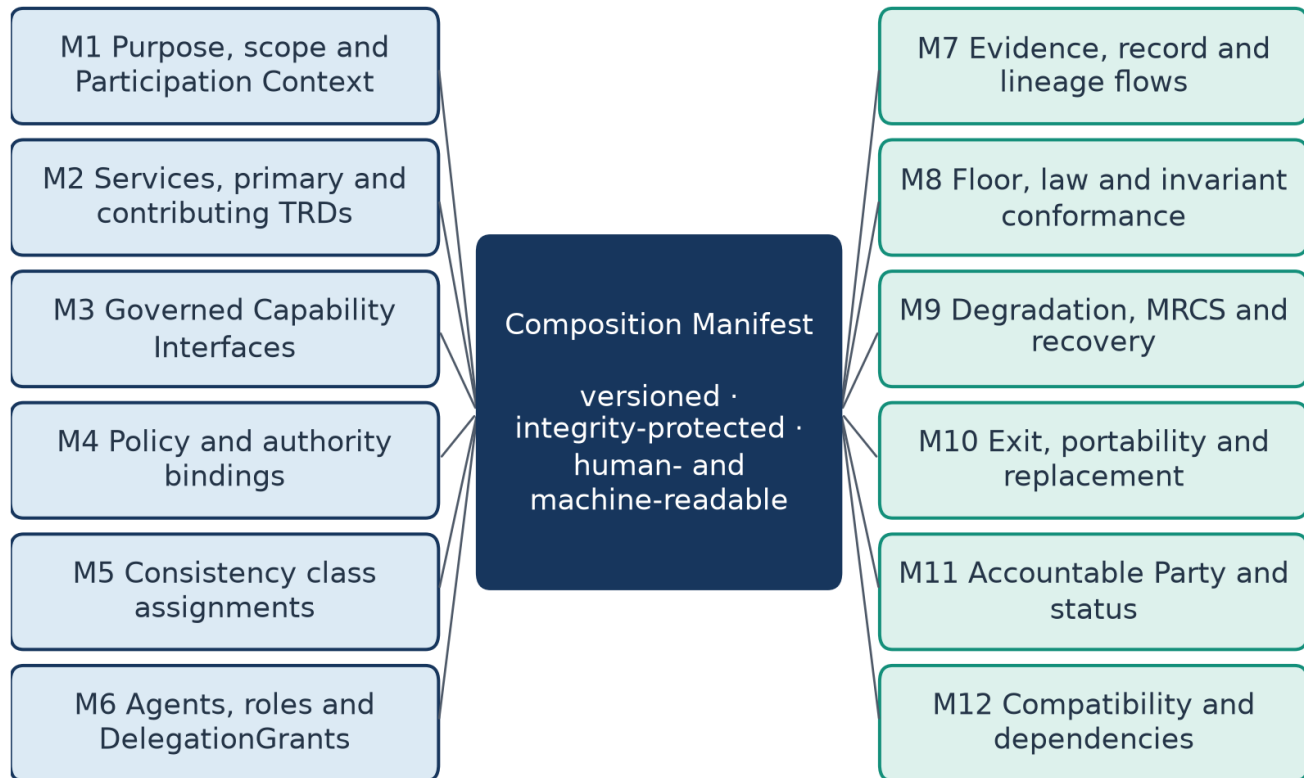
Rule	Statement
CM-04	A Composition operates within one declared Participation Context, or declares each context it spans and the policy that governs crossing between them.
CM-05	Compositions may include other Compositions only by reference to their manifests, so that nesting never hides responsibility.
CM-06	Every Composition names its Accountable Party (a human or legal person), an accountable owner acting for it and a continuity owner, who may be the same person.

10.2 The Composition Manifest

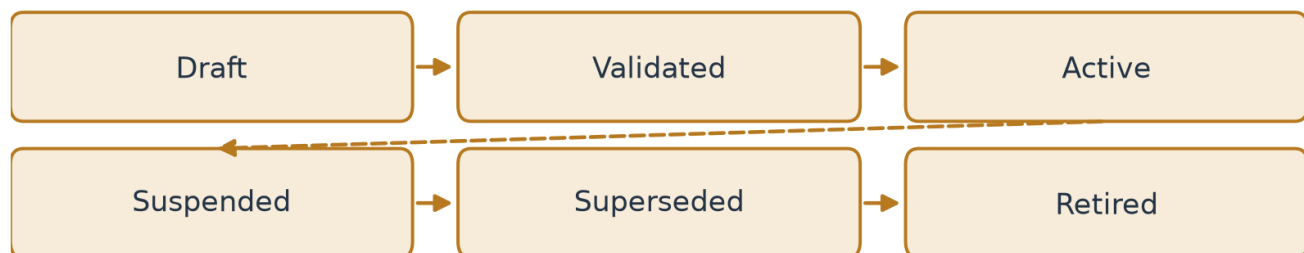
The Composition Manifest is the authoritative declaration of a Composition. It is both human-readable, so that stewards, control owners and participants' representatives can understand and challenge it, and machine-readable, so that the control plane can validate and enforce it. It is versioned, integrity-protected and governed by the Deployment's control plane. It is the means by which TR-L9 makes every consequential runtime Composition reconstructable.

VA-04 Composition Manifest Model

Nothing consequential acts outside a valid, current manifest



Manifest lifecycle



VA-04 Composition Manifest Model

Section	Content	Declares	Basis
M1	Purpose, scope and Participation Context	The purpose served, beneficiaries, Participation Context(s), Domain references, boundary and any federation terms relied on	WP06.1; WP06.7; WP06.9 object declaration; TR-L9

Section	Content	Declares	Basis
M2	Capability Services and declarations	Every service with its primary and contributing TRDs, version, owner, technical dependencies, shared controls, systemic consequences, continuity dependency and replacement path (Section 9.1)	TR-L8; TR-L13; TRI-16
M3	Governed Capability Interfaces	Every interface exposed or consumed, with contract version and realisation mode (automated, human-mediated, offline or hybrid)	TR-L6; TRI-03; Section 11
M4	Policy and authority bindings	Policies applied, authority sources, decision rights referenced	WP06.2; WP06.8; TRD-03
M5	Consistency class assignments	Class for each bounded consequential operation in its declared context, with rationale and any declared emergency envelope	TR-L16; Section 13
M6	Agents, roles and DelegationGrants	Agents with identities and configuration versions; Agent Principal, Human Authority Holder, Agent Operator and Accountable Party; grants, ceilings, memory classes and containment settings	TR-L4; TR-L5; TRI-10; Section 14
M7	Evidence, record and lineage flows	What is recorded, where, with what lineage and retention; evidence supplied to WP06.11 methods	WP06.3; WP06.11; TRD-02
M8	Floor, law and invariant conformance	How each floor element F1 to F8 is met; the law and invariant conformance statement for TR-L1 to TR-L17 and TRI-01 to TRI-16	TR-L17; TRI-15; Section 19
M9	Degradation, MRCS and recovery plan	Degradation behaviour, protective routes under degradation, MRCS definition, recovery objectives and last recovery test	TR-L12; TR-L14; TRI-11; TRI-14; Sections 16 and 17
M10	Exit, portability and replacement path	How participants obtain packages or Disclosure Views, how services are replaced, how the Composition is retired	TR-L11; TR-L13; TRI-13; TRI-16; Sections 15 and 18
M11	Accountable Party and conformance status	Accountable Party, accountable owner, continuity owner, current conformance status and linked WP06.9 Acceptance Records	TR-L4; WP06.8; WP06.9
M12	Compatibility and dependency declarations	CompatibilityManifest references, interface and Domain version constraints, deprecations	WP06.3; WP06.7

10.3 Manifest lifecycle

State	Meaning	Who may move it	Execution effect
Draft	Being prepared; not validated	Composition owner	No execution at consequence; test environments only
Validated	Control plane has checked completeness, compatibility, floor conformance and law statement	Control plane validation, with human sign-off for CC-3 and CC-4 content	Ready to activate; WP06.9 design acceptance may rely on it
Active	Current and enforced	Accountable owner, subject to WP06.9 acceptance where required	Composition executes as declared
Suspended	Enforcement paused because of degradation, incident, revocation or lapsed conformance	Control plane automatically, or an authorised human	Protective routes continue; consequential actions refused or held
Superseded	Replaced by a later Active version	Activation of the successor	No new actions; in-flight commitments completed or migrated
Retired	The Composition has ended	Accountable owner after exit obligations are met	No execution; records and lineage retained under WP06.3 lifecycle rules

10.4 Controlled Composition Variability

Deployments will not be identical. Communities, organisations and Domains need to vary Compositions to fit their context, scale and jurisdiction. Uncontrolled variation, however, destroys interoperability and makes assurance unrepeatable. WP06.10 resolves this tension through Controlled Composition Variability: variation is permitted within declared variation points and prohibited elsewhere.

Variation class	Examples	Rule
Fixed	Floor elements; frozen-law and invariant conformance; semantic bindings; protective route presence	Shall not vary between Deployments
Bounded	Consistency class of a given operation (may rise, never fall below the declared minimum); retention within WP06.2 limits; freshness windows	May vary within stated bounds; variation recorded in the manifest
Open	Technology choice; topology; user interface presentation above accessibility requirements; additional controls	May vary freely provided laws, invariants and floor are met

RESEARCH POSITION

Controlled Composition Variability is not yet demonstrated to preserve interoperability and repeatable assurance across many independently operated Deployments. It is registered as RV-02 in Section 22.

10.5 Manifest validation

Validation is performed by the control plane and produces a validation record. Validation is technical evidence for WP06.9 design acceptance; it is not the acceptance. A manifest is valid only if all of the following hold.

1. Every section M1 to M12 is present and complete for the Composition's consistency classes.
2. Every service in M2 exposes only interfaces declared in M3, each of which is a Governed Capability Interface (Section 11).
3. Every consequential operation has a consistency class in M5 and the class is at least the minimum for its consequence, reversibility and harm (Section 13.2).
4. Every Agent in M6 has an identity, a current DelegationGrant from its Agent Principal, a named Agent Operator, an identifiable Accountable Party and a declared containment setting.
5. Every floor element in M8 is met and the law and invariant conformance statement is complete, or the Composition is not permitted to act at consequence.
6. Compatibility declarations in M12 are satisfied by the current versions of all referenced services, Domain Packs and federated peers.
7. The MRCS in M9 is defined and a recovery test has been completed within its declared interval for Compositions at CC-3 or above.

THE ONLY WAY IN

11. Governed Capability Interface

An interface is where architecture is most often lost. Data leaves without its context, permission or history; operations are invoked without authority being checked; errors are returned without a route to challenge. The Governed Capability Interface (GCI) is WP06.10's answer (TR-L6; TRI-03). It is a governed interaction contract, not only a digital endpoint.

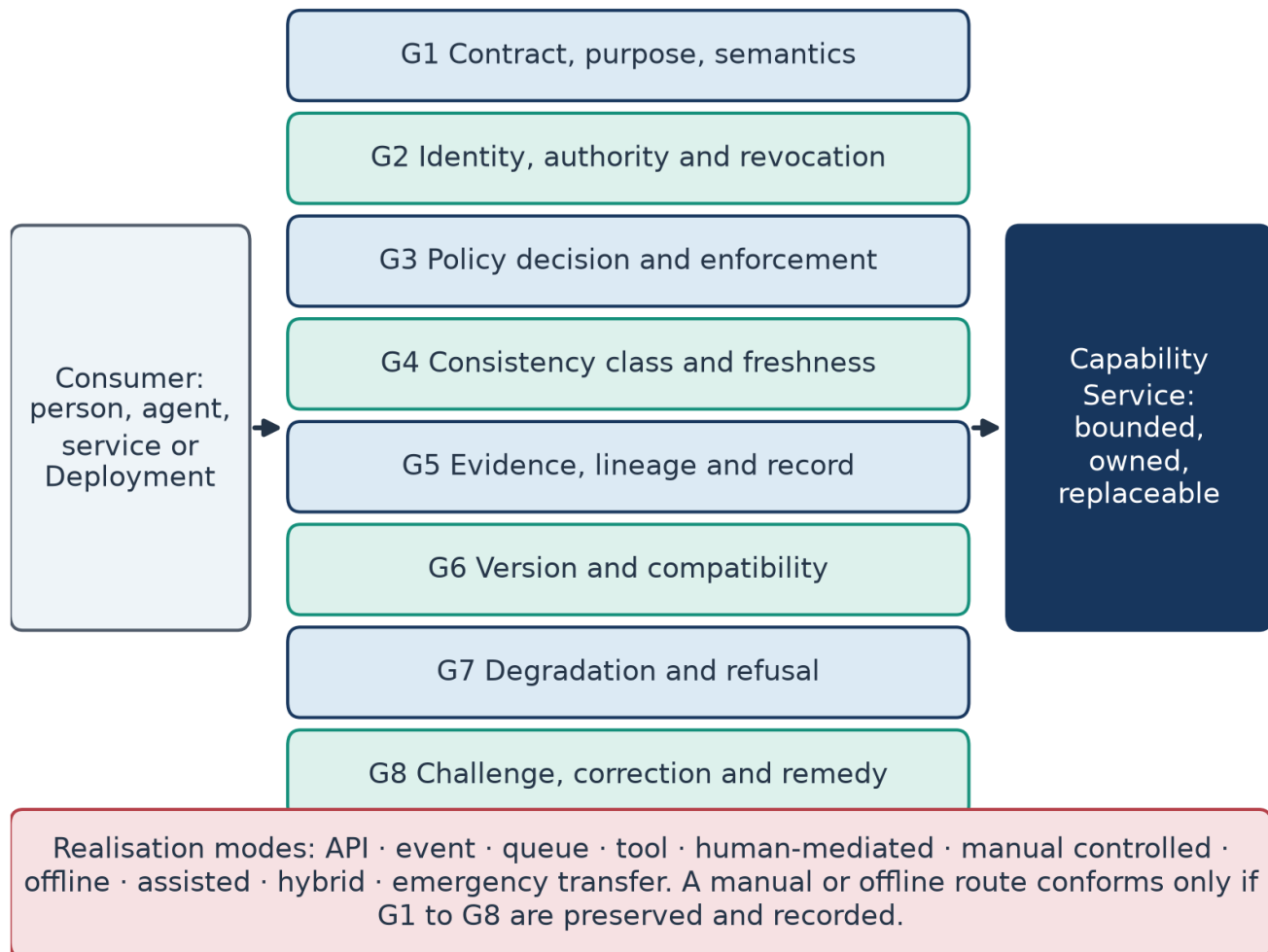
CANONICAL FORMULATION

A Governed Capability Interface is the declared contract through which capability is invoked or information is exchanged. It binds the interaction to identity, purpose, authority, semantics, consistency, evidence, lineage, correction, degradation, refusal, revocation and challenge obligations. Its implementation may be automated, human-mediated, offline or hybrid.

The prohibition on ungoverned side channels for consequential operation is retained. A manual or offline route is conformant only when the same applicable obligations are preserved and recorded: the identity and authority of the person acting, the purpose, the semantic content, the evidence and the challenge route must survive the route, even where no system is involved at the moment of interaction.

VA-05 Governed Capability Interface

A governed contract: automated, human-mediated, offline or hybrid



VA-05 Governed Capability Interface

11.1 Realisation modes

Realisation mode	Typical use	Conformance condition
Automated API	Service-to-service invocation	Enforcement point obtains a control decision; record emitted automatically
Event	Publication of governed events	Events attributed, bound to WP06.3 semantics and authorised for subscribers
Queue	Deferred or buffered work	Authority re-verified at processing time for CC-2 and above
Tool interface	Capability exposed to Agents	DelegationGrant scope and class ceiling checked before each call

Realisation mode	Typical use	Conformance condition
Human-mediated service	A person performs the operation for a participant	The person's identity, authority and the purpose are recorded; outcome recorded with lineage
Manual controlled exchange	Paper, verbal or file-based transfer between parties	A controlled log records who, what, why, under which authority and with which restrictions
Offline exchange	Operation without connectivity	Recorded locally; reconciled on reconnection (Section 13.7); CC-4 rules apply
Assisted participation	Supported route under the Supported Participation Principle	Same outcome as the primary route; assistance recorded without penalising the participant
Hybrid route	Part automated, part human	Every step preserves the applicable elements; hand-offs recorded
Emergency evidence transfer	Urgent protective sharing	Only under the Emergency and Protective Action pattern (Section 13.10)

11.2 Interface elements

Element	Requirement	Why it matters
G1 Contract, purpose and semantic binding	Each operation declares its purpose, inputs, outputs and effects in terms of WP06.3 entities, relationships, events and states, including context, time and permission dimensions	Prevents implementation capture; lets recipients know what the data means
G2 Identity, authority and revocation	Each operation declares the actor classes that may invoke it, the authority it requires and how revocation of that authority takes effect	Realises TR-L3 at the boundary
G3 Policy decision and enforcement	Each consequential invocation passes through an enforcement point that obtains a control plane decision	Realises TRI-05 at every crossing
G4 Consistency class and freshness	Each operation declares its consistency class and the freshness of authority and state it requires	Realises TR-L16
G5 Evidence, lineage and record	Each consequential operation emits an attributable record of what happened, under which authority and manifest, with lineage to its inputs	Realises TRI-09 and feeds WP06.9 and WP06.11
G6 Version and compatibility	Interfaces are versioned; breaking change requires a new version and a deprecation window	Protects federated peers and supports replaceability

Element	Requirement	Why it matters
G7 Degradation and refusal	Each operation declares how it behaves when dependencies are degraded and how refusals are expressed	Realises TRI-11; prevents silent failure
G8 Challenge, correction and remedy	Each consequential operation exposes a route to challenge its outcome and to request correction	Makes F1 and F4 reachable from every consequential action

11.3 Interface classes

Class	Purpose	Minimum elements
Command	Requests a consequential change of state	G1 to G8
Query	Reads state or projections	G1, G2, G3, G4 (freshness disclosed), G6, G7
Event	Publishes governed events to subscribers	G1, G2 (subscriber authority), G3, G5, G6
Exchange	Moves Capability Information Packages between Deployments or to participants	G1 to G8, plus package integrity verification
Control	Carries decision requests and decisions between enforcement points and control planes, or between federated control planes	G1, G2, G3, G5, G6, G7
Tool	Exposes a capability to Agents	G1 to G8, plus DelegationGrant scope check (Section 14.8)
Assisted or manual	Carries any of the classes above through a human-mediated, manual, offline or hybrid route	The elements of the class carried, preserved and recorded by the person or process acting (Section 11.1)

11.4 Semantic binding

Semantic binding is the discipline that keeps meaning intact across boundaries. Every field an interface carries is bound either to a WP06.3 semantic element or to a declared technical attribute (such as an integrity proof or a transport identifier). A field bound to neither is prohibited for consequential operations. Where two parties' implementations represent the same semantic element differently, the interface translates between representations and records the translation in lineage, so that a recipient can tell a transformed value from an original.

SEMANTIC LOSS RULE

If an exchange cannot carry a semantic dimension, for example context, time, permission or confidence, the recipient shall receive an explicit marker that the dimension is missing and shall treat the claim ceiling as constrained, as WP06.3 requires when a grammar dimension is unknown.

11.5 Refusal and error discipline

- A refusal shall distinguish denial (not permitted), indeterminate (cannot decide now), invalid (malformed or semantically unbound) and unavailable (dependency degraded).
- A refusal affecting a person shall carry a human-readable reason and a challenge route; technical error codes alone do not satisfy the floor.
- Retrying a refused CC-3 or CC-4 operation shall not bypass the hold or escalation that caused the refusal.

11.6 Compatibility and deprecation

Change type	Definition	Required handling
Additive	New optional operation or field bound to existing semantics	Minor version; no deprecation window
Semantic-preserving	Representation changes but binding is unchanged	Minor version; translation recorded in lineage
Breaking	Removed operation or field, changed binding or stricter authority	Major version; parallel availability through a deprecation window declared in M12; federated peers notified
Semantic change upstream	WP06.3 or another owner changes a meaning	Governed by the owning paper; WP06.10 realises through a major version and migration (Section 18)

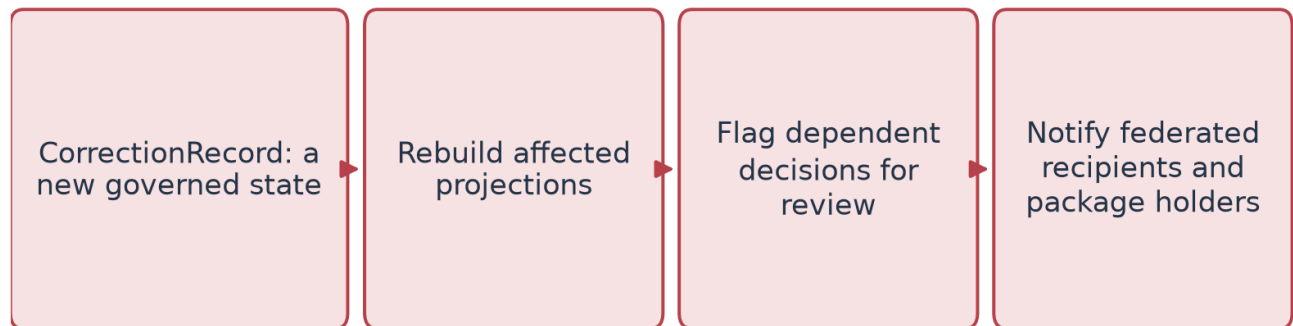
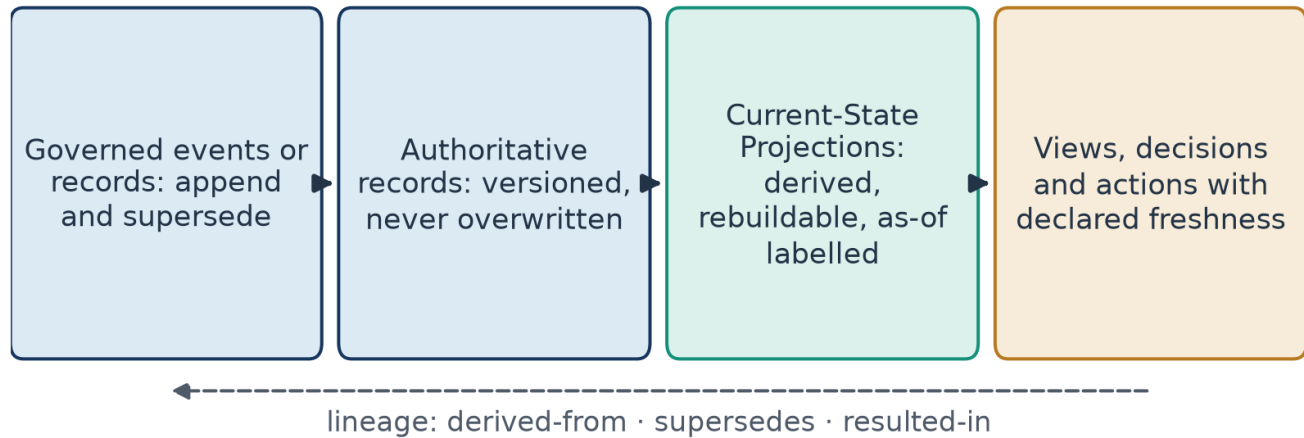
IMPLEMENTING THE SEMANTIC CONSTITUTION

12. Semantic realisation, records and lineage

The Information, Evidence and Lineage Realisation Plane implements WP06.3. It does not reinterpret it. Its task is to persist governed events and authoritative records so that history remains resolvable, to derive current state without mistaking a projection for the truth, to realise evidence and lineage so that every derived object can expose its sources, to realise memory under governance, and to make correction reach everything that relied on the corrected item.

VA-06 Semantic Realisation and Lineage

History is appended and superseded; projections are derived; correction propagates



VA-06 Semantic Realisation and Lineage

12.1 Realisation principles

WP06.3 modelling principle	Technical realisation
Stable identity	Identifiers are opaque, permanent and never reused; mutable meaning is held in versioned attributes
Definition before instance	Definitions, declarations, events, assessments, reviews and forecasts are stored as distinct record types, never collapsed into one table or document for convenience
Context before reuse	Participation Context and Domain context are carried with every record and every exchange
Append and supersede before overwrite	Consequential records are appended and superseded; supersession creates a new version linked to its predecessor. Full event sourcing is one optional way to achieve this

WP06.3 modelling principle	Technical realisation
Relationship before inference	Derived records hold typed lineage to sources and transformations
Time is part of meaning	observed-at, valid-from, valid-to, review-by and superseded-by are first-class attributes, distinct from technical write time
Uncertainty is representable	Contradictory assertions coexist until governed review; stores do not enforce a single value where WP06.3 permits alternatives

12.2 Event storage

Governed events, or equivalent append-and-supersede records, are the primary record of what happened. Each is attributed to an actor and authority, timed in both semantic time and technical time, bound to a Participation Context and a manifest version, and integrity-protected. Consequential records are never silently edited. A record later found to be wrong is superseded or corrected by a new record that references it. WP06.10 does not require full event sourcing; it requires append-and-supersede integrity for consequential history (Section 7.5).

Erasure, restriction and consequential history

Append-and-supersede and rights to deletion can pull in different directions. WP06.2 treats deletion, exit and remedy as system rights rather than discretionary support, and WP06.3 requires that retention and deletion vary by object, context, right and evidential need. WP06.10 does not claim the tension is resolved in every case. It adopts the following bounded architectural position, which Engineering Cycle 2 confirmed as sufficient for freeze (ED-10.02): it is consistent with WP06.2, WP06.3 lifecycle rules, correction propagation and the audit obligations of F5, and it leaves final treatment in each case to applicable law through the WP06.2 specialist review gate.

- Append-and-supersede preserves consequential history for integrity, correction and challenge.
- Personal content may require deletion, redaction, restriction or anonymisation, and the architecture shall be able to perform each.
- A minimum accountability trace (the fact that a consequential record existed and how it was treated) may remain only where legitimate and necessary.
- Applicable rights, jurisdiction and qualified legal interpretation govern the final treatment in each case; WP06.10 does not interpret law.
- Backups, projections, Agent memory, indexes and exported packages shall receive the corresponding retirement or restriction action, traced through lineage like a correction (Section 12.6). Erasure, redaction and restriction are themselves governed, attributable actions performed by an authorised party other than the actor whose record is affected, so that audit integrity is preserved without preventing lawful removal of personal content.

12.3 Authoritative records

Authoritative records hold the governed state of WP06.3 entities and relationships over time. They are versioned; every version carries validity interval, authority and lineage. The

authoritative record is the only source from which Current-State Projections, Capability Information Packages and federated exchanges may be derived.

12.4 Current-State Projections

Most decisions need current state, not history. Current-State Projections provide it. They are the most useful construct in the plane and the most dangerous, because a projection that is stale, partial or derived from an uncorrected source looks exactly like the truth.

Projection rule	Statement
CSP-01	Every projection declares its source records, derivation logic version, as-of time and freshness bound.
CSP-02	A projection is never authoritative, and need not imply command-query separation or any particular storage architecture. Writing to a projection does not change authoritative state.
CSP-03	Every projection is rebuildable from authoritative records; a projection that cannot be rebuilt is an undeclared authoritative store and breaches TRI-07.
CSP-04	A consumer using a projection for a consequential action shall check that its freshness meets the action's consistency class (Section 13).
CSP-05	Projections receive corrections. A projection that has not yet reflected a correction is marked as affected until rebuilt.
CSP-06	Projections honour prohibited traversals: a projection shall not join, aggregate or expose information in a way WP06.3 prohibits, whatever the query.

12.5 Evidence and lineage realisation

Evidence is realised so that WP06.11 methods can assess it: each evidence item carries its source, method of capture, context, time, completeness markers and any known visibility limitations. Lineage is realised as typed, queryable links using the WP06.3 relationship families. Lineage queries shall be able to answer, for any consequential decision, which evidence, projections, Agent outputs and records it relied on, and for any record, which decisions relied on it. The second direction is what makes correction propagation and WP06.9 Decision Contamination Review technically possible.

12.6 Correction propagation

WP06.3 requires that correction creates a new governed state rather than rewriting history silently, and that correction preserves prior state and downstream reliance. WP06.10 realises this as a propagation obligation (TR-L7; TRI-08), which also realises WP06.9 FR-15.02.

Step	Technical action	Evidence produced
1 Record	Create a CorrectionRecord superseding the corrected item, with reason, authority and effective time	CorrectionRecord and supersession link
2 Trace	Query lineage for all dependants: projections, decisions, Agent memories, exported packages, federated recipients	Dependency set

Step	Technical action	Evidence produced
3 Rebuild	Rebuild or mark affected every Current-State Projection in the dependency set	Rebuild records
4 Flag	Flag every dependent decision for WP06.9 Decision Contamination Review; TRD-09 tracks the review	Contamination flags
5 Notify	Notify federated recipients and package holders through Exchange interfaces within the declared window	Notification receipts
6 Inform	Inform affected participants where the correction concerns them, through accessible routes	Participant notices
7 Close	Record completion or residual gaps; unreachable dependants recorded as residual risk	Propagation completion record

RESEARCH POSITION

The economics of correction propagation at scale, including the cost of tracing, rebuilding and notifying across federated Deployments, are not yet understood. This is registered as RV-05. Until evidence exists, Deployments shall size correction capacity conservatively and report propagation completion rates.

12.7 Memory realisation

WP06.3 defines OrganisationalMemoryRecord as retained context linking prior observation, judgement, consequence and Learning, and treats Organisational Wisdom as a derived concept that is never a stored authority object. WP06.10 realises organisational memory as governed records under TRD-02, and realises Agent memory under the classes in Section 14.6. No technical memory, including Agent memory, may become an authority object or a shadow record that escapes correction.

KEEPING STATE HONEST ACROSS DISTANCE AND TIME

13. Distributed state and transaction integrity

Capability Infrastructure is distributed by nature. Services run in different places, Deployments are separately governed, networks partition, Agents act concurrently with humans, and control planes cannot always be reached. In such a system, perfect and instantaneous agreement about state is neither achievable nor affordable for every operation. The question is not whether to accept inconsistency but where, how much and with what safeguards.

CANONICAL LAW (TR-L16)

Consistency shall be proportionate to consequence, reversibility and harm.

CANDIDATE CANONICAL PATTERN

The consistency classes CC-0 to CC-4 are adopted as the default realisation of TR-L16. They are a Candidate Canonical Pattern introduced in Engineering Cycle 1 and retained in Engineering Cycle 2, pending implementation validation (RV-11). The law is canonical; the class boundaries, freshness obligations and partition behaviours below may be refined by evidence without changing the law.

The law rejects two common errors. The first applies the strongest consistency everywhere, which makes the system slow, brittle under partition and expensive enough to exclude small Deployments. The second applies eventual consistency everywhere because it scales, which allows irreversible harm to be done on the basis of stale authority. WP06.10 instead assigns each consequential operation a consistency class according to what is at stake.

VA-07 Distributed State and Transaction Integrity

Candidate Canonical Pattern realising TR-L16

Class	Commit requirement	Under partition
CC-0 Informational	Eventual; as-of shown	Proceed; mark stale
CC-1 Advisory	Bounded staleness declared	Proceed; label freshness
CC-2 Consequential, reversible	Fresh authority; compensation declared	Proceed locally; reconcile
CC-3 Consequential, hard to reverse	Strong consistency at commit	Queue or refuse
CC-4 Irreversible or rights-affecting	Strongest current verification; human confirmation	Refuse; emergency envelope only

Downward: rising consequence and harm, falling reversibility.
Class is assigned per operation in its declared context.

VA-07 Distributed State and Transaction Integrity

13.1 Consistency classes

Class	Name	Typical operations	Consistency at commit	Authority freshness	Reversal
CC-0	Informational	Displays, notifications, non-decision browsing	Eventual; as-of time shown	Any recognised authority; staleness tolerated	Not required; superseded by later state
CC-1	Advisory	Recommendations, signals, forecasts, draft analyses	Bounded staleness declared and displayed	Authority current within a declared window	Not required; advice is contestable
CC-2	Consequential, reversible	Scheduling, provisional allocations, reversible workflow steps, record updates with supersession	Read-your-writes within the Composition; fresh authority at commit	Verified within the class freshness window	Compensating action defined in advance
CC-3	Consequential, hard to reverse	Opportunity allocation, entrustment grants, payments, publication of claims, evidence transfer	Strong consistency on authority and target state at commit	Verified at commit against the authoritative record; revocation checked	Remedy plan; compensation where possible
CC-4	Irreversible or rights-affecting	Exclusion, erasure, sanctions, irreversible disclosure, withdrawal of rights, safety-relevant action	The strongest current verification and transaction integrity required to prevent conflicting or stale authority from committing the action; pre-commit hold where circumstances permit (Section 13.9)	Verified at commit, plus confirmation by a Human Authority Holder where human judgement is required	Remedy only; no compensation assumed

13.2 Assigning a class

The class is assigned per operation in manifest section M5, using the three factors named by the law and the WP06.9 proportionality factors. The assignment rule is conservative: an operation takes the highest class indicated by any factor.

Context-dependent classification

An operation may have different consistency classes in different Participation Contexts or under different consequences. The class is assigned to the bounded operation in its declared context, not solely to an interface name. The same record update may be CC-2 in a practice environment and CC-3 where it feeds an opportunity allocation; the manifest declares each context separately.

Where CC-4 appears in the tables below it refers to irreversible or rights-affecting operations. 'Linearisable' consistency, where used in distributed-systems discussion, is one possible implementation property of CC-4 commitment, not a universal technology requirement.

Factor	Indicates CC-0 or CC-1	Indicates CC-2	Indicates CC-3	Indicates CC-4
Consequence	No decision relies on it	Affects work, time or convenience	Affects income, opportunity, evidence or reputation	Affects rights, safety, exclusion or legal position
Reversibility	Fully and trivially reversible	Reversible by a defined compensating action	Reversible only partly or at cost	Irreversible
Harm	None foreseeable	Minor and recoverable	Significant or concentrated on vulnerable parties	Severe, lasting or rights-affecting

CLASS FLOOR AND VULNERABILITY

A Deployment may raise an operation's class but shall not lower it below the class indicated by this table. Vulnerability, power imbalance or limited alternatives shall require explicit reassessment of the class, protective routes and evidential threshold. The class shall rise where the vulnerability materially increases potential consequence or harm.

13.3 Authority freshness

Authority is not a fact that is true forever; it is a state that can be revoked, expire or be suspended. Every authority verification therefore has an age, and every consistency class sets the maximum age it will accept.

Class	Maximum authority age at commit	Revocation propagation obligation	When freshness cannot be met
CC-0	Any recognised authority	Best effort	Proceed; mark stale
CC-1	Declared window, shown to the user	Within the declared window	Proceed; label freshness
CC-2	Class window declared in M5	Within the class window across the Deployment	Proceed locally only if compensation is defined; otherwise hold
CC-3	Verified against the authoritative authority record at commit	Before any CC-3 action that relies on the revoked grant	Queue or refuse

Class	Maximum authority age at commit	Revocation propagation obligation	When freshness cannot be met
CC-4	Verified at commit and, where human judgement is required, confirmed by a Human Authority Holder	Synchronous: revocation effective before the next CC-4 decision	Refuse and escalate, unless the Emergency and Protective Action pattern applies (Section 13.10)

Federated authority (an identity or grant recognised from a peer Deployment) inherits the freshness obligations of the class, plus the propagation terms of the declared federation terms. Where the peer cannot meet the class obligation, cross-Deployment actions at that class are Indeterminate.

13.4 Concurrency

Concurrency arises whenever two actors, human or Agent, act on the same target at overlapping times. WP06.10 does not prescribe a concurrency mechanism; it prescribes outcomes.

- **CC-0 and CC-1:** concurrent updates may merge; the last-writer outcome is acceptable only where the semantics permit a single value and the loser is recorded.
- **CC-2:** conflicting updates are detected at commit; the second writer receives a conflict response with the current state and may retry or compensate.
- **CC-3 and CC-4:** the target is protected so that only one consequential action can commit on the basis of a given state; concurrent requests are serialised or refused.
- **Contradictions are not conflicts.** Where WP06.3 permits alternative assertions to coexist (for example competing interpretations or contested evidence), concurrency control shall not force a single winner.
- **Agents and humans are not privileged by speed.** An Agent's ability to act faster than a human shall not allow it to pre-empt a human decision on the same target; where a human decision is pending, Agent actions at CC-2 and above on that target are held.

13.5 Compensation

Compensation is a new, governed action that offsets the effect of an earlier one. It is the mechanism that makes CC-2 practical: an operation may proceed on locally fresh state because, if it later proves wrong, a defined compensating action restores an acceptable position.

Compensation rule	Statement
CP-01	Compensation is declared in advance in the manifest for every CC-2 operation. An operation without a declared compensation is at least CC-3.
CP-02	Compensation is a new event linked by lineage to the action it offsets; it never deletes the original.
CP-03	Compensation reaches affected parties. A technical reversal that leaves a person worse off without notice is not compensation; it is an incident.
CP-04	Compensation failures are recorded as WP06.9 Degradation Events and routed to TRD-09.

Compensation rule	Statement
CP-05	Irreversible effects cannot be compensated, only remedied. This is why CC-4 exists.

13.6 Stale state

Stale state is state that was true when observed and may no longer be. It is unavoidable; what is avoidable is acting on it unknowingly.

- Every projection, cached value and federated copy carries its as-of time and source (CSP-01).
- User interfaces presenting state for decision show freshness in plain language where the class is CC-1 or above.
- Agents shall check freshness against the class of the action they are about to take and shall not treat their own memory as current state (Section 14.6).
- Stale state discovered after a consequential action triggers the correction path in Section 12.6 if the action relied on a now-superseded value.

13.7 Reconciliation

Reconciliation restores agreement after divergence, whether caused by partition, concurrent federated activity or delayed propagation. WP06.10 prescribes a reconciliation discipline, not an algorithm.

Step	Action	Class treatment
R-1 Exchange	Peers exchange digests of events and record versions since last agreement	All classes
R-2 Detect	Divergent records and conflicting actions are identified	All classes
R-3 Merge	Divergence resolvable by WP06.3 supersession rules is merged automatically, with lineage	CC-0 to CC-2
R-4 Surface	Divergence involving CC-3 or CC-4 actions, or semantic contradictions, is surfaced to Human Authority Holders acting for the relevant Accountable Parties; never resolved silently	CC-3 and CC-4; contradictions
R-5 Compensate or remedy	Where reconciliation shows an action was taken on invalid authority or state, compensation (CC-2) or remedy (CC-3, CC-4) is initiated	CC-2 to CC-4
R-6 Record	A reconciliation record documents what diverged, how it was resolved, by whom, and any residual inconsistency	All classes

13.8 Partition handling

A partition is any condition in which parts of the system, or federated Deployments, cannot reach one another or their control plane reliably. Partitions will happen. The architecture's

obligation is that they do not cause the two harms that matter most: people losing their protective routes, and consequential actions being taken on unverifiable authority.

During partition	Behaviour
Protective routes	Challenge intake, accessible participation, exit requests and remedy intake remain available and are recorded locally for later processing (TR-L14; TRI-11)
CC-0 and CC-1	Proceed with freshness clearly labelled
CC-2	Proceed locally where authority was verified within the class window and compensation is defined; otherwise hold
CC-3	Queue for commit on heal, or refuse; queued actions are re-verified at commit, not merely replayed
CC-4	Do not proceed by default. Limited exception: a locally sovereign protective authority may take an urgent action within a previously declared emergency envelope where delay would create greater immediate harm. The action must be recorded locally, must not rely on unverified federated authority, and must undergo mandatory post-reconnection review and acceptance (Section 13.10)
On heal	Reconcile (Section 13.7); process locally recorded protective requests first; review every emergency action taken during the partition

RESEARCH POSITION

Partition reconciliation across many separately governed Deployments, especially where federated authority and correction propagation interact, is not yet demonstrated. It is registered as RV-08.

13.9 Irreversible action

Irreversible actions deserve their own discipline because the usual safety net of the architecture, correction and compensation, does not work for them. WP06.10 treats every irreversible or rights-affecting action as CC-4 and requires the following before commit.

1. Authority verified against the authoritative record at commit, with no reliance on cached or federated authority beyond the class obligation.
2. Confirmation, where human judgement is required, by a Human Authority Holder with the relevant decision right under WP06.8, acting within an accountability arrangement whose Accountable Party may ultimately be a legal person. An Agent may prepare but not confirm. Confirmation must be meaningful: WP06.2 holds that nominal human approval does not cure opaque delegation, so the confirmer must have visibility of the evidence, understanding of the consequence and the practical ability to refuse.
3. A pre-commit hold proportionate to the harm, during which the affected party is notified where WP06.2 permits and may challenge. The hold applies where the action and circumstances permit advance notice and challenge; urgent safeguarding or protective action may require immediate execution under the Emergency and Protective Action pattern (Section 13.10), followed by rapid review and challenge.
4. A recorded Containment Consequence Assessment where the action is a containment measure, consistent with WP06.9.

5. An attributable, tamper-evident record of the action, the authority, the confirmation and the evidence relied on.
6. A remedy route that remains available after the action.

IRREVERSIBILITY TEST

If the architecture cannot say who confirmed an irreversible action, on what evidence, under what authority and for which Accountable Party, the action should not have been technically possible.

13.10 Emergency and Protective Action pattern

Some harms cannot wait for the ordinary discipline. A safeguarding concern, an active security compromise or an Agent behaving dangerously may require immediate containment, even where full verification, advance notice or reconnection is not possible. The Emergency and Protective Action pattern makes such action possible without creating an unbounded exception. It applies only where delay would create greater immediate harm than acting. Engineering Cycle 2 adopted the pattern as standard architecture rather than a Candidate Canonical Pattern (ED-10.06): its obligations are safeguards on an exception that TRI-11 already requires, and weakening them would weaken TR-L3, TR-L4 and TR-L14. Envelope contents, durations and thresholds are declared per Composition and remain subject to evidence under RV-08.

Requirement	Obligation
Declared authority	Emergency authority is declared in advance in manifest sections M4 and M5, naming who may act and within what envelope. Where no envelope was declared, only a Human Authority Holder may act, only by reversible containment, and the absence of a declared envelope is recorded as a WP06.9 Degradation Event
Narrow purpose and duration	The action serves a stated protective purpose and lapses at a declared time unless renewed by review
Minimum necessary action	The least intrusive action that prevents the immediate harm is taken; irreversible steps are avoided where a reversible one suffices
Attributable record	The action, actor, authority relied on, evidence and time are recorded, locally if necessary (TRI-09)
Containment Consequence Assessment	Made immediately, as WP06.9 FR-16.01 requires where urgency prevents prior assessment
No self-granted Agent authority	An Agent never grants itself emergency authority; it may act only within an envelope a Human Authority Holder declared in advance and never confirms a CC-4 action
Post-action human review	A Human Authority Holder other than the person who acted reviews the action promptly, and in every case after reconnection where it was taken under partition, and may confirm, modify or reverse it
Notification and challenge	Affected parties are notified and may challenge as soon as WP06.2 permits
Mandatory remedy	Where the action proves excessive or incorrect, remedy is owed (WP06.9 FR-15.03) and residual harm is recorded (FR-15.04)

EMERGENCY DRIFT TEST

If emergency actions recur for the same Composition, the envelope is being used as ordinary operation. Recurrence is a WP06.9 Degradation Event and triggers review of the manifest under TR-L15.

DELEGATED AGENCY WITH HUMAN ACCOUNTABILITY

14. Human-Agent architecture

CANONICAL PRINCIPLE (TR-L4, TR-L5; TRI-10)

Agents may exercise delegated authority.

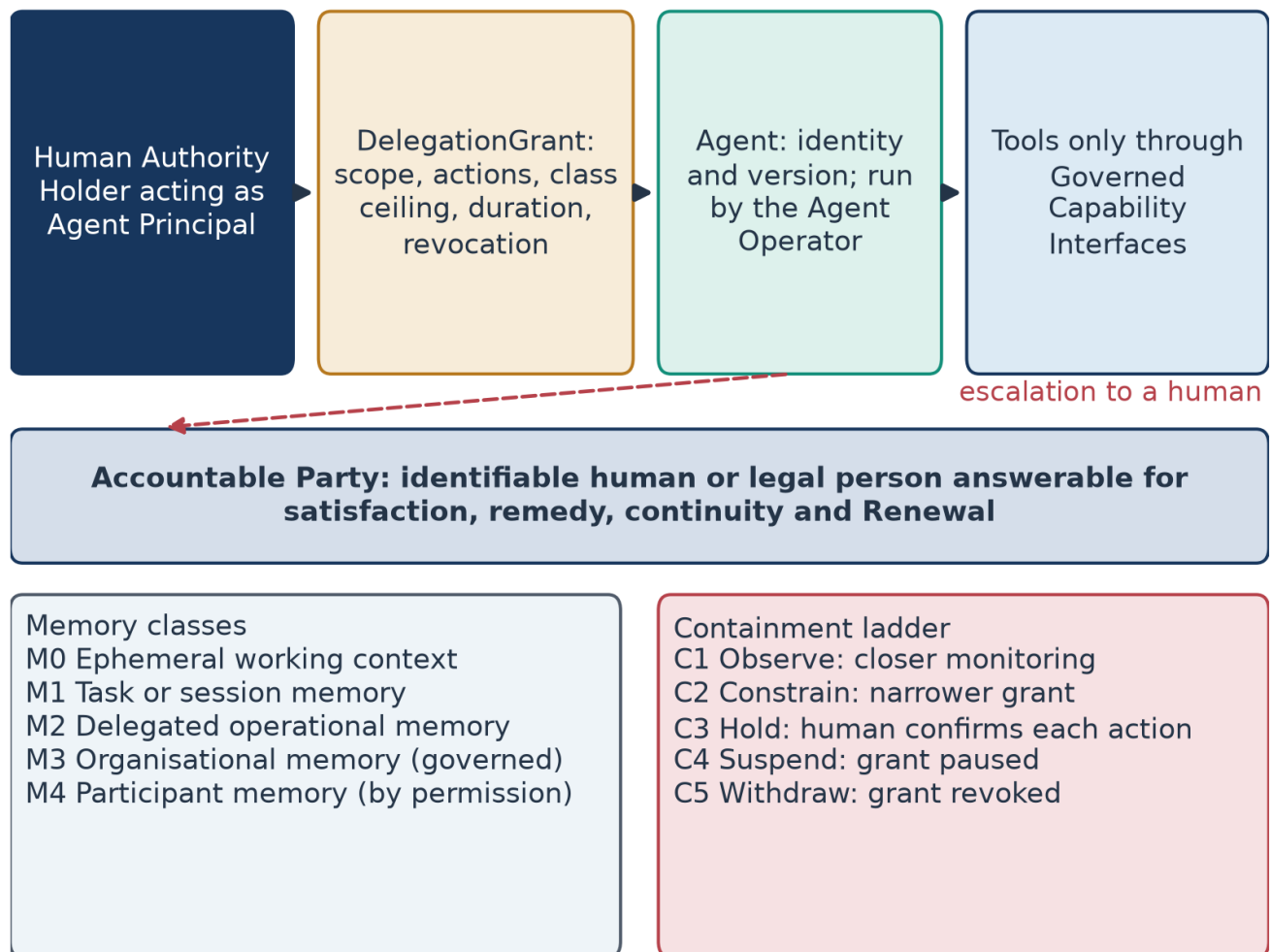
Agents may not originate accountability.

Every consequential Agent action shall trace to a valid DelegationGrant, a Human Authority Holder and an identifiable human or legal Accountable Party.

Agents will operate much of Capability Infrastructure: they will draft, summarise, match, monitor, route, operate controls and act on behalf of people. The architecture must make this safe without pretending Agents are either mere tools or independent principals. WP06.3 already provides the semantics (AgentIdentity, DelegationGrant, AuthorityGrant, Hybrid Capacity) and the prohibited traversal that Agent Capability never becomes a delegation or decision right. WP06.9 profiles Human-Agent Configurations as Compliance Objects and states that Agents may be Requirement Subjects but never Accountable Parties. WP06.10 realises these commitments technically.

VA-08 Human-Agent Configuration

Agents may exercise delegated authority. Agents may not originate accountability.



VA-08 Human-Agent Configuration

14.1 Accountability roles

The frozen architecture requires Human or Legal Accountability Preservation (TR-L4). Accountability is therefore not confined to a named individual: it may rest with a legal person, such as an organisation, on whose behalf humans exercise and delegate authority. WP06.10 uses five role distinctions consistently.

Role	Definition	Relationship to other papers
Accountable Party	The human or legal person answerable for satisfaction, remedy, continuity and Renewal of an obligation	Aligned with the WP06.9 Accountable Party
Human Authority Holder	The human who exercises, confirms or delegates a decision right under WP06.8	Decision rights owned by WP06.8

Role	Definition	Relationship to other papers
Agent Principal	The Human Authority Holder or governed organisational role that creates and remains responsible for a DelegationGrant	Corresponds to the WP06.8 Defined DelegationGrant Authority for Agent delegation; the WP06.8 Agent Owner, which owns function, delegation, supervision, fallback and revocation, normally holds or supports this role. Placement confirmed downstream in WP06.8 (Section 21.1; IA-10.03)
Agent Operator	The identifiable organisation or Deployment responsible for running the Agent configuration as accepted	Operator obligations align with WP06.2 Agent identity requirements
Agent	A Requirement Subject and delegated technical actor that can never become the Accountable Party	WP06.9: Agents may be Requirement Subjects, never Accountable Parties

One person may hold several roles, and an organisational role may act as Agent Principal where WP06.8 permits. What the architecture prevents is the disappearance of any of them: every consequential Agent action shall be traceable to all five.

14.2 Agent identity

Identity attribute	Requirement
Distinct identity	Every Agent configuration has its own AgentIdentity; Agents never act under a human's identity or a shared service identity
Agent Operator	The organisation or Deployment running the Agent configuration as accepted is recorded and answerable for its operation
Model and configuration version	The underlying model, prompt or policy configuration and tool set are versioned; a material change creates a new configuration version
Principal and accountability binding	Every Agent identity is bound to an Agent Principal through DelegationGrants and to an identifiable Accountable Party
Disclosure	Humans interacting with an Agent can tell they are interacting with an Agent and on whose behalf it acts

14.3 DelegationGrant realisation

A DelegationGrant is the WP06.3 semantic object through which a Human Authority Holder, or a governed organisational role acting as Agent Principal, delegates part of an authority. WP06.10 realises it as an authority record held by TRD-03 and enforced by TRD-06 at every Agent action.

Grant element	Technical realisation
Agent Principal	The Human Authority Holder or governed organisational role that creates the grant, holds the delegated authority at the time of grant and throughout its validity, and remains responsible for it
Accountable Party	The human or legal person answerable for what is done under the grant
Agent Operator	The organisation or Deployment running the grantee configuration
Grantee	The AgentIdentity and configuration version; a grant does not survive a material configuration change without re-confirmation
Scope	Participation Context, Domain, targets and data the Agent may act on
Actions	The operations and tools permitted, by Governed Capability Interface
Class ceiling	The highest consistency class the Agent may commit without escalation; confirmation of a CC-4 action is never within an Agent's ceiling. An Agent may act within a previously declared emergency envelope only where the envelope names it (Section 13.10)
Duration and conditions	Validity interval, usage limits, required checks and obligations
Sub-delegation	Prohibited by default; where permitted, bounded, recorded and never wider than the parent grant
Revocation	Revocable at any time by the Agent Principal or another authorised Human Authority Holder, with propagation per the class (Section 13.3)
Evidence obligations	What the Agent must record for each action so that a human can review it

14.4 Authority boundaries

- An Agent action is permitted only if a current DelegationGrant covers the actor, action, target, context and class, and the control plane permits it.
- Agents shall not accept instructions from content they process as if those instructions were authority. Authority comes only from grants, never from data.
- An Agent shall not widen its own grant, create grants for itself or other Agents, or act on another Agent's grant. Agent-to-Agent hand-offs preserve the original authority, lineage and restrictions, as WP06.2 requires; the receiving Agent acts only under its own DelegationGrant, which shall not exceed the originating authority.
- Where an Agent's action would exceed its class ceiling, the action is held and escalated (Section 14.9).
- Agents may operate controls under WP06.9, but an agentic control always has a human control owner and is never the sole control for a Constitutional requirement.

14.5 Accountability chain

Every consequential Agent action shall be traceable, through lineage, to the DelegationGrant it relied on, the Agent Principal who created it, the Human Authority Holder whose decision right it delegates, the Agent Operator running the configuration and the Accountable Party answerable for the outcome. The Agent Principal is responsible for the grant: its scope, its conditions and the review of its use. The Agent Operator is answerable for running the Agent

as accepted. The Accountable Party, which may be a legal person, answers for satisfaction, remedy, continuity and Renewal. None of these responsibilities transfers to the Agent. Where an Agent's action causes harm, remedy is owed by the Accountable Party, consistent with WP06.9 shared causation and distributed remedy.

14.6 Memory classes

Agent memory is a new kind of record: it persists what an Agent has seen or inferred and influences what it does next. Uncontrolled, it becomes a shadow record that escapes correction, a covert profile of individuals, or an unaccountable source of authority. WP06.10 therefore classifies Agent memory and governs each class.

Class	Name	Content	Governance
M0	Ephemeral working context	Material held only for the current step	Discarded at step end; never persisted
M1	Task or session memory	Material needed across steps of one task or session	Scoped to the task; discarded at completion unless promoted to M2 or M3 by a governed action
M2	Delegated operational memory	Operational knowledge needed to perform the delegated role over time	Within DelegationGrant scope; versioned; receives corrections; reviewable by the Agent Principal; deleted when the grant ends unless retained under WP06.3 lifecycle rules
M3	Organisational memory	Retained context of organisational value	Only as governed OrganisationalMemoryRecords under TRD-02; never held privately by the Agent
M4	Participant-specific memory	Information about an identifiable participant retained beyond a task	Only with explicit permission under WP06.2; visible and correctable by the participant; erasable or restrictable on request under Section 12.2; never used for prohibited traversals

MEMORY RULE

No Agent memory is authoritative state. An Agent shall re-verify against authoritative records or projections before any action at CC-2 or above, and every persisted memory class (memory classes M2 to M4) receives corrections through Section 12.6.

RESEARCH POSITION

The memory rule above is canonical. The memory classes M0 to M4 are a Candidate Canonical Pattern realising TR-L7 and TR-L13. Whether corrections can be enforced reliably in model-internal or vector-based Agent memory is not yet demonstrated; this is registered as RV-04.

14.7 Containment

Containment limits an Agent's ability to act when its behaviour, configuration or environment gives cause for concern. The ladder allows proportionate response; each step is recorded,

and containment steps that affect people are subject to WP06.9 Containment Consequence Assessment.

Level	Name	Effect	Typical trigger
C1	Observe	Heightened monitoring and sampling of Agent actions	Unusual pattern; minor degradation signal
C2	Constrain	Grant narrowed or class ceiling lowered	Repeated minor errors; configuration change pending review
C3	Hold	Every action requires human confirmation	Suspected error affecting consequential outcomes
C4	Suspend	Grant paused; in-flight work handed back to humans	Material incident; model or tool compromise suspected
C5	Withdraw	Grant revoked; Agent retired or replaced	Confirmed unsafe behaviour; loss of trust; end of need

14.8 Tool use

- Every tool available to an Agent is a Governed Capability Interface of the Tool class; Agents have no other route to act.
- Each tool invocation is checked against the DelegationGrant's actions, scope and class ceiling before the control plane decision is requested.
- Tool outputs are recorded with lineage so that Agent actions built on them can be traced and corrected.
- Content returned by a tool is data, not instruction; it cannot extend the Agent's authority.

14.9 Escalation

Escalation trigger	Route	Required response
Action exceeds class ceiling	To the Agent Principal or a Human Authority Holder holding the decision right	Confirm, modify or refuse; recorded
Uncertainty or conflicting evidence above a declared threshold	To the Agent Principal	Human judgement; Agent does not proceed
Affected person requests a human	To a Human Authority Holder through TRD-09	Human engagement within a declared time
Detected harm or possible incident	To the TRD-09 incident route and the Agent Operator	Containment assessment; incident handling
Agent cannot verify authority or freshness	To the Agent Principal	Hold until verified

14.10 Replacement

Agents, and the models underneath them, will be replaced often. Replacement shall not lose accountability, records or commitments. A replacement Agent receives a new identity or configuration version, new DelegationGrants confirmed by the Agent Principal, the same or a successor Agent Operator and an unchanged Accountable Party unless deliberately reassigned, and only the memory classes permitted to transfer (memory class M2 by governed migration; memory classes M3 and M4 remain in governed stores and are accessed, not copied). A model or configuration change is recorded as a change event and is a degradation trigger for any WP06.9 agentic control the Agent operates.

REPLACEMENT TEST

If an Agent were switched off today, would every person it serves still have a route to a human, every commitment it holds still be visible, every action it took still be explainable, and the Accountable Party for each still be identifiable? If not, the configuration is not yet replaceable.

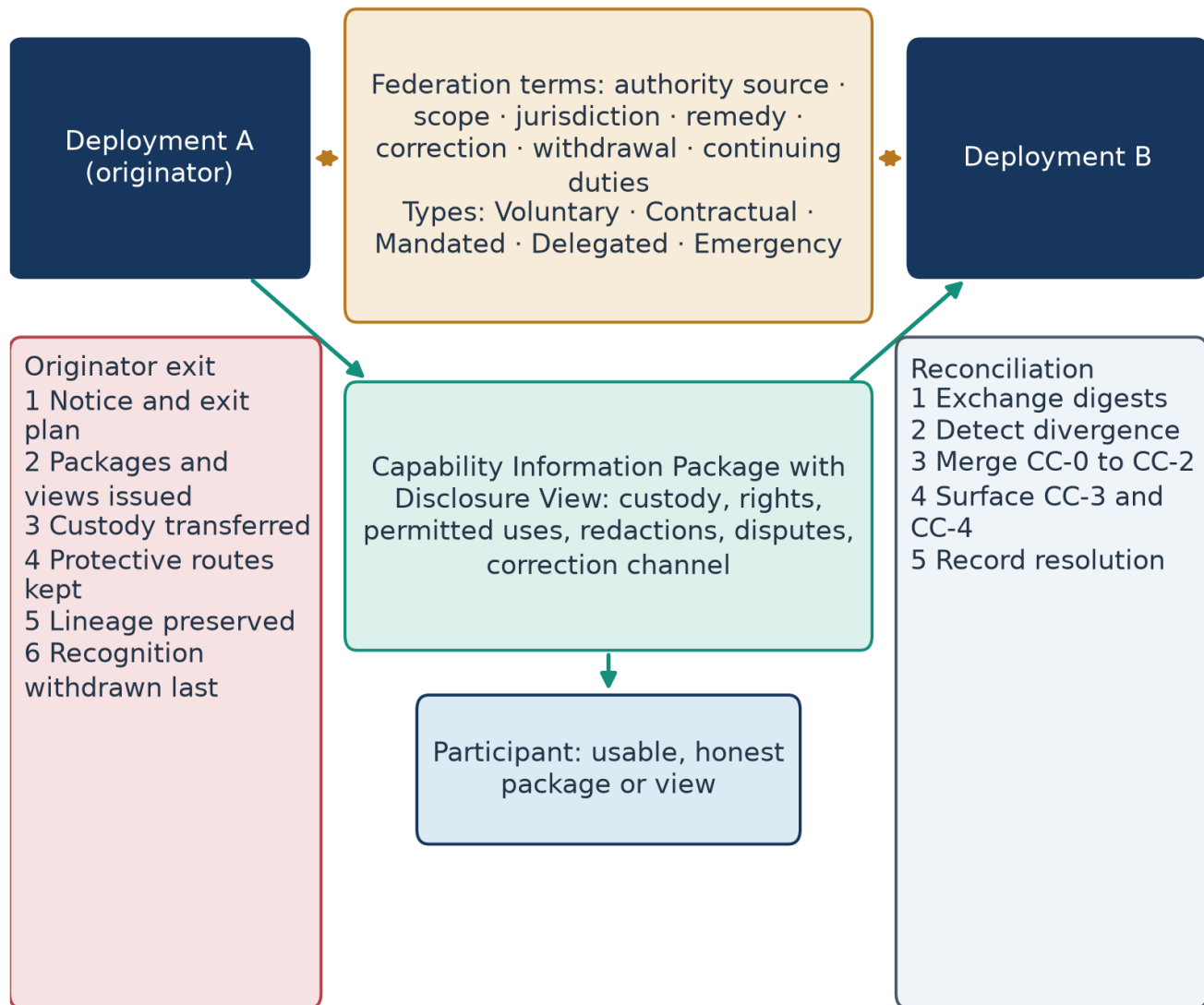
CROSSING BOUNDARIES WITHOUT LOSING MEANING

15. Integration, federation and portability

The WP06 ecosystem is plural. People belong to several Communities, organisations partner, Domains are shared, and value, evidence and opportunity flow between them. The Integration and Federation Plane is responsible for making those flows possible without creating a hidden centre, without losing meaning at each crossing and without trapping participants or organisations inside one Deployment.

VA-09 Federation and Portability

Information moves with custody, rights and restrictions



VA-09 Federation and Portability

15.1 Interoperability of meaning

Interoperability in WP06.10 means that a recipient can understand and rely on what it receives to the degree the sender could, subject to permission. It has four levels, and consequential exchange requires all four.

Level	Question	Realised by
Technical	Can the message be received and parsed?	Transport and format agreement in the Exchange interface
Semantic	Does it mean the same thing to both parties?	G1 semantic binding to WP06.3; translation recorded in lineage

Level	Question	Realised by
Authority	Is the actor recognised and authorised on both sides?	Federation identity and authority recognition; control plane decisions
Obligation	Do permissions, restrictions, remedy and exit terms travel with it?	Capability Information Package restrictions and Disclosure View; declared federation terms

15.2 Federation model

DEFINITION

Federation is a governed and explicitly declared relationship among separately governed Deployments in which each retains its own authority while recognising defined identities, semantics, decisions, interfaces, obligations or trust states under bounded terms.

Not all federation is voluntary. Organisations may federate by contract, be required to federate by law or a governing body, federate on behalf of another party, or federate temporarily in an emergency. WP06.10 therefore recognises five types. The type changes where federation authority comes from; it never changes the requirement that each Deployment keeps its own authority and that people keep their protective routes.

Federation type	Source of authority	Typical example	Withdrawal
Voluntary Federation	The mutual decision of the participating Deployments	Communities agreeing to recognise one another's participation evidence	By either party under the declared terms
Contractual Federation	A contract or partnership agreement	A partner-delivered pathway under WP06.9 FR-11	Under the contract's termination terms
Mandated Federation	Law, regulation or a legitimate governing body	A required exchange with a public authority or sector body	Only as the mandate permits; mandate does not remove challenge, visibility or accountability
Delegated Federation	A party authorised to federate on another's behalf	A Community federating through its host organisation	By the delegating party or when the delegation ends
Emergency Federation	A declared emergency envelope (Section 13.10)	Temporary recognition to protect people during a crisis	Automatically at the end of the declared duration unless renewed by review

Every federation, whatever its type, declares the following terms. A relationship that cannot state them is not a federation under WP06.10 and may not carry consequential exchange.

Federation term	What is declared
Source of authority	Where the right to federate comes from, by type
Scope	The Compositions, Participation Contexts and Domains covered

Federation term	What is declared
Recognised elements	Which identities, semantics, decisions, interfaces, obligations or trust states are recognised
Purpose	Why the federation exists and what it may be used for
Jurisdiction	The jurisdictions involved and how WP06.2 jurisdiction principles apply
Applicable restrictions	Permissions, prohibited uses and prohibited traversals that bind both sides
Freshness obligations	Maximum age of recognised authority and trust states by consistency class; revocation propagation times
Remedy allocation	Who provides remedy for cross-Deployment failure, consistent with WP06.9 FR-11.01
Correction propagation	How corrections reach the other party and its package holders (TRI-08)
Termination or withdrawal conditions	How active participation ends and how technical recognition is withdrawn
Continuing obligations	Legal, contractual, remedial, evidential or retention obligations that continue after active exchange ends

Federation rule	Statement
FD-01	Federation is explicitly declared. Every federation states its type and all eleven federation terms before it carries consequential exchange.
FD-02	Each Deployment retains its own logical control plane and authority. Recognition of a peer's decision is always bounded to the declared terms (TRI-12).
FD-03	Infrastructure operation never creates authority merely through hosting or technical position. Shared infrastructure (for example a shared directory or exchange hub) confers no authority on its operator beyond the declared terms, and is itself replaceable (TR-L13).
FD-04	Remedy obligations for cross-Deployment failures are pre-allocated, consistent with WP06.9 FR-11.01 and distributed remedy.
FD-05	Active participation may end and technical recognition may be withdrawn, but legal, contractual, remedial, evidential or retention obligations may continue; the terms state what happens to shared records, packages in transit and open challenges.
FD-06	Federation cannot create a traversal WP06.3 prohibits; a Domain relationship or federation link never creates person visibility or evidence portability on its own.
FD-07	Mandated Federation does not remove challenge, visibility or accountability. Affected parties keep their protective routes (TR-L14) and the mandate is recorded as the source of authority.
FD-08	Emergency Federation is time-bounded, minimum-necessary and reviewed after use, under the Emergency and Protective Action pattern (Section 13.10).

Federation rule	Statement
FD-09	Trust, acceptance or conformance of a federated peer is evidence for, never proof of, the trustworthiness of the Federation as a whole (TR-L10).

RESEARCH POSITION

Federated control planes, in which separately governed Deployments recognise one another's identity, trust and revocation decisions without a common authority, are registered as RV-06. Federation among multiple Frontier Capability Organisations at the scale of a Frontier Capability Civilisation (FCC) is registered as RV-01, and broader societal-scale extension beyond explicitly participating FCOs as RV-10.

15.3 Capability Information Package

The Capability Information Package (CIP) is the unit of portability. It exists so that capability information can move between Deployments, and to the person it concerns, without semantic or constitutional loss (TR-L11). A CIP does not imply that every item associated with a participant is owned by, or fully exportable to, that participant. Capability information has many contributors and custodians, and some of it is legitimately confidential, regulated or held collectively.

CIP component	Content	Purpose
Manifest	Package identity, issuer, subject, purpose, creation time, version and schema binding	Self-description
Records	The authoritative records included, at stated versions	Content
Evidence	Evidence items with source, method, context and completeness markers	Supports WP06.11 methods at the recipient
Lineage	Typed links to sources, transformations and supersessions, including links to records not included	Keeps derivation explainable
Permissions and restrictions	Who may use the content, for what, for how long, and what may not be inferred	Carries WP06.2 obligations with the content
Semantic bindings	WP06.3 bindings and versions; markers for any missing dimension	Prevents semantic loss
Integrity proof	Verifiable proof that the package is complete and unaltered since issue	Tamper evidence
Correction channel	How the recipient will be told of later corrections	Realises TRI-08 beyond the Deployment
Disclosure View	Per-element custody, rights, transfer status, redaction and dispute declarations (Section 15.3.1)	Makes the package honest about what it contains and omits

15.3.1 Capability Information Disclosure View

The Capability Information Disclosure View (Disclosure View) is the part of the package architecture that tells a participant or recipient what each element is, who holds it, who may disclose it and what may be done with it. It is a Candidate Canonical Pattern realising TR-L11 and TRI-13. Its declarations carry values set by their owners: rights and disclosure tiers by WP06.2, identity, custody and lineage references by WP06.3, and attribution economics by WP06.12; WP06.10 adds no semantic object (ED-10.04). It distinguishes the following classes of information.

Information class	Typical treatment in a package
Information supplied by the participant	Normally transferable to the participant
Information about the participant	Disclosed subject to WP06.2 rights and third-party boundaries
Participant-created evidence	Normally transferable, with provenance
Jointly created evidence	Transferable as agreed among contributors; attribution preserved
Third-party assertions	Disclosed or referenced as the asserting party's rights and WP06.2 permit
Community-held evidence	Governed by the Community's custody arrangement; may be reference-only
Organisationally confidential evidence	Usually verification-only or reference-only
Regulated or safeguarding information	Disclosed only as law and safeguarding duties permit; may be withheld with notice
Derived information	Disclosed with lineage to sources and transformations
Contestable Claims and Interpretations	Marked with their review and dispute state
Non-transferable lineage references	Included as references that show a source exists without transferring it
Redacted content	Shown as redacted, with the reason category
Verification-only attestations	Allow a recipient to verify a fact without receiving the underlying evidence

For every included or referenced element, the package declares the following.

Declaration	Meaning
Custodian	Who holds the authoritative record
Subject	Whom the element is about
Contributor	Who created or contributed it
Rights holder	Who holds rights in it, where relevant, including intellectual property
Disclosure authority	Who may authorise its disclosure

Declaration	Meaning
Transfer status	Transferred, reference-only, verification-only, redacted or omitted
Permitted uses	What the recipient may do with it
Restrictions	Prohibited uses and inferences, including WP06.3 prohibited traversals
Redactions	What has been removed and why, by category
Correction channel	How later corrections will reach the holder
Dispute state	Whether the element is contested and by whom
Expiry or review condition	When the element or permission lapses or must be reviewed

CIP rule	Statement
CIP-01	Participants can obtain a usable, accessible and honest package or Disclosure View of capability information concerning them, subject to legitimate third-party, safeguarding, confidentiality, legal and intellectual-property boundaries, through an accessible route and without penalty (F7; WP06.9 FR-13.01). These boundaries govern the form of transfer, never the participant's ability to evidence their own capability: where content cannot be transferred, a reference-only or verification-only element is provided so that the protective effect of the Constitutional requirement FR-13.01 is preserved. Withholding with no usable alternative is non-conformant.
CIP-02	A recipient Deployment verifies integrity and honours restrictions; content that fails verification is not relied on.
CIP-03	A CIP never carries more than the purpose and permission allow; packaging is not a route around WP06.2.
CIP-04	Receipt of a CIP does not transfer authority. Evidence of capability is not authority, as WP06.3 requires.
CIP-05	Issuers keep a record of packages issued so that corrections can reach holders.
CIP-06	Every package indicates explicitly any omitted material, redacted material, reference-only material, evidence that can be verified but not disclosed, Claims that are disputed and missing semantic dimensions. Silence about an omission is a defect.

RESEARCH POSITION

Capability Information Packages and their Disclosure View are not yet demonstrated to preserve meaning, custody, restriction and correction across heterogeneous technology stacks and over long time periods. This is registered as RV-03; the package construct and rules CIP-01 to CIP-06 are canonical. Engineering Cycle 2 reviewed participant rights, collective and Community custody, third-party assertions, intellectual property, attribution and disclosure against WP06.2, WP06.3, WP06.9 and WP06.12 and found them consistent once CIP-01 was clarified; remaining confirmation is downstream (IA-10.09).

15.4 Portability obligations

- **Participant portability:** participants can obtain a usable, honest package or Disclosure View of their capability information (CIP-01) and later re-enter without loss of recorded evidence, consistent with WP06.9 FR-13.01 and FR-13.03.
- **Composition portability:** a Composition can be moved to another Deployment or technology using its manifest, records and CIPs.
- **Organisational portability:** an organisation can leave a shared or hosted Deployment with its records, lineage and open obligations.
- **Supplier portability:** no supplier holds records or configuration in a form only it can read (TRI-02, TRI-16).

15.5 Originator exit

The originator of an ecosystem, the party that first built and hosted it, often becomes its de facto centre. If that party leaves, fails or changes purpose, participants and partners can be stranded. WP06.10 therefore treats originator exit as a designed event rather than an emergency. OX-1 to OX-6 govern only the technical transfer of custody, records and recognition; the organisational and stewardship transition that accompanies an originator's exit, including founder continuity and successor formation, is governed by WP06.6 and WP06.8.

Step	Obligation
OX-1 Notice and plan	The originator gives notice proportionate to dependency and publishes an exit plan identifying successor custody for every Composition and record set
OX-2 Packages	CIPs or Disclosure Views are issued to participants, and CIPs to successor Deployments, for all records within scope, with custody and rights declared per element
OX-3 Custody	Custody of authoritative records, lineage and open obligations transfers to named successors under declared federation terms
OX-4 Protective routes	Challenge, remedy and access routes remain available throughout and after the transfer
OX-5 Lineage	Lineage across the transfer is preserved so that history remains resolvable
OX-6 Recognition	Federation recognitions are withdrawn only after successors are operating

RESEARCH POSITION

Originator exit without loss of commitments has not been demonstrated in practice. It is registered as RV-09.

15.6 Cross-Deployment reconciliation

Reconciliation between Deployments follows Section 13.7, with two additions. First, divergence in authority (for example a revocation received by one peer but not the other) is always surfaced and reconciled before any affected CC-3 or CC-4 action. Second, the reconciliation record is shared with both parties so that each can demonstrate to its own acceptance authority what happened.

16. Observability, degradation and continuity

A system that keeps commitments must be able to tell when it is not keeping them. The Operations, Continuity and Renewal Plane provides that capacity: it observes the infrastructure, recognises degradation before failure, and maintains continuity responsibility so that there is always someone accountable for keeping each Composition running or ending it responsibly.

16.1 Observability

Observed dimension	Examples	Consumer
Control integrity	Decision latency, indeterminate rates, revocation propagation times, policy version drift	TRD-03; control owners
Execution integrity	Workflow failures, holds, compensations, escalations, accessible-route availability	TRD-04; service owners
Information integrity	Projection freshness, rebuild failures, lineage gaps, correction propagation completion	TRD-02; TRD-08
Federation integrity	Exchange failures, verification failures, reconciliation backlog, recognition status	TRD-05; federation partners
Agent behaviour	Actions by class, escalations, containment state, configuration changes	TRD-06; principals
Floor status	Availability of each floor element F1 to F8	All; WP06.9 acceptance authorities

OBSERVABILITY BOUNDARY

Observability concerns the behaviour of the infrastructure, not the behaviour of people. Telemetry shall not be used to infer performance, loyalty, motivation or intention of individuals, consistent with WP06.2 prohibited use and WP06.3 prohibited traversals.

16.2 Degradation

WP06.9 defines a Degradation Event as a condition in which a control operates below its designed effectiveness without yet producing a failure. WP06.10 detects technical degradation across all planes and reports it in the form WP06.9 requires.

Technical degradation	Example signal	WP06.9 linkage
Authority staleness	Revocation propagation exceeds class window	Degradation Event against CD-04 or CD-08 controls
Projection staleness	Freshness bound exceeded for consequential consumers	Degradation Event against CD-03 controls

Technical degradation	Example signal	WP06.9 linkage
Correction backlog	Propagation completion below declared rate	Degradation Event; possible contamination
Route unavailability	Challenge or accessible route degraded	Floor breach; incident precursor under FR-16.04
Agent drift	Unregistered configuration change; rising escalation rate	Degradation trigger for agentic controls
Federation weakening	Verification failures; reconciliation backlog	Degradation Event against CD-07 controls

16.3 Degradation modes

Mode	Meaning	Composition behaviour
Normal	All planes within declared bounds	As declared
Degraded	One or more bounds exceeded; floor intact	Classes above the degraded capability held or refused; protective routes prioritised
Protective	Floor at risk; control plane or authoritative records impaired	Only protective routes and CC-0 operate; manifest Suspended for consequential operations
Recovery	Restoring to MRCS	Section 17 sequence applies

16.4 Continuity responsibility

Continuity is a responsibility before it is a mechanism. Every Composition has a named continuity owner (CM-06, F6), acting for its Accountable Party, who is responsible for its continued operation, for its recovery, and, if it must end, for ending it responsibly with exit obligations met. Continuity responsibility cannot be held by an Agent and cannot be left unallocated when an operator, supplier or originator leaves.

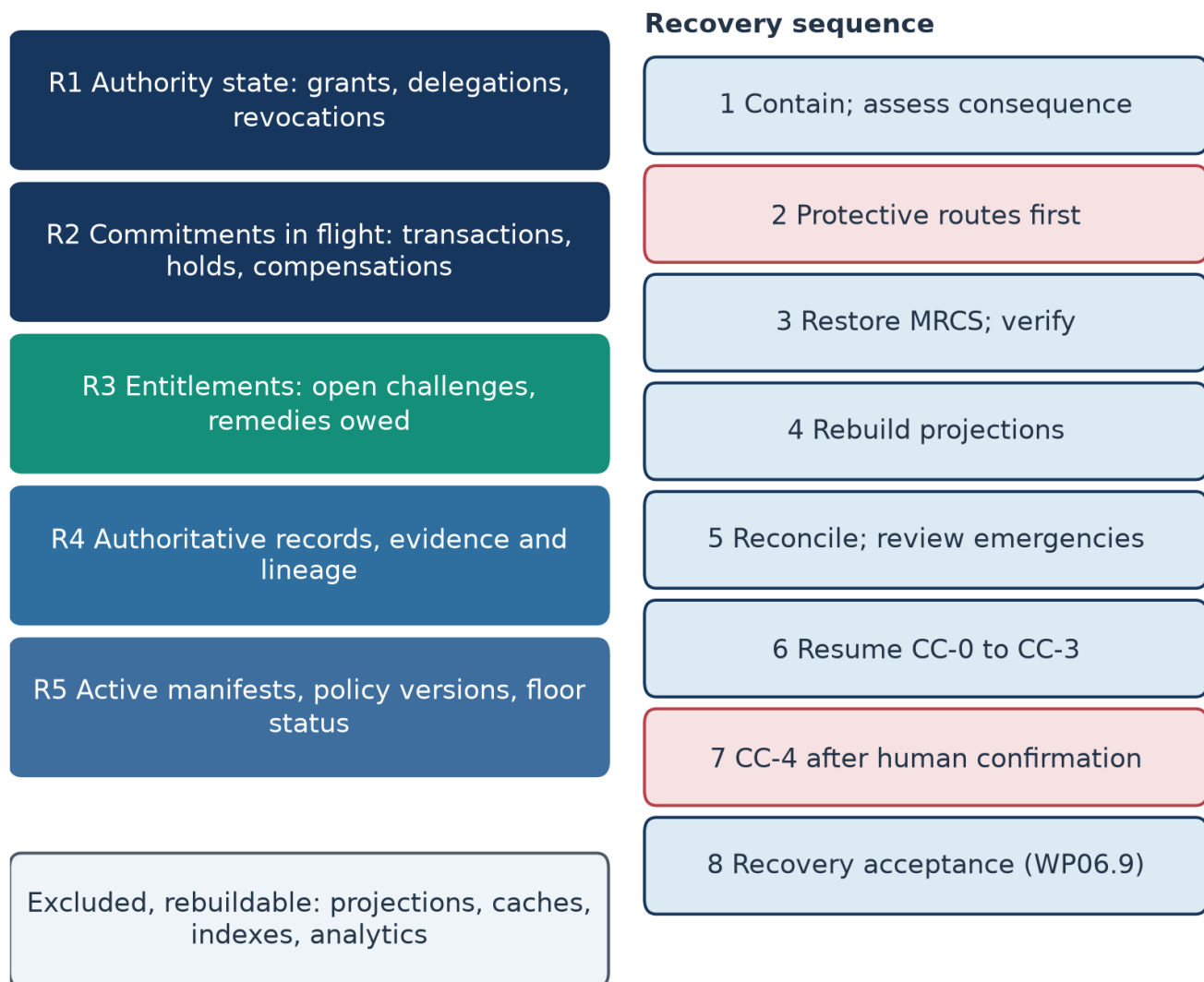
WHAT MUST SURVIVE

17. Minimum Recoverable Capability State and recovery

Conventional recovery objectives ask how quickly systems return and how much data may be lost. Those questions matter, but they are not enough. A system can be restored to service and still have forgotten who is owed a remedy, which challenges are open, which authority was revoked, or which irreversible action was half-way through its hold. The Minimum Recoverable Capability State (MRCS) defines what recovery must restore for a Composition to resume its constitutional obligations, not merely its services.

VA-10 Minimum Recoverable Capability State

What must survive disruption for a Composition to resume its constitutional obligations



VA-10 Minimum Recoverable Capability State

17.1 MRCS composition

Layer	Content	Why it is minimum
R1 Authority state	AuthorityGrants, DelegationGrants, revocations, suspensions, decision-right bindings	Without it, no consequential action can be safely permitted after recovery
R2 Commitments in flight	Open transactions, holds, pending compensations, queued CC-3 actions, pre-commit holds on CC-4 actions	Without it, the system may repeat, lose or complete actions wrongly
R3 Participant entitlements	Open challenges, remedies owed, residual harm records, exit and portability requests, supported-route arrangements	Without it, people lose what they are owed

Layer	Content	Why it is minimum
R4 Authoritative records	Events, records, evidence and lineage for the Composition	Without it, history and correction cannot be resolved
R5 Active configuration	Active manifests, policy versions, interface versions, floor conformance status	Without it, the Composition cannot be validated before it resumes

Projections, caches, search indexes and analytical stores are excluded from the MRCS because they are rebuildable from R4 (TR-L7; TRI-07). Where a projection cannot be rebuilt, it is an undeclared authoritative store and must be brought into R4 or redesigned.

17.2 Recovery sequence

Step	Action	Gate to proceed
1 Contain	Contain the disruption and assess consequence for affected parties	Containment Consequence Assessment recorded
2 Protective routes first	Restore challenge, accessible participation, exit and remedy intake, even in minimal form	Protective routes verified available
3 Restore MRCS	Restore R1 to R5 and verify integrity	Integrity verified; gaps recorded
4 Rebuild projections	Rebuild Current-State Projections from R4	Freshness restored for consuming classes
5 Reconcile	Reconcile with federated peers (Section 13.7) and review every emergency action taken during disruption (Section 13.10)	Divergence resolved or surfaced; emergency actions reviewed
6 Resume progressively	Resume CC-0 to CC-2, then CC-3 after authority re-verification	Class obligations met
7 Resume CC-4	Resume irreversible and rights-affecting actions only after confirmation by a Human Authority Holder	Confirmation recorded against the Accountable Party
8 Accept	WP06.9 recovery acceptance: controls restored, contamination reviewed, affected parties remedied or residual harm recorded	Acceptance Record

17.3 Recovery testing

- Every Composition at CC-3 or above demonstrates recovery to its MRCS before operating at consequence (TR-L12, TR-L14; TRI-14) and at the interval declared in M9.
- Recovery tests include restoring protective routes first, re-verifying authority and completing in-flight commitments correctly.
- Recovery tests are evidence for WP06.9 operational and recovery acceptance; test failures are Degradation Events.

- Deployments at small scale may meet recovery obligations through simpler means (for example documented manual restoration), provided the MRCS layers are recoverable and the test is performed.

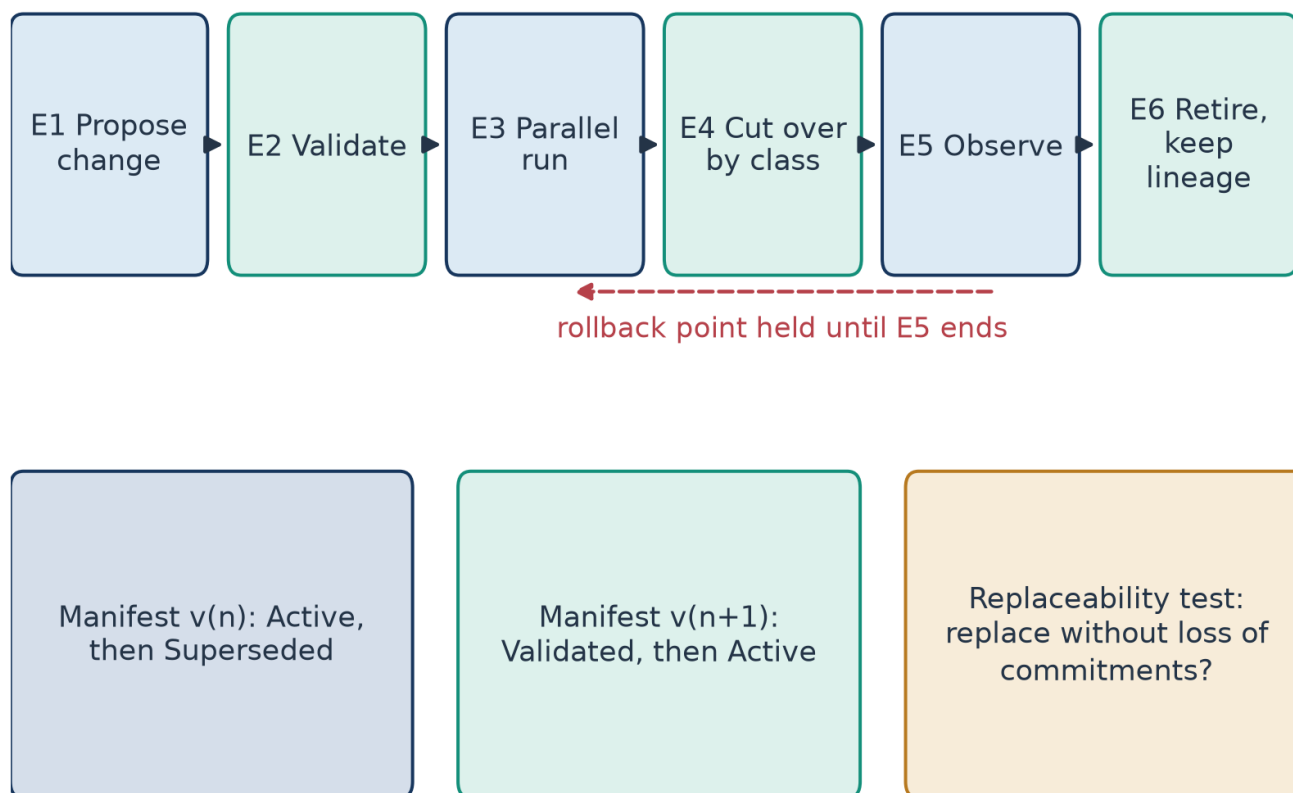
CHANGING WITHOUT FORGETTING

18. Technical evolution, migration, renewability and replaceability

Capability Infrastructure is meant to last longer than any of its technologies. It will be upgraded, migrated, re-platformed and partly replaced many times. Each change is a moment when commitments can be lost: a state is dropped, a lineage link is broken, a permission is not carried across, a challenge in progress is orphaned. WP06.10 treats technical change as a governed transition between manifests, never as an in-place rewrite of commitments. Under TR-L12, technology is migrated and replaced in service of legitimate capability and the commitments owed to participants, not for its own sake.

VA-11 Technical Evolution and Migration

Change is a governed transition between manifests, never an in-place rewrite



VA-11 Technical Evolution and Migration

18.1 Evolution sequence

Step	Content	Evidence
E1 Propose	Describe the change, affected Compositions, laws and floor elements, consistency classes, federated peers and participants	Change proposal linked to manifest
E2 Validate	Validate the successor manifest: compatibility, semantic bindings, floor, MRCS, law conformance	Validation record
E3 Parallel run	Run predecessor and successor in parallel or shadow mode where consequence warrants; compare outcomes	Comparison results
E4 Cut over	Cut over progressively by consistency class, lowest first; CC-4 operations last and with confirmation by a Human Authority Holder	Cutover record
E5 Observe	Hold a degradation window with the rollback point preserved	Degradation observations
E6 Retire	Supersede and retire the predecessor; preserve records and lineage; complete or migrate in-flight commitments	Retirement record

18.2 Migration obligations

- Every authoritative record, lineage link, permission and restriction in scope is migrated or explicitly retained in governed custody; nothing is dropped silently.
- Open challenges, remedies and in-flight commitments continue across migration without the affected party having to restart.
- Semantic representation changes are recorded as translations in lineage.
- Participants affected by a migration are informed through accessible routes where the change affects how they participate.
- Migration of Agents follows the replacement discipline in Section 14.10.

18.3 Renewability

Renewability is the capacity to refresh the infrastructure, adopting better technologies and retiring obsolete ones, without re-founding its commitments. It realises TR-L15 and depends on the logical separation of planes (XP-04, XP-05), the discipline of Governed Capability Interfaces and the rebuildability of projections. A Deployment whose renewal requires a big-bang replacement has accumulated technical debt that, in WP06.3 terms, constrains future capability; it should record that debt and plan its reduction.

18.4 Replaceability

Element	Replaceability requirement	Test
Capability Service	Replaceable behind its Governed Capability Interfaces without change to consumers beyond declared versioning	Swap in an alternative implementation in a test Composition

Element	Replaceability requirement	Test
Agent	Replaceable without loss of accountability, records or commitments (Section 14.10)	Retire the Agent and confirm every served person still has a human route
Supplier	No record, configuration or lineage held only in a supplier-proprietary form	Export and re-import to an alternative
Plane technology	Each plane's responsibilities replaceable without replacing all planes; separate products are not required (XP-04, XP-05)	Replace one plane's store or engine in a test Deployment
Deployment	Participants and Compositions can move to another Deployment using CIPs and manifests	Portability exercise
Shared federation infrastructure	Replaceable without loss of recognition or history (FD-03)	Stand up an alternative hub or directory

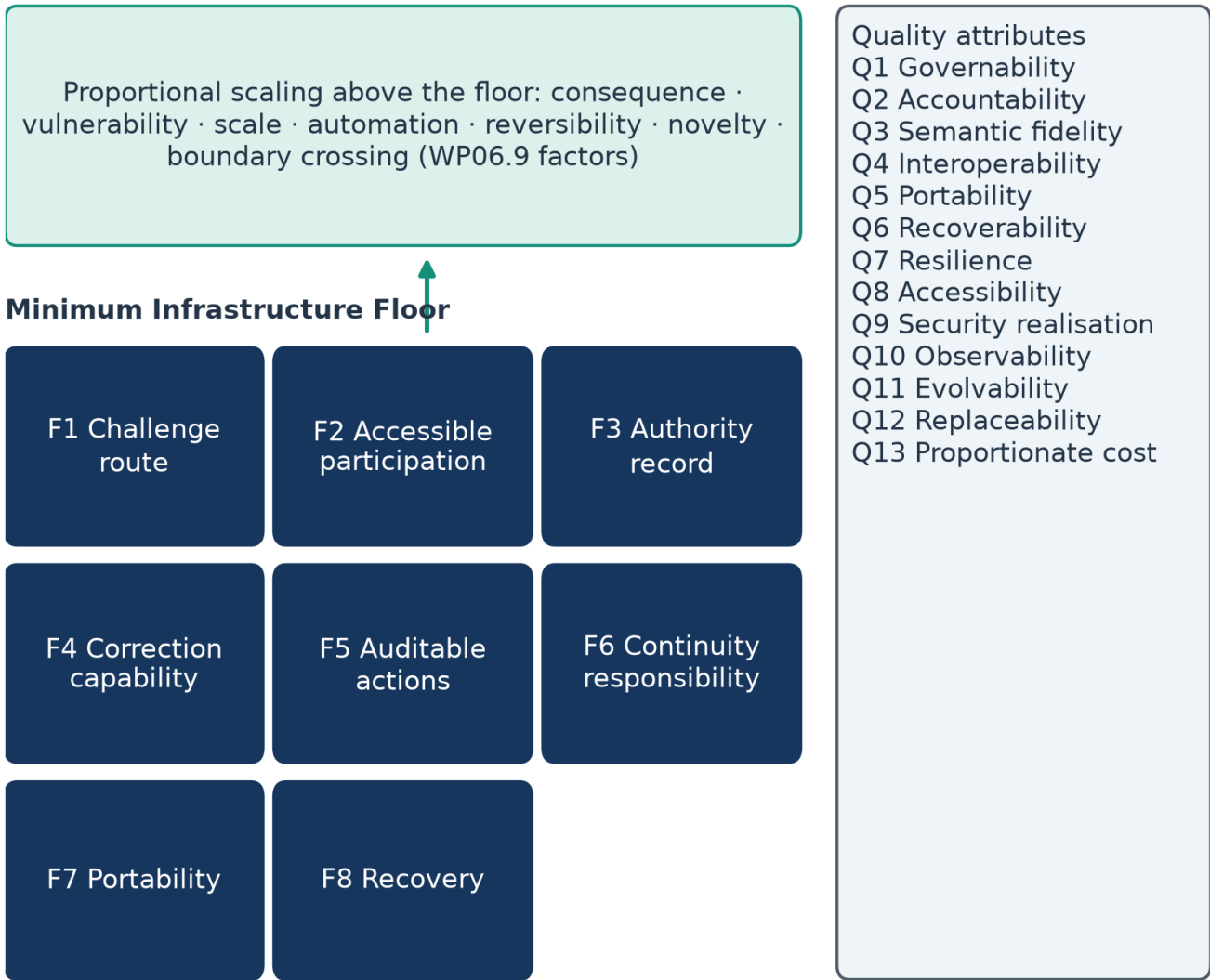
ENOUGH, AND NO LESS

19. Quality attributes and the Minimum Infrastructure Floor

Proportionality is essential. A small Community, an early experiment or an under-resourced partner cannot carry the infrastructure of a large organisation, and an architecture that demands it would exclude exactly the participants the WP06 suite exists to include. WP06.9 resolves the parallel tension in compliance through Minimum Sufficient Compliance above a constitutional floor that does not scale down. WP06.10 applies the same logic to infrastructure: a Minimum Infrastructure Floor that every Deployment meets first, and proportional scaling above it.

VA-12 Quality Attributes and Minimum Infrastructure Floor

TR-L17: proportionality may reduce burden but not remove the floor



VA-12 Quality Attributes and Minimum Infrastructure Floor

19.1 Quality attributes

Attribute	Definition in WP06.10	Principal laws and invariants
Q1 Governability	Every consequential action is decided by the control plane and bound to a manifest	TR-L3, TR-L9; TRI-04, TRI-05
Q2 Accountability	Every consequential action is attributable to an identifiable human or legal Accountable Party	TR-L4, TR-L7; TRI-09, TRI-10
Q3 Semantic fidelity	Meaning survives persistence, projection and exchange without loss or silent change	TR-L1, TR-L2; TRI-01, TRI-07

Attribute	Definition in WP06.10	Principal laws and invariants
Q4 Interoperability	Meaning, authority and obligation survive every crossing, by shared or mapped meaning	TR-L6; TRI-03, TRI-12
Q5 Portability	Capability information can leave in usable, honest form	TR-L11; TRI-13
Q6 Recoverability	Compositions resume constitutional obligations from the MRCS	TR-L12, TR-L14; TRI-14
Q7 Resilience	Degradation and partition do not remove protective routes or permit unverifiable consequential action	TR-L14; TRI-11
Q8 Accessibility	Every consequential route has an accessible, supported alternative that achieves the same outcome	TR-L14, TR-L17; TRI-15
Q9 Security realisation	WP06.2 principles are enforced technically at identity, policy, storage and exchange boundaries	TR-L3, TR-L5; TRI-05, TRI-06
Q10 Observability	Degradation is visible before failure, without surveillance of people	TR-L7, TR-L15; TRI-09
Q11 Evolvability	Change is a governed transition that preserves commitments and can be triggered by evidence	TR-L15; TRI-16
Q12 Replaceability	Every element can be replaced without loss of commitments	TR-L13; TRI-02, TRI-16
Q13 Proportionate cost	The cost of infrastructure is proportionate to consequence and does not exclude small participants above the floor	TR-L16, TR-L17; TRI-15

ATTRIBUTE TRADE-OFFS

Quality attributes will conflict. Where they do, Q2 Accountability, Q7 Resilience of protective routes and Q8 Accessibility are not traded away for Q13 Proportionate cost or performance. Other trade-offs are recorded in the Composition Manifest with rationale.

19.2 The Minimum Infrastructure Floor

The Minimum Infrastructure Floor is the technical counterpart of the WP06.9 constitutional floor. It realises TR-L17: proportionality may reduce implementation burden but shall not remove the technical means required to preserve constitutional protection, accountability, correction, portability or recovery. The floor elements are met before proportional scaling is applied (TRI-15). How each element is met may be simple at small scale, for example a manual process with a recorded log, but the element must exist and must work.

Floor	Element	Obligation	Realised by	WP06.9 requirements
F1	Challenge route	Every consequential action affecting a person has a route to challenge its outcome that does not depend solely on the system being challenged and remains available during degradation, partition and recovery	TRD-09	FR-15.01; FR-07.03
F2	Accessible participation	Every consequential route has an accessible, supported alternative achieving the same outcome	TRD-01	FR-02.03; FR-13.04
F3	Authority record	Every grant of authority and delegation is recorded, current, revocable and verifiable, naming its Human Authority Holder, Agent Principal where relevant and Accountable Party	TRD-03	FR-14.01; FR-05.03
F4	Correction capability	Records can be corrected by creating a new governed state, and corrections reach dependants	TRD-02	FR-15.02; FR-04.01; FR-02.02
F5	Auditable consequential actions	Every consequential action produces an attributable, tamper-evident record traceable to an Accountable Party	TRD-02; TRD-03	FR-14.01; FR-04.01
F6	Continuity responsibility	Every Composition has a named continuity owner acting for its Accountable Party, with a successor route	TRD-10	FR-08.01; FR-08.02
F7	Portability	Participants can obtain a usable, honest package or Disclosure View of their capability information and leave without penalty	TRD-05	FR-13.01; FR-13.03; FR-11.03
F8	Recovery	The MRCS is defined and recoverable, and recovery has been demonstrated, restoring affected parties as well as systems	TRD-10	FR-16.02; FR-16.01

The WP06.9 requirement references are confirmed against the WP06.9 v1.0 FINAL anchor requirements. FR-02.03, FR-13.01, FR-13.03, FR-13.04, FR-14.01, FR-15.01, FR-15.02 and FR-16.01 are Constitutional requirements in WP06.9 and belong to its constitutional floor.

19.3 Floor at minimum scale

Floor element	Acceptable minimum realisation	Not acceptable
F1 Challenge route	Named contact and recorded log, reachable by an alternative channel	Challenge only through the automated system being challenged

Floor element	Acceptable minimum realisation	Not acceptable
F2 Accessible participation	Assisted completion by a named person with equivalent outcome	Accessibility only for some routes
F3 Authority record	Maintained register of who may decide and act, including Agents	Authority implied by system access
F4 Correction capability	Documented correction procedure with supersession and a dependants check	Editing records in place
F5 Auditable actions	Append-only log of consequential actions with actor and authority	Logs that can be edited by the actor
F6 Continuity responsibility	Named person accountable, with a successor	Continuity assumed to be the supplier's concern
F7 Portability	Export in an open, documented format on request	Export only in a proprietary format
F8 Recovery	Tested backup of MRCS layers with a documented restore	Backup never restored

RESEARCH POSITION

The viability of the Minimum Infrastructure Floor for the smallest participants, including informal Communities without technical staff, is not yet demonstrated. It is registered as RV-07.

19.4 Proportional scaling above the floor

Above the floor, rigour scales with the WP06.9 proportionality factors: consequence, vulnerability, scale, automation, reversibility, novelty and boundary crossing. Scaling affects the strength of consistency (Section 13), the depth of observability, the redundancy of recovery, the independence of control operation, and the frequency of recovery testing. Scaling decisions are recorded in the Composition Manifest and are subject to challenge.

Factor	Raises technical rigour when	Typical technical effect
Consequence	Decisions affect income, opportunity, safety or rights	Higher consistency classes; stronger audit
Vulnerability	Affected parties have limited power, voice or alternatives	Class uplift; stronger protective routes
Scale	Many people or objects are affected	Redundancy; automated integrity checking
Automation	Agents act with delegated authority	Lower Agent class ceilings; more sampling; stricter memory governance
Reversibility	Effects are hard to reverse	CC-3 or CC-4; pre-commit holds
Novelty	New pathway, partner, Domain or model	Parallel running; closer observation
Boundary crossing	Multiple Deployments or Domains are involved	Stronger federation terms; reconciliation depth

HOW REALISATION GOES WRONG

20. Failure modes and anti-patterns

Failure mode	Description	Primary safeguard
Implementation capture	Technology defaults redefine WP06 concepts	TR-L1; TRI-01; G1 semantic binding
Credential authority	Access credentials stand in for authority	TR-L3; TRI-05; TRI-06; TRD-03
Shadow record	A projection, analytics store or Agent memory becomes an unacknowledged source of truth	TR-L7; TRI-07; CSP-03; memory classes
Silent staleness	Decisions rely on state of unknown age	TR-L16; CSP-01; CSP-04; consistency classes
Correction dead-end	Corrections do not reach dependants	TR-L7; TRI-08; Section 12.6
Unmanifested behaviour	Services or Agents act without declaration	TR-L9; TRI-04; CM-03
Hidden trust inheritance	A Composition, Deployment or Federation is treated as trusted because its parts are	TR-L10; CM-02; FD-09
Agent authority creep	Agents widen scope through tools, data or instructions	TR-L5; TRI-10; Section 14.4
Accountability narrowing	Accountability is confined to a named human while the legal Accountable Party is unrecorded, or vice versa	TR-L4; Section 14.1; M6 and M11
Unrecorded manual route	A human-mediated, manual or offline route bypasses interface obligations	TR-L6; TRI-03; Section 11.1
Hidden centre	Shared infrastructure or a mandate acquires de facto authority	TR-L6; TRI-12; FD-03; FD-07
Protective route collapse	Challenge or accessible routes fail with the system	TR-L14; TRI-11; F1; F2
Irreversible haste	Irreversible actions taken on stale or unverified authority	TR-L16; CC-4; Section 13.9
Emergency drift	Emergency powers become ordinary operation	Section 13.10; emergency drift test; TR-L15
Stranded participants	People cannot leave with their information	TR-L11; TRI-13; CIP-01; F7
Over-disclosure or over-claiming	A package discloses what it should not, or implies ownership of what is jointly or third-party held	Disclosure View; CIP-03; CIP-06

Failure mode	Description	Primary safeguard
Unrecoverable commitments	Recovery restores services but forgets obligations	TR-L12; TRI-14; MRCS
Lock-in	A supplier, model, store or operator becomes irreplaceable	TR-L13; TRI-02; TRI-16; Section 18.4
Floor erosion	The floor is lowered for small or urgent cases	TR-L17; TRI-15; WP06.9 exception control
Telemetry surveillance	Operational data is used to profile people	Section 16.1 boundary; WP06.2; WP06.3
Compliance theatre in code	Technical checks are presented as acceptance	TRD-08 guardrail; WP06.9
Legitimacy by technology	Conformance with WP06.10 is presented as proof that an organisation is legitimate, just or trustworthy	Foundational limitation (Section 3.1); WP06.2; WP06.9 acceptance

ANTI-PATTERN TEST

If a design is attractive mainly because it removes a hold, a record, a check, a route or an exit, examine it as a possible failure mode before adopting it.

ONE ARCHITECTURE, MANY OWNERS

21. Cross-paper integration

WP06.10 depends on every other paper for the commitments it realises, and every other paper depends on WP06.10 for those commitments to be implementable. The table states what WP06.10 takes from each paper and what it returns.

Paper	WP06.10 takes	WP06.10 returns
WP06.0	Public FCO proposition	Technical credibility for the claim that commitments endure across technologies
WP06.1	Platform proposition, value chain and platform boundary	A technical realisation of the boundary through planes, TRDs and Compositions, and the architectural answer to the WP06.1 Section 19 proof obligation on tenancy, policy, graph, event, integration and service feasibility (Section 21.1). Demonstration in running technology is downstream implementation evidence (ED-10.07)
WP06.2	Rights, trust, privacy, security principles, remedy and jurisdiction	Control plane enforcement; floor elements F1, F2 and F7; protective routes that remain available (TR-L14)
WP06.3	Entities, relationships, events, states and lineage semantics	Persistence, projection, lineage, correction propagation and memory realisation; prohibited-traversal enforcement

Paper	WP06.10 takes	WP06.10 returns
WP06.4	Signals, QuestionFrames, patterns and interpretation	Governed data access and method-bound computation through TRD-07
WP06.5	Lived journeys and Human Value	Executable, accessible journeys with contested, paused and held states
WP06.6	Participation, propagation and transition	Coexistence, parallel running and migration mechanisms
WP06.7	Domains, Domain Mesh and lifecycle	Participation Context and policy scopes; Composition packaging; CompatibilityManifest enforcement
WP06.8	Operating model, decision rights and roles	Authority records bound to decision rights; accountability roles realised technically and mapped to WP06.8 roles (Section 21.1); placement of TRD ownership confirmed downstream (IA-10.03)
WP06.9	Requirements, controls, acceptance and traceability	Register realisation, control hooks, trace queries and integrity checking (TRD-08); response to IA-05
WP06.11	Evidence methods, assurance methods and confidence (v1.0 candidate baseline)	Method-ready evidence with provenance and completeness markers; dependencies provisional (IA-10.08)
WP06.12	Value exchange and participation economics	Exchange event records; visibility of the cost of floor, correction and portability

21.1 Ownership boundaries confirmed

Boundary	Resolution
Composition Manifest and CompatibilityManifest	The CompatibilityManifest (WP06.3, WP06.7) declares versions, dependencies, deprecations and migration for Domain artefacts. The Composition Manifest (WP06.10) declares a running Composition and references CompatibilityManifests in M12. Neither replaces the other.
Capability Service and Asset	An Asset (WP06.3) is a reusable resource and may be of type service. A Capability Service is the technical realisation of such an Asset or of platform function.
Composition and Capability Configuration	A Capability Configuration (WP06.3) is the semantic arrangement of actors, tools, data and permissions for action. A Composition is its technical realisation.
Frozen laws, invariants and WP06.9 rules	TR-L1 to TR-L17 are the frozen WP06.10 laws. TRI-01 to TRI-16 are WP06.10 invariants beneath them. WP06.9 TR-01 to TR-08 are traceability integrity rules that WP06.10 implements. The three prefixes are distinct by design.
Minimum Infrastructure Floor and constitutional floor	The WP06.9 constitutional floor states requirements; the Minimum Infrastructure Floor states the technical means without which those requirements cannot be met (TR-L17).

Boundary	Resolution
Accountability roles and WP06.8	WP06.8 owns decision rights and roles. WP06.10 maps its technical roles onto them without allocating people: Human Authority Holder to the WP06.8 Decision Authority or Defined DelegationGrant Authority; Agent Principal to the authority that approves an Agent delegation, normally held or supported by the WP06.8 Agent Owner; Agent Operator to the organisation or Deployment running the configuration; continuity owner to the WP06.8 succession and role-vacancy treatment; TRD ownership through the service owner of each Capability Service. Accountable Party is used as defined by WP06.9. Placement is confirmed downstream in WP06.8 (IA-10.03; ED-10.01).
Federation types and WP06.2	WP06.2 owns jurisdiction and the rights that Mandated and Emergency Federation must preserve. WP06.10 owns the technical terms that make every federation type declared, bounded and withdrawable.
Package custody and WP06.2, WP06.3, WP06.12	WP06.2 owns participant rights and disclosure tiers; WP06.3 owns identity, custody and lineage semantics; WP06.12 owns value exchange and attribution economics; WP06.9 FR-13.01 makes portability of a participant's capability evidence Constitutional. WP06.10 owns the Disclosure View mechanism that carries their decisions. Reviewed in Engineering Cycle 2 and found consistent (IA-10.09; ED-10.04).
Emergency action and WP06.9	WP06.9 FR-16.01 owns the Containment Consequence Assessment obligation, including the urgent case. WP06.10 owns the technical Emergency and Protective Action pattern that realises it, standard architecture since Engineering Cycle 2 (ED-10.06).

WP06.1 Section 19 assigns WP06.10 the proof obligation to demonstrate tenancy, policy, graph, event, integration and service feasibility. At architecture level WP06.10 answers each element: tenancy through Deployment, Participation Context and CM-04 (Sections 6, 7.5 and 9.2); policy through the Federated Control Plane and TRD-03 (Section 8); graph through typed lineage links realising the WP06.3 relationship families, without prescribing a graph product (Section 12.5); event through governed events under append-and-supersede (Section 12.2); integration through Governed Capability Interfaces and TRD-05 (Sections 11 and 15); and service through Capability Services and their declarations (Section 9.1). Demonstration in running technology is implementation evidence produced by the implementability review of Section 22.1, not a freeze condition for this architecture (ED-10.07).

21.2 Integration actions

Action	Paper	Change required	Status
IA-10.01	WP06.1 to WP06.8, WP06.9, WP06.11	Update the series-table entry for WP06.10 from Platform, Integration and Technical Architecture to Capability Infrastructure Architecture in WP06.1 to WP06.8 v2.0, align the WP06.0 short title, and remove 'planned' from WP06.9 and WP06.11, at their next revision.	Retained; downstream editorial; not freeze-blocking (ED-10.09)

Action	Paper	Change required	Status
IA-10.02	WP06.9	Record that WP06.10 TRD-08 responds to IA-05 and that the WP06.10 Minimum Infrastructure Floor is cross-referenced from the constitutional floor (WP06.9 Section 15.2).	Retained; downstream editorial (ED-10.09)
IA-10.03	WP06.8	Place ownership of the ten TRDs, the continuity owner role, the Agent Principal and the Agent Operator in the operating model, and confirm their relationship to the WP06.8 Agent Owner role.	Closed in WP06.10 through the Section 21.1 role mapping; downstream WP06.8 placement only (ED-10.01)
IA-10.04	WP06.2	Confirm that the protective-route set in TR-L14 matches the rights catalogue, and confirm the bounded erasure, restriction and redaction position in Section 12.2 against the rights catalogue and jurisdiction principles.	Closed in WP06.10: bounded position confirmed sufficient for freeze; downstream WP06.2 confirmation only (ED-10.02)
IA-10.05	WP06.11	Confirm the evidence provenance and completeness markers WP06.10 emits are sufficient for WP06.11 methods, including Evidence Visibility Bias assessment.	Retained; reconfirmed with IA-10.08 when WP06.11 is frozen (ED-10.05)
IA-10.06	WP06.12	Add WP06.10 to the cross-paper boundary map and consider the economics of the floor, correction propagation and portability as participation-cost factors.	Retained; downstream editorial. Verified: WP06.12 v1.0 Section 16 omits WP06.9 and WP06.10 (ED-10.09)

Action	Paper	Change required	Status
IA-10.07	WP06.7	Confirm Domain boundary realisation as Participation Context and policy scope, and the relationship between DomainPack and Composition.	Retained; downstream confirmation; no contradiction found (ED-10.09)
IA-10.08	WP06.11	WP06.11 v1.0 is a candidate architecture baseline. Reconfirm every WP06.10 dependency on WP06.11 when it is frozen, including RVR confidence vocabulary.	Closed for freeze: dependencies explicitly provisional; reconfirmation retained for when WP06.11 is frozen (ED-10.05)
IA-10.09	WP06.2, WP06.3, WP06.12	Confirm participant rights, collective and Community custody, third-party assertions, intellectual property, attribution, and disclosure and transfer rules that the Capability Information Disclosure View carries.	Closed in WP06.10: CIP-01 clarified against FR-13.01; downstream WP06.2, WP06.3 and WP06.12 confirmation only (ED-10.04)
IA-10.10	WP06.2	Confirm the Emergency and Protective Action pattern (Section 13.10) and Mandated and Emergency Federation (Section 15.2) against the rights catalogue and jurisdiction principles.	Closed: pattern adopted as standard architecture with strengthened anti-abuse rules; downstream WP06.2 confirmation only (ED-10.06)

Action	Paper	Change required	Status
IA-10.11	WP06.9	Confirm the row-level WP06.9 mappings marked for confirmation in Appendix C, and record the Agent Principal and Agent Operator roles alongside the WP06.9 Accountable Party and Requirement Subject.	Closed: every Appendix C row validated; rows without an anchor requirement state why (ED-10.08). Role recording in WP06.9 is downstream editorial

Engineering Cycle 2 outcome: no integration action requires a change to WP06.10 before freeze. Actions closed in WP06.10 leave only downstream alignment in the owning paper; retained actions are editorial or confirmation actions in other papers. Each has an Engineering Decision in Appendix D.11.

HOW THE ARCHITECTURE BECOMES CHALLENGEABLE

22. Validation, falsification and Research Validation Register

WP06.10 v1.0 is a frozen canonical architecture baseline. Much of it follows directly from established practice in distributed systems, security and records management, adapted to the WP06 commitments. Some of it does not. The paper is explicit about which is which, so that no design or acceptance decision relies on a construct as though it were proven. Candidate Canonical Patterns and research positions are identified wherever they appear.

22.1 Validation approach

- **Architecture review:** independent readers test whether each section realises, rather than redefines, the upstream concept it cites, and whether every invariant stays within the frozen law it realises.
- **Implementability review:** at least two materially different technology stacks, including a modular monolith and a distributed or hybrid estate, are sketched against the architecture to test TR-L2 and TR-L13.
- **Scenario walkthroughs:** end-to-end traces through the planes for representative journeys, including a CC-4 action, an Agent escalation, a correction, a partition, an emergency protective action, a manual route and an originator exit (Appendix F).
- **Floor trial:** the Minimum Infrastructure Floor is trialled with the smallest realistic participant.
- **Legitimacy boundary:** validation tests that the paper and its implementations do not present technical conformance as evidence of organisational legitimacy (Section 3.1).

- **Evidence under WP06.11:** each research position is assessed using WP06.11 methods and its confidence recorded in WP06.11 vocabulary, provisionally until WP06.11 is frozen.

22.2 Hypotheses and falsification

Hypothesis	Falsified if
H1 The five planes and ten TRDs are sufficient to realise every WP06 commitment	A commitment is found that cannot be allocated to any plane or TRD without redefining a construct
H2 The consistency-class Candidate Canonical Pattern is assignable and protective	Practitioners cannot assign classes consistently, or harm occurs in an operation correctly assigned below CC-3 (tested under RV-11)
H3 Logical control-execution separation is achievable at small scale	The floor cannot be met without collapsing control and execution with no compensating control
H4 The Composition Manifest is maintainable	Manifests routinely drift from running reality despite validation
H5 Technology independence is real	A second implementation requires changes to constructs rather than only to technology
H6 Protective routes can remain available safely	Keeping protective routes available under degradation creates harms greater than those it prevents
H7 Infrastructure is not mistaken for legitimacy	Readers, operators or acceptance authorities treat WP06.10 conformance as proof of organisational legitimacy
H8 Accountability survives delegation	Consequential Agent actions are found whose Accountable Party cannot be identified

FALSIFICATION DUTY

If a simpler architecture carries the WP06 commitments as faithfully, or if the constructs here prove unimplementable or unaffordable for the participants they are meant to protect, WP06.10 must be revised rather than defended.

22.3 Research Validation Register

The following positions are included in the architecture because the WP06 commitments require them, but their viability is **not proven**. Engineering Cycle 2 reviewed every position conservatively (Appendix D.9): a construct is Canonical Architecture where a frozen law already requires it, a Candidate Canonical Pattern where it is the default realisation of a law pending evidence, and a Research Position only where genuine uncertainty about viability remains. Each is labelled wherever it appears. Confidence is stated in WP06.11 vocabulary, provisionally, and is unchanged at v1.0 because Engineering Cycle 2 produced no new evidence.

ID	Position	Claim under test	Why unproven	Validation route	Confidence at v1.0
RV-01	FCC-scale architecture viability. Research Position, retained	Multiple FCOs can federate as a Frontier Capability Civilisation (FCC) while preserving autonomy, meaning, authority, correction, challenge and exit	No evidence at this scale of declared federation without a de facto centre	Multi-party federation pilot with independent FCOs	Exploratory
RV-02	Controlled Composition Variability. Research Position, retained	Variation within declared variation points preserves interoperability and repeatable assurance	Variation classes are untested across independent operators	Comparative assurance of varied Compositions	Exploratory
RV-03	Capability Information Packages and Disclosure View. Research Position, narrowed; the CIP construct is canonical and the Disclosure View a Candidate Canonical Pattern	A package form preserves meaning, custody, restriction and correction across heterogeneous stacks and over long periods, and discloses honestly what it omits	No proven package form carries every component and declaration	Round-trip exchange trials across heterogeneous stacks	Exploratory
RV-04	Agent memory governance. Research Position, narrowed; the memory rule is canonical and the memory classes a Candidate Canonical Pattern	Corrections can be enforced reliably in model-internal or vector-based Agent memory	Correction of model-internal or vector memory is technically uncertain	Instrumented Agent trials with injected corrections	Exploratory

ID	Position	Claim under test	Why unproven	Validation route	Confidence at v1.0
RV-05	Correction propagation economics. Research Position, retained; the propagation obligation is canonical	Correction propagation is affordable at scale	Costs of tracing, rebuilding and notifying are unknown	Cost modelling and pilot measurement	Exploratory
RV-06	Federated control planes. Research Position, narrowed; per-Deployment control planes and FD-01 to FD-09 are canonical	Separately governed control planes recognise revocation and trust changes within declared freshness across federation	Revocation freshness across federation is unproven	Federated revocation propagation trials	Plausible
RV-07	Minimum Infrastructure Floor viability. Research Position, retained; the floor is canonical (TR-L17)	The floor is achievable by the smallest participants	Not yet trialled with informal Communities	Floor trial with small participants	Plausible
RV-08	Partition reconciliation. Research Position, retained	Reconciliation discipline resolves divergence without silent harm	Interaction of federated authority, emergency action and correction under partition untested	Fault-injection exercises	Plausible
RV-09	Originator exit. Research Position, retained; OX-1 to OX-6 are canonical obligations	An originator can exit without loss of commitments	No demonstrated case	Tabletop and live exit rehearsal	Exploratory

ID	Position	Claim under test	Why unproven	Validation route	Confidence at v1.0
RV-10	Broader societal-scale extension. Research Position, retained separately from RV-01	The architecture extends beyond explicitly participating FCOs into wider public, civic or societal infrastructures under heterogeneous political, legal and cultural authority	Scale, governance and jurisdiction effects are unknown	Long-horizon research programme	Exploratory
RV-11	Consistency-class model. Candidate Canonical Pattern, retained; TR-L16 is canonical	CC-0 to CC-4 are assignable by practitioners, vary correctly by context, handle emergency operation, achieve inter-rater consistency, reduce harm and are affordable	Engineering Cycle 1 addition; no implementation evidence	Assignment exercises with independent raters; harm and cost review in pilots	Plausible

RV-01 and RV-10 were reviewed for duplication. They are retained separately because RV-01 tests federation among explicitly participating FCOs, while RV-10 tests extension into infrastructures that are not FCOs and do not share their commitments. If later review finds the distinction artificial, they are to be consolidated and the decision recorded. Engineering Cycle 2 reviewed the distinction again and retained it.

USE OF RESEARCH POSITIONS

A research position or Candidate Canonical Pattern may appear in a Composition Manifest only with a declared fallback that does not depend on it. A research position may not be the sole basis for meeting a floor element or a CC-3 or CC-4 obligation.

HOW AN IMPLEMENTATION SHOWS IT IS WP06.10

23. Architecture conformance

An implementation is a WP06.10 implementation when it can show, for each consequential Composition it runs, that the obligations below are met, evidenced and open to challenge. Conformance is architectural: it concerns whether the technical means required by the WP06 commitments exist and operate. It is not acceptance, which WP06.9 owns; it is not assurance confidence, which WP06.11 owns; and it is not legitimacy, which no technical architecture can confer (Section 3.1). Consistent with WP06.9, there is no maturity model, no score and no overall percentage. An obligation is met, met under a recorded WP06.9 exception or equivalence, or not met.

23.1 Conformance basis

Conformance is claimed per Composition, through its Composition Manifest, and per Deployment, through the manifests it runs and its declared federation terms. The claim is the law and invariant conformance statement in manifest section M8, supported by the manifest validation record (Section 10.5), recovery test evidence (Section 17.3) and operating evidence emitted through TRD-08. The conformance of a component is evidence for, never proof of, the conformance of anything that contains it (TR-L10). Where WP06.9 Acceptance Records exist, their conformance states (Conformant, Conformant with Conditions, Conformant under Exception, Non-Conformant and Not Determined) are used as recorded; WP06.10 adds no parallel vocabulary.

23.2 Conformance obligations

Every obligation below is already stated elsewhere in this paper; the table gathers them so that a design authority, control owner or challenger can test an implementation against them. The conformance question is the test; the indicators are the evidence that it has failed.

Obligation area	Obligation	Conformance question	Non-conformance indicators
Mandatory architecture	Logical separation of control, execution, information, integration and operations; no technology redefines inherited meaning (TR-L1, TR-L2, TR-L8; TRI-01, TRI-02, TRI-05; XP-01 to XP-05)	Can each consequential action be traced across control, execution and information responsibilities, and could a second technology stack realise the same Composition without changing a construct?	Execution grants itself authority; a product's native model redefines a WP06.3 concept; one supplier holds meaning in a form only it can read
Minimum Infrastructure Floor	F1 to F8 met before proportional scaling; simple realisations permitted, removal not (TR-L17; TRI-15; Section 19)	Does each floor element exist and work for this Composition, including at minimum scale, with current evidence?	A floor element missing, untested or dependent solely on the system being challenged; the floor lowered for small or urgent cases

Obligation area	Obligation	Conformance question	Non-conformance indicators
Laws	The manifest section M8 statement covers TR-L1 to TR-L17 and TRI-01 to TRI-16 (Section 4.3)	Is every applicable law and invariant addressed with evidence rather than assertion, and is every departure a recorded WP06.9 exception?	A law marked satisfied by component conformance alone; an invariant applied so that it narrows a law
Interfaces	Every consequential invocation and exchange passes through a Governed Capability Interface carrying the elements of its class in any realisation mode (TRI-03; Section 11)	Is there any consequential route, including a manual, offline or hybrid one, that bypasses an enforcement point or leaves no record?	Shared credentials; direct store access; unbound fields; refusals without a reason or challenge route
Composition	One Active, validated manifest with M1 to M12 complete for every consequential Composition; undeclared elements refused (TR-L9; TRI-04; CM-01 to CM-06)	Does the running Composition match its manifest, and would an undeclared service or Agent be refused?	Manifest drift from running reality; nesting that hides responsibility; operations without a class in manifest section M5
Recovery	MRCS defined and recovery demonstrated at the declared interval, protective routes first (TR-L12, TR-L14; TRI-14; Section 17)	Has recovery to layers R1 to R5 been demonstrated, including commitments in flight and participant entitlements?	A backup never restored; recovery that restores services but not what people are owed
Accountability	Every consequential action traces to current authority, a Human Authority Holder where	For any consequential action, can the Deployment name who acted, under which authority,	Authority implied by system access; audit records editable by the actor; an emergency action

Obligation area	Obligation	Conformance question	Non-conformance indicators
	required and an identifiable human or legal Accountable Party (TR-L3, TR-L4; TRI-06, TRI-09; F3, F5; Section 13.10)	manifest and policy version, and for which Accountable Party?	reviewed only by the person who took it
Federation	Every federation declares its type and the eleven federation terms; each Deployment keeps its own logical control plane (TR-L6, TR-L10, TR-L13; TRI-12; FD-01 to FD-09)	Could each party withdraw recognition under the declared terms while continuing obligations are still met, and does any hosting position confer authority?	Undeclared federation carrying consequential exchange; a shared hub whose operator decides for others; a mandate that removes challenge
Human-Agent	Every Agent has its own identity, a current DelegationGrant, a named Agent Principal, Agent Operator and Accountable Party, a class ceiling that excludes CC-4 confirmation, governed memory and a containment setting (TR-L4, TR-L5; TRI-10; Section 14)	Could every Agent be switched off today without any person losing a route to a human or any commitment becoming invisible (Section 14.10)?	An Agent acting under a human or shared identity; tool use outside a Tool-class interface; memory treated as current state; a self-widened grant
Candidate Canonical Patterns	A Candidate Canonical Pattern in use is declared as such, with a fallback that does not depend on it, and evidence is reported for its validation (Sections 1.2 and 22.3)	Is any floor element or CC-3 or CC-4 obligation met solely through a Candidate Canonical Pattern or research position?	A pattern presented as proven; no declared fallback; a class set below the Section 13.2 floor

23.3 Challenge routes

A conformance claim is itself challengeable. Any participant, steward, control owner, federated peer or acceptance authority may challenge a claim that an implementation conforms, on the ground that an obligation in Section 23.2 is not met. The challenge is raised through TRD-09 like any other (Section 4.3), is recorded against the Composition Manifest and does not depend solely on the system being challenged (F1). A challenge upheld against a floor element or a frozen law moves the manifest to Suspended for the affected consequential operations (Section 10.3) until the obligation is met or a WP06.9 exception or equivalence is approved. Other upheld challenges are recorded as Degradation Events and resolved in the next manifest version. A challenge showing that a law is itself defective is escalated for architecture review, not resolved locally (Section 4.1).

23.4 What conformance does not show

Conformance shows that the technical means exist and operate. It does not show that an organisation is legitimate, that its decisions are just or that its people use the routes provided (Section 3.1; H7). It is never presented as a certification, and it lasts only as long as its evidence: a material change, failure, upheld challenge, lapsed recovery-test interval or new evidence requires the conformance statement to be revisited (TR-L15).

CONCLUSION

24. Architectural conclusion

WP06.10 closes the gap the rest of the suite deliberately left open: how commitments made in architecture become true in running technology, and stay true as that technology changes. It does so without choosing a technology, because the commitments must outlast every such choice.

The paper's answer has a simple shape, governed by seventeen frozen laws and sixteen invariants beneath them. Decisions are made in a logically separate, federated control plane and enforced where execution happens. Meaning is realised faithfully, with history appended and superseded and current state derived rather than trusted. Every crossing, automated or human, is a Governed Capability Interface that carries meaning, authority and obligation with it. Consistency is proportionate to consequence, reversibility and harm. Agents act only within delegated authority, and every consequential Agent action traces to a Human Authority Holder and an identifiable human or legal Accountable Party. Every Composition is declared, recoverable to a state that remembers what people are owed, portable without semantic or constitutional loss and replaceable. And beneath all proportional scaling sits a floor that does not move: a route to challenge, an accessible way to participate, a record of authority, the ability to correct, an audit of consequential action, someone responsible for continuity, the ability to leave, and the ability to recover.

The paper does not claim that every construct is proven. Ten positions remain registered as research; the consistency classes, the Agent memory classes and the Capability Information Disclosure View are Candidate Canonical Patterns; and the architecture is designed so that none of them is load-bearing for the floor or for irreversible action until evidence supports it. Section 23 states how an implementation shows that it is a WP06.10 implementation, without a score or maturity level. Nor does the paper claim that infrastructure can make an organisation legitimate. Capability Infrastructure can enable, constrain, evidence and make

challengeable legitimate operation; honesty, justice, competence, participation, remedy and institutional courage remain the work of people and institutions.

FINAL CANONICAL POSITION

Capability Infrastructure makes the commitments of the WP06 architecture implementable, governable, interoperable, recoverable and replaceable across separately governed deployments, so that what the organisation has promised remains true whichever technologies it uses, whoever operates them and whatever happens to them.

APPENDICES

Appendix A. Visual catalogue and production record

A.1 Visual catalogue

Every visual in this paper is a technology-neutral architecture diagram. Visual numbers follow reading order; Engineering Cycle 2 corrected VA-10 and VA-11, which had been out of order (Appendix A.3). Each visual has a numbered caption, alternative text in the document, a textual explanation in the body of the section where it appears, and text labels that repeat any meaning carried by colour.

Visual	Title	Location	Purpose
VA-01	Technical Realisation Architecture	Section 7	Five logical planes on the inherited foundation
VA-02	Federated Control and Execution Model	Section 8	Decision and enforcement within and across Deployments
VA-03	Technical Responsibility Domains	Section 9	The ten TRDs and their primary planes
VA-04	Composition Manifest Model	Section 10	Manifest sections M1 to M12 and lifecycle
VA-05	Governed Capability Interface	Section 11	Interface elements G1 to G8 and realisation modes
VA-06	Semantic Realisation and Lineage	Section 12	Records, projections and correction propagation
VA-07	Distributed State and Transaction Integrity	Section 13	Consistency classes CC-0 to CC-4 as a Candidate Canonical Pattern
VA-08	Human-Agent Configuration	Section 14	Accountability roles, delegation chain, memory classes and containment ladder
VA-09	Federation and Portability	Section 15	Federation types and terms, packages with Disclosure View, originator exit and reconciliation
VA-10	Minimum Recoverable Capability State	Section 17	MRCS layers R1 to R5 and recovery sequence
VA-11	Technical Evolution and Migration	Section 18	Evolution steps E1 to E6 and replaceability
VA-12	Quality Attributes and Minimum Infrastructure Floor	Section 19	Floor elements F1 to F8 and attributes Q1 to Q13

A.2 Accessibility and production record

Check	Result in v1.0	Correction made in Engineering Cycle 1
Visual numbering	VA-01 to VA-12 follow reading order after the Engineering Cycle 2 correction of VA-10 and VA-11 (Appendix A.3)	VA-07 and VA-08 renumbered so that VA-07 is Distributed State and Transaction Integrity (Section 13) and VA-08 is Human-Agent Configuration (Section 14); the v0.1 out-of-order note removed
Text size inside visuals	All visual text is at least 10 pt at printed width	All twelve visuals redrawn at a fixed scale with text wrapping; labels shortened where needed; v0.1 visuals carried text of about 8 pt
Alternative text	All twelve visuals carry meaningful alternative text	Alternative text rewritten to match the corrected labels, roles, federation types and interface modes
Captions and body explanation	Each visual has a numbered caption and is explained in the text of its section	Captions renumbered for VA-07 and VA-08; explanations updated
Colour	No meaning is carried by colour alone	Bracketed plane labels added to VA-03; red warnings in visuals carry explicit text
Data table headers	Every multi-row data table has a visible, labelled first row marked as a repeating Word header row	Header marking verified for every data table in the build; no blank or invisible headers
Key-value tables	Document control tables use labelled Attribute and Value headers	No fake empty headers
Callouts	Labelled callouts are shaded, bordered paragraphs, not tables	v0.1 one-cell callout tables converted so that assistive technology does not announce them as data tables
Header contrast	Navy header text (17365D) on pale blue (DCEAF4), contrast ratio above 10:1	Retained
Minimum text size	10 pt minimum for body, table, caption, callout, header and footer text	Retained; no production exception required

A.3 Engineering Cycle 2 visual review

All twelve visuals were reviewed for numbering, captions, cross-references, alternative text, consistency, terminology, readability, hierarchy and technology independence. One defect was corrected; no visual was added or redesigned.

Check	Finding	Decision
Numbering	VA-11 (Section 17) appeared before VA-10	Visual titles, captions and A.1 corrected: Minimum

Check	Finding	Decision
	(Section 18), contrary to the A.2 claim	Recoverable Capability State is VA-10 and Technical Evolution and Migration is VA-11; content unchanged
Captions and cross-references	All twelve captions match A.1; no body text cites a visual by number	No change
Alternative text	Alternative text matches each visual's labels and carries no visual number	Retained
Terminology	Labels use the canonical names in B.2; VA-02 'Control plane (logical)' is a Deployment's instance of the Federated Control Plane; VA-09 'package or view' abbreviates package or Disclosure View	No change; abbreviations recorded in B.2
M-prefixed labels	VA-04 shows manifest sections M1 to M12 and VA-08 shows memory classes M0 to M4, each under an explicit panel title	Retained; body citations qualified (ED-10.03)
Technology independence	No visual names a vendor, product, cloud or protocol; VA-05 lists realisation modes, not technologies	No change
Readability and hierarchy	Visual text remains at least 10 pt at printed width; title, subtitle and panel hierarchy consistent across VA-01 to VA-12	No change
Omissions	No critical omission; Section 23 is carried by a table and needs no diagram	No visual added

Appendix B. Glossary of WP06.10 constructs

Term	Meaning	Section
Accountable Party	The human or legal person answerable for satisfaction, remedy, continuity and Renewal of an obligation, aligned with WP06.9	14.1

Term	Meaning	Section
Agent	A Requirement Subject and delegated technical actor that can never become the Accountable Party	14.1
Agent Operator	The identifiable organisation or Deployment responsible for running the Agent configuration as accepted	14.1
Agent Principal	The Human Authority Holder or governed organisational role that creates and remains responsible for a DelegationGrant	14.1
Candidate Canonical Pattern	A pattern adopted as the default realisation of a frozen law, pending implementation validation: the consistency classes, the Agent memory classes and the Capability Information Disclosure View	1.2, 13
Capability Infrastructure	The enduring, governed technical substrate through which WP06 commitments are realised	6
Capability Information Disclosure View	The per-element declaration of custody, rights, transfer status, permitted use, redaction, dispute and correction within a Capability Information Package; short form Disclosure View; Candidate Canonical Pattern	15.3.1
Capability Information Package	Portable, self-describing, integrity-protected bundle of capability information with its Disclosure View; canonical construct, with long-horizon viability registered as RV-03; abbreviated CIP	6, 15.3
Capability Service	A bounded, separately governable unit of technical responsibility that realises obligations from one primary TRD, exposes its consequential operations through Governed Capability Interfaces, and declares its semantic, authority, consistency, evidence, degradation, dependency, ownership and replacement obligations	6, 9.1
Composition	Declared arrangement of services, interfaces, policies, records and roles for a purpose	6, 10
Composition Manifest	Authoritative, versioned declaration of a Composition, sections M1 to M12, cited as 'manifest section Mn'	10
Consistency class	CC-0 to CC-4 classification of a bounded operation in context by consequence, reversibility and harm (Candidate Canonical Pattern)	13
Containment ladder	C1 Observe to C5 Withdraw levels of Agent containment	14.7
Controlled Composition Variability	Variation of Compositions within Fixed, Bounded and Open classes (research position RV-02)	10.4
Current-State Projection	Derived, rebuildable, freshness-declared view of current state	6, 12.4

Term	Meaning	Section
Deployment	Separately governed instance of Capability Infrastructure under an accountable operator	6
Emergency and Protective Action pattern	Bounded pattern for urgent protective action where delay would cause greater immediate harm; standard architecture since Engineering Cycle 2	13.10
Federation	A governed and explicitly declared relationship among separately governed Deployments in which each retains its own authority while recognising defined identities, semantics, decisions, interfaces, obligations or trust states under bounded terms	6, 15.2
Federation types	Voluntary, Contractual, Mandated, Delegated and Emergency Federation	15.2
Frozen architecture laws	TR-L1 to TR-L17, as frozen in the WP06.10 structural baseline	4.1
Governed Capability Interface	The declared contract through which capability is invoked or information is exchanged; automated, human-mediated, offline or hybrid; elements G1 to G8	6, 11
Human Authority Holder	The human who exercises, confirms or delegates a decision right under WP06.8	14.1
Memory classes	M0 to M4 classification of Agent memory, cited as 'memory class Mn'; Candidate Canonical Pattern	14.6
Minimum Infrastructure Floor	Floor elements F1 to F8 retained whatever proportionality is applied (TR-L17; research position RV-07 for small-scale viability)	6, 19
Minimum Recoverable Capability State	Layers R1 to R5 that recovery must restore	6, 17
Plane	Logical grouping of technical responsibility with a distinct integrity concern	7
Protective routes	Protected participation, challenge, correction, containment, exit and remedy routes that remain available (TR-L14)	4, 13.8
Technical Realisation Invariant	Operational rule TRI-01 to TRI-16 that realises one or more frozen laws	4.2
Technical Responsibility Domain	One of ten areas of technical obligation, TRD-01 to TRD-10	9

B.2 Canonical terminology register

Engineering Cycle 2 froze one canonical name for each architectural term. The register gives the accepted short form, where one exists, and the variants removed from body text, tables, visual text references, appendices and the decision record. Terms owned by other papers are used exactly as their owners define them.

Canonical term	Defined in	Accepted short form	Variants removed or not to be used
Capability Infrastructure	6	None	platform; technical platform (as synonyms)
Capability Service	6, 9.1	service, where unambiguous	independently governable service; component; microservice (as synonyms)
Composition	6, 10	None	solution; application (as synonyms)
Composition Manifest	6, 10.2	manifest; manifest section Mn	deployment manifest; Compatibility Manifest, which is the WP06.7 spelling of the WP06.3 CompatibilityManifest
Deployment	6	None	tenant; instance; environment (as synonyms)
Federation	6, 15.2	None	integration; partner network (as synonyms)
Capability Information Package	6, 15.3	CIP; package	export bundle; data package
Capability Information Disclosure View	15.3.1	Disclosure View; 'view' in VA-09 labels only	disclosure view in lower case
Current-State Projection	6, 12.4	projection	state projection; read model; cache (as synonyms)
Governed Capability Interface	6, 11	GCI; interface within Section 11	API; endpoint (as synonyms)
Technical Responsibility Domain	9	TRD	responsibility area; technical domain
Minimum Recoverable Capability State	6, 17	MRCS	minimum viable state; recovery point
Minimum	6, 19.2	the floor; F1 to F8	minimum viable

Canonical term	Defined in	Accepted short form	Variants removed or not to be used
Infrastructure Floor			platform; MVP
Federated Control Plane	7.2, 8	a Deployment's control plane, meaning its logical instance of the plane	central or global control plane
Other plane names	7.2	None	execution plane; information plane
Agent	14.1	None; always capitalised	agent in lower case as a separate term
Human-Agent Configuration	WP06.9 CO-05; 14	Human-Agent	human-agent in lower case
Domain Pack	WP06.7; WP06.3 DomainPack	None	Domain pack
Memory class	14.6	memory class Mn	a bare Mn where a manifest section could be meant
Architecture conformance	23	conformance	compliance, certification or maturity (as synonyms)

Appendix C. Law and invariant traceability

C.1 traces each frozen law through the invariants that realise it to sections, Technical Responsibility Domains, Minimum Infrastructure Floor elements and WP06.9 requirements. C.2 does the same for each invariant. In Engineering Cycle 2 every WP06.9 reference was validated row by row against the WP06.9 v1.0 FINAL anchor requirements (Sections 8.4 to 8.7), Control Domains (Section 9.1) and structural rules. Where no anchor requirement exists, the row names the WP06.9 section that provides the nearest architectural basis and states why no requirement can be cited (ED-10.08). No row is left for later confirmation.

C.1 Frozen law traceability

Law	Invariants	Sections	TRDs	Floor	WP06.9 requirements
TR-L1	TRI-01, TRI-07	5, 11.4, 12.1	TRD-02, TRD-05	F4	No anchor requirement exists. Nearest basis: WP06.9 Section 11.4 (traceability as a specialisation of WP06.3 lineage) and IA-05. WP06.9 anchors govern obligations to people, not preservation of technical meaning
TR-L2	TRI-01, TRI-02	3, 7.5	TRD-10	F7	No anchor requirement exists. Nearest basis: FR-11.03 and FR-09.03 through replaceability. Topology and mechanism variation is not a WP06.9 subject
TR-L3	TRI-03, TRI-05, TRI-06, TRI-11	8, 13.3	TRD-03	F3	FR-14.01; FR-05.03
TR-L4	TRI-09, TRI-10	14.1, 14.5	TRD-03, TRD-06	F3, F5, F6	FR-14.01; FR-15.03; WP06.9 Section 5.3 (Agents never Accountable Parties)
TR-L5	TRI-06, TRI-10	14.3 to 14.9	TRD-06	F3	FR-05.03; FR-04.03; FR-09.02
TR-L6	TRI-03, TRI-12	11, 15.1	TRD-05	F7	FR-12.02; FR-11.01
TR-L7	TRI-03, TRI-07, TRI-08, TRI-09	12	TRD-02	F4, F5	FR-04.01; FR-15.02
TR-L8	TRI-04, TRI-05	7.5, 9.1	TRD-04 and every primary TRD	F6	FR-11.01; FR-12.01
TR-L9	TRI-04	10	TRD-04	F5	FR-12.01; FR-14.01
TR-L10	TRI-12	6.2, 10.1, 15.2	TRD-08, TRD-05	Not floor-specific	WP06.9 Section 12.3 (no automatic inheritance)
TR-L11	TRI-08, TRI-13	15.3, 15.4	TRD-05	F7	FR-13.01; FR-13.03; FR-11.03
TR-L12	TRI-14, TRI-16	17, 18	TRD-10	F8	FR-16.02; FR-10.03
TR-L13	TRI-02, TRI-12, TRI-16	15.2, 18.4	TRD-10, TRD-05	F6, F7	FR-08.02; FR-11.03; FR-09.03

Law	Invariants	Sections	TRDs	Floor	WP06.9 requirements
TR-L14	TRI-08, TRI-11, TRI-14	8.2, 13.8, 13.10, 16.3	TRD-09, TRD-01	F1, F2, F4, F7	FR-15.01; FR-13.02; FR-13.03; FR-16.01; FR-02.03
TR-L15	TRI-16	16.2, 18	TRD-10, TRD-08	F4, F8	FR-16.03; FR-16.04; FR-10.03
TR-L16	Realised directly by Section 13	13	TRD-04, TRD-02	F5	No anchor requirement exists. Nearest basis: WP06.9 Section 15.1 proportionality factors (consequence, reversibility) and FR-09.02. Consistency strength is a technical property WP06.9 does not regulate
TR-L17	TRI-15	19	All	F1 to F8	WP06.9 Section 15.2 constitutional floor

C.2 Invariant traceability

Invariant	Laws	Sections	TRDs	Floor	WP06.9 requirements
TRI-01	TR-L1, TR-L2	5, 11.4, 12.1	TRD-02, TRD-05	F4	No anchor requirement exists. Nearest basis: WP06.9 Section 11.4 and IA-05 (as TR-L1)
TRI-02	TR-L2, TR-L13	3, 7.5, 18	TRD-10	F7	FR-11.03; FR-09.03
TRI-03	TR-L6, TR-L3, TR-L7	11	TRD-05	F1, F5	FR-12.02; FR-14.01
TRI-04	TR-L9, TR-L8	10	TRD-04, TRD-03	F5	FR-12.01; FR-14.01
TRI-05	TR-L3, TR-L8	7.5, 8	TRD-03	F3	FR-14.01; FR-05.03
TRI-06	TR-L3, TR-L5	8, 13.3, 14.3	TRD-03, TRD-06	F3	FR-05.03
TRI-07	TR-L7, TR-L1	12	TRD-02	F4, F5	FR-04.01
TRI-08	TR-L7, TR-L11, TR-L14	12.6, 15.3	TRD-02, TRD-05, TRD-09	F4	FR-15.02
TRI-09	TR-L7, TR-L4	11.2, 12.2, 16	TRD-02, TRD-03	F5	FR-14.01; FR-04.01
TRI-10	TR-L4, TR-L5	14	TRD-06	F3, F5	FR-05.03; FR-04.03; FR-09.02
TRI-11	TR-L14, TR-L3	8.2, 13.8, 13.10, 16.3	TRD-09, TRD-01	F1, F2	FR-15.01; FR-13.02; FR-16.01

Invariant	Laws	Sections	TRDs	Floor	WP06.9 requirements
TRI-12	TR-L6, TR-L10, TR-L13	8.3, 15.2	TRD-05, TRD-03	F3	FR-11.01
TRI-13	TR-L11	15.3, 15.4	TRD-05	F7	FR-13.01; FR-13.03
TRI-14	TR-L12, TR-L14	17	TRD-10	F8	FR-16.02
TRI-15	TR-L17	19	All	F1 to F8	WP06.9 Section 15.2 constitutional floor
TRI-16	TR-L13, TR-L15, TR-L12	18	TRD-10, TRD-05	F6, F7	FR-08.02; FR-10.03; FR-16.03

Appendix D. Architectural decision record

D.1 Contradiction and ownership checks

Check	Finding	Resolution
Composition Manifest versus WP06.3 CompatibilityManifest	Names are similar; purposes differ	Kept distinct; Composition Manifest references CompatibilityManifests in M12 (Section 21.1)
Law and rule prefixes	TR-L, TRI and WP06.9 TR prefixes could be confused	Three distinct prefixes; WP06.9 rules cited unchanged (Section 4)
DelegationGrant and AgentIdentity	Owned semantically by WP06.3	Realised technically only; no semantic attributes added (Section 14)
Organisational memory	WP06.3 forbids Organisational Wisdom as a stored authority object	Agent memory classes prohibit memory becoming authority (Sections 12.7 and 14.6)
Erase versus append-and-supersede	WP06.2 treats deletion as a system right; TRI-07 preserves consequential history	Bounded position adopted (Section 12.2) and confirmed sufficient for freeze in Engineering Cycle 2; downstream WP06.2 confirmation only (IA-10.04; ED-10.02)
Control plane federation versus single-operator simplicity	A single control plane would contradict TR-L6, TR-L13 and WP06.2 jurisdiction	Each Deployment runs its own logical control plane; recognition only under declared federation terms (Section 8.3)
Proportionality versus floor	Small participants may be excluded by floor cost	Floor defined with minimum-scale realisations (Section 19.3); viability registered as RV-07

Check	Finding	Resolution
Visual order	v0.1 placed VA-08 before VA-07; v0.2 placed VA-11 before VA-10	Both corrected: VA-07 and VA-08 renumbered in Engineering Cycle 1; VA-10 and VA-11 relabelled in Engineering Cycle 2 (Appendix A.3)

D.2 Constructs introduced beyond the structural baseline

The following elements were introduced to make the frozen baseline implementable and self-consistent. Each resolves an implementation impossibility or gap rather than adding new architecture. Each was confirmed at the Engineering Cycle 2 freeze review (Appendix D.9); the Cycle column records any change of status.

Element	Reason introduced	Section	Cycle
Technical Realisation Invariants TRI-01 to TRI-16	Retain the v0.1 operational laws beneath the restored frozen laws	4.2	Engineering Cycle 1
Consistency classes CC-0 to CC-4 (Candidate Canonical Pattern)	TR-L16 requires assignable classes; baseline does not enumerate them	13.1	v0.1; adjudicated in Cycle 1
Emergency and Protective Action pattern	Urgent protective action must be possible without an unbounded exception	13.10	Engineering Cycle 1; standard architecture from Engineering Cycle 2
Decision outcomes (Permit, Permit with obligations, Escalate, Deny, Indeterminate)	Enforcement requires a defined outcome set, including the indeterminate case needed for TR-L14	8.2	v0.1
Manifest sections M1 to M12 and lifecycle states	The Composition Manifest cannot be validated without defined content and states	10.2, 10.3	v0.1; M2, M6, M8, M11 amended in Cycle 1
Interface elements G1 to G8 and realisation modes	The GCI cannot be tested without defined elements; manual and offline routes need conformance conditions	11.1, 11.2	v0.1; modes added in Cycle 1
Accountability roles (Human Authority Holder, Agent Principal, Agent Operator)	TR-L4 requires human or legal accountability to be traceable through delegation	14.1	Engineering Cycle 1

Element	Reason introduced	Section	Cycle
Memory classes M0 to M4 and containment levels C1 to C5	The baseline requires memory classes and containment; enumeration makes them enforceable	14.6, 14.7	v0.1; memory classes a Candidate Canonical Pattern from Engineering Cycle 2
Federation types and eleven federation terms	Federation is not always voluntary; every type needs declared bounds	15.2	Engineering Cycle 1
Capability Information Disclosure View	Packages must not imply ownership or exportability of everything associated with a participant	15.3.1	Engineering Cycle 1; Candidate Canonical Pattern from Engineering Cycle 2
Capability Service declarations	TR-L8 requires dependencies and systemic consequences to be explicit	9.1	Engineering Cycle 1
Logical and physical separation rule XP-05	Prevents the architecture implying one technical style	7.4, 7.5	Engineering Cycle 1
MRCS layers R1 to R5	The MRCS cannot be tested without defined layers	17.1	v0.1
Floor element numbering F1 to F8	Enables traceability to WP06.9 without changing baseline floor content	19.2	v0.1
Rule sets XP, CM, CSP, CP, FD, CIP and OX	Operational rules needed to make the constructs checkable	7.4, 10.1, 12.4, 13.5, 15	v0.1; FD and CIP amended in Cycle 1

D.3 Open items

Item	v0.1 description	Decision in v0.2	Status
OI-01	Law wording authored without the frozen baseline text	Frozen TR-L1 to TR-L17 restored word for word; v0.1 laws reclassified as TRI-01 to TRI-16; all references, the manifest conformance statement, glossary, visuals, failure modes, traceability and conclusion updated	Closed

Item	v0.1 description	Decision in v0.2	Status
OI-02	Expansion of FCC not confirmed	FCC confirmed as Frontier Capability Civilisation. RV-01 redefined as FCC-scale architecture viability; RV-10 as broader societal-scale extension; distinction reviewed and retained (Section 22.3)	Closed
OI-03	WP06.9 mappings indicative	Mappings validated against WP06.9 v1.0 FINAL anchor requirements; specific requirement identifiers now cited; rows that cannot be derived are marked individually for confirmation (IA-10.11); blanket disclaimer removed	Closed; the three rows carried to IA-10.11 resolved in Engineering Cycle 2 (ED-10.08)
OI-04	Erasure realisation as governed redaction	Not declared resolved. Bounded position adopted in Section 12.2; WP06.2 v2.0 does not give a definitive technical answer	Closed for WP06.10 (ED-10.02); downstream WP06.2 confirmation
OI-05	TRD ownership placement	WP06.8 has not yet placed TRD ownership, continuity owner, Agent Principal or Agent Operator roles	Closed for WP06.10 through the Section 21.1 mapping (ED-10.01); downstream WP06.8 placement

D.4 Frozen-input metadata audit

Each input was checked on 23 September 2026 by reading its file name and its internal document control (version, status, baseline or freeze date and supersedes statement). The audit corrected two v0.1 errors: v0.1 described its inputs as 'WP06.3 v2.0 FINAL' and 'WP06.6 v2.0 FINAL', whereas the internal version of both is v2.0 with the status 'frozen canonical architecture baseline' and only the file names carry the FINAL suffix; and v0.1 described WP06.11 as frozen, whereas its internal status is 'candidate architecture baseline'.

Paper	File name suffix	Internal version	Internal status and date	Treatment in WP06.10
WP06.0	v2.0_FINAL (a v2.1_CANDIDATE also exists)	v2.0	Frozen canonical architecture baseline; 21 September 2026	Frozen input at v2.0
WP06.1	v2.0_FINAL	v2.0	Frozen canonical architecture baseline; 21 September 2026	Frozen input

Paper	File name suffix	Internal version	Internal status and date	Treatment in WP06.10
WP06.2	v2.0_FINAL	v2.0	Frozen canonical architecture baseline; 21 September 2026	Frozen input
WP06.3	v2.0_FINAL	v2.0	Frozen canonical architecture baseline; 21 September 2026; supersedes v1.0 frozen baseline and v1.1 integration candidate	Frozen input, cited as WP06.3 v2.0
WP06.4	v2.0_FINAL	v2.0	Frozen canonical architecture baseline; 21 September 2026	Frozen input
WP06.5	v2.0_FINAL	v2.0	Frozen canonical architecture baseline; 21 September 2026	Frozen input
WP06.6	v2.0_FINAL	v2.0	Frozen canonical architecture baseline; 21 September 2026	Frozen input, cited as WP06.6 v2.0
WP06.7	v2.0_FINAL	v2.0	Frozen canonical architecture baseline; 21 September 2026	Frozen input
WP06.8	v2.0_FINAL	v2.0	Frozen canonical architecture baseline; 21 September 2026	Frozen input
WP06.9	v1.0_FINAL	v1.0 FINAL	Frozen canonical architecture baseline; 22 September 2026	Frozen input
WP06.1 1	v1.0 (no FINAL suffix)	v1.0	Candidate architecture baseline; 22 September 2026	Candidate input; dependencies provisional (IA-10.08)
WP06.1 2	v1.0 in the architecture folder; v1.0_FINAL copy elsewhere	v1.0 (footer: v1.0 FINAL)	Frozen canonical architecture baseline; freeze date 22 September 2026	Frozen input

D.5 Engineering Cycle 1 findings register

Finding	Severity	Description	Closure
EC1-01	Critical	v0.1 laws did not match the frozen structural baseline wording	Frozen laws restored (Section 4.1); v0.1 laws reclassified as invariants (Section 4.2)
EC1-02	Critical	Accountability narrowed to an 'accountable human principal', contrary to TR-L4	Five accountability roles defined (Section 14.1) and applied throughout
EC1-03	Critical	'Independently governable services' contradicted the frozen baseline	Replaced by 'separately governable, with explicit dependencies and systemic consequences'; canonical Capability Service definition adopted

Finding	Severity	Description	Closure
EC1-04	Major	Consistency classes presented as settled canonical architecture	Positioned as Candidate Canonical Pattern; context, vulnerability, emergency, partition, pre-commit and technology-neutrality nuances added; RV-11 added
EC1-05	Major	Governed Capability Interface read as a digital endpoint only	Redefined as a governed interaction contract with ten realisation modes (Section 11.1)
EC1-06	Major	Federation defined as voluntary and fully revocable	Broadened definition, five federation types and eleven declared terms (Section 15.2)
EC1-07	Major	Packages implied participants own or can export everything associated with them	Disclosure View, information classes, per-element declarations, revised CIP-01 and new CIP-06 (Section 15.3)
EC1-08	Major	Frozen-input metadata misdescribed WP06.3, WP06.6 and WP06.11	Audit completed and front matter corrected (D.4)
EC1-09	Major	Visible table header rows not structurally marked; callouts represented as tables	Header rows marked and repeated; callouts converted to shaded paragraphs (Appendix A.2)
EC1-10	Major	'Capability Services belong to exactly one TRD' was too narrow	Primary and contributing TRDs; service declarations (Section 9.1)
EC1-11	Major	Text could imply one required technical style	Logical and physical separation rule XP-05 and Section 7.5
EC1-12	Important	VA-07 and VA-08 out of reading order	Renumbered
EC1-13	Important	Visual text below 10 pt at printed size	Visuals redrawn
EC1-14	Important	No explicit limitation on what infrastructure can achieve	Foundational limitation (Section 3.1) traced into Sections 5.3, 20, 22 and 23
EC1-15	Important	Erasure described as resolved	Bounded position (Section 12.2)
EC1-16	Important	Open items OI-01 to OI-05 unresolved	Closed or retained (D.3)

D.6 Secondary contradiction review

After all corrections were applied, the paper was reviewed against each frozen input for the twelve failure patterns below.

Check	Finding	Decision
Semantic redefinition (WP06.3)	No WP06.3 object redefined. DelegationGrant, AgentIdentity, CorrectionRecord and OrganisationalMemoryRecord used as defined	No change
Trust or rights invention (WP06.2)	The Emergency and Protective Action pattern and Mandated Federation touch rights but create none	Confirmation requested (IA-10.10). Engineering Cycle 2 found the pattern compatible with WP06.2 Sections 2, 6 and 13 (ED-10.06)
Change-method duplication (WP06.6)	Section 18 describes technical migration only	No change
Compliance duplication (WP06.9)	TRD-08 records acceptance and never performs it; laws and invariants are not acceptance decisions	No change
Assurance duplication (WP06.11)	RVR confidence uses WP06.11 vocabulary without defining it; WP06.11 is a candidate baseline	Dependencies marked provisional (IA-10.08); re-verified in Engineering Cycle 2 (ED-10.05)
Economic-policy invention (WP06.12)	No prices or economic rules set; cost of floor and correction made visible only	No change
Hidden automatic trust inheritance	Checked Compositions, Deployments, Federations and packages	TR-L10 applied through CM-02, FD-09 and Section 6.2
Human versus legal accountability drift	All former 'accountable human' and 'principal' wording reviewed	Replaced with the Section 14.1 roles; CC-4 human confirmation retained within an accountability arrangement that may belong to a legal person
Centralisation hidden within federation	Shared infrastructure and Mandated Federation could create a centre	FD-03 and FD-07
Ungoverned Agent authority	Emergency envelopes could be read as Agent self-authority	Agents act only within envelopes declared by a Human Authority Holder and never confirm CC-4
Patterns presented as proven	Consistency classes and packages	Labelled Candidate Canonical Pattern and research position respectively
Research positions becoming load-bearing	Checked floor elements and CC-3 and CC-4 obligations	No floor element or CC-3 or CC-4 obligation depends solely on a research position

Check	Finding	Decision
WP06.8 Agent Owner role	WP06.8 names an Agent Owner that owns function, delegation, supervision, fallback and revocation	Mapped to WP06.8 roles in Section 21.1 in Engineering Cycle 2; downstream WP06.8 placement only (IA-10.03; ED-10.01)

D.7 Consistency-class adjudication

Question	Adjudication
Canonical status	TR-L16 is canonical. CC-0 to CC-4 are a Candidate Canonical Pattern pending implementation validation (RV-11)
Retained classes	CC-0 Informational; CC-1 Advisory; CC-2 Consequential and reversible; CC-3 Consequential and hard to reverse; CC-4 Irreversible or rights-affecting
Context	Class is assigned to the bounded operation in its declared context, not to an interface name
Vulnerability	Automatic one-class uplift replaced by explicit reassessment; the class rises where vulnerability materially increases consequence or harm
Emergency	Emergency and Protective Action pattern added (Section 13.10)
Partition	CC-4 does not proceed under partition by default; limited, locally sovereign emergency exception with mandatory post-reconnection review
Pre-commit hold	Applies where the action and circumstances permit advance notice and challenge; urgent protective action follows the emergency pattern
Technology neutrality	'Linearisable verification' replaced by the strongest current verification and transaction integrity required; linearisability noted only as one possible implementation property

D.8 Decisions carried into Engineering Cycle 2

Decision	Owner	Engineering Cycle 2 outcome
Confirm placement of TRD ownership, continuity owner, Agent Principal and Agent Operator roles	WP06.8 (IA-10.03)	Closed for freeze. Section 21.1 maps the roles to WP06.8; placement is downstream alignment only (ED-10.01)

Decision	Owner	Engineering Cycle 2 outcome
Confirm the bounded erasure, restriction and redaction position	WP06.2 (IA-10.04)	Closed for freeze. Bounded position confirmed (ED-10.02)
Confirm package custody, rights, attribution and disclosure rules	WP06.2, WP06.3, WP06.12 (IA-10.09)	Closed for freeze. CIP-01 clarified against FR-13.01; downstream confirmation only (ED-10.04)
Confirm the three WP06.9 rows marked for confirmation in Appendix C	WP06.9 (IA-10.11)	Closed. Every row validated; rows without an anchor requirement state why (ED-10.08)
Reconfirm WP06.11 dependencies when WP06.11 is frozen	WP06.11 (IA-10.08)	Closed for freeze with WP06.11 dependencies explicitly provisional; reconfirmation retained (ED-10.05)
Series-table title updates and boundary map additions	WP06.2, WP06.3, WP06.8, WP06.12 (IA-10.01, IA-10.06)	Not freeze-blocking; retained as downstream editorial actions (ED-10.09)

D.9 Engineering Cycle 2 findings register

Engineering Cycle 2 was a freeze-readiness review, not a redesign. It found no contradiction requiring a new construct. The sixteen findings below were resolved by refinement, clarification or reclassification.

Finding	Severity	Description	Closure
EC2-01	Major	CIP-01 disclosure boundaries could be read as narrowing the Constitutional requirement FR-13.01	CIP-01 clarified: boundaries shape the form of transfer, never the ability to evidence one's own capability (ED-10.04)
EC2-02	Major	Emergency actions could be reviewed	Separate reviewer and no-envelope

Finding	Severity	Description	Closure
		only by the person who took them; the pattern was silent where no envelope was declared	rule added; pattern adopted as standard architecture (ED-10.06)
EC2-03	Major	No statement of how an implementation shows it is a WP06.10 implementation	Section 23 Architecture conformance (ED-10.10)
EC2-04	Important	VA-11 appeared before VA-10, contrary to the Appendix A.2 claim	Visuals, captions and A.1 corrected (ED-10.12)
EC2-05	Important	Manifest sections and memory classes both use the M prefix	Every citation qualified (ED-10.03)
EC2-06	Important	Agent Principal relationship to the WP06.8 Defined DelegationGrant Authority and Agent Owner was ambiguous	Role mapping in Sections 14.1 and 21.1 (ED-10.01)
EC2-07	Important	WP06.2 Section 6 Agent-to-Agent hand-off rule not realised	Rule added to Section 14.4
EC2-08	Important	WP06.1 Section 19 proof obligation not acknowledged	Section 21.1 statement (ED-10.07)
EC2-09	Important	Appendix C: TRI-05 cited FR-05.01 by analogy; TR-L8 omitted FR-11.01; TR-L4 omitted WP06.9 Section 5.3; rows left for confirmation	Corrected; no-anchor rows state why (ED-10.08)
EC2-10	Important	The CIP was labelled a research position in its own construct definition	Construct canonical; viability research only (ED-10.11)
EC2-11	Important	Agent memory	Erasure and

Finding	Severity	Description	Closure
		class M4 had no erasure path although Section 12.2 requires one	restriction added (ED-10.02)
EC2-12	Important	Originator exit boundary with WP06.6 and WP06.8 transition not stated	Sentence added to Section 15.5
EC2-13	Minor	Section 5.2 did not mark the WP06.11 dependency provisional	Marked (ED-10.05)
EC2-14	Minor	IA-10.01 understated: WP06.1 and WP06.4 to WP06.7 also carry the planned title	Scope updated (ED-10.09)
EC2-15	Minor	Terminology variants: disclosure view, Domain pack, human-agent, state projections, lower-case agent, informal plane names	Normalised; register in Appendix B.2 (ED-10.13)
EC2-16	Minor	Appendix A.2 and D.8 described the v0.2 state	Updated to v1.0

Research register changes: RV-03, RV-04 and RV-06 were narrowed to the genuine uncertainty that remains; the Capability Information Package construct was confirmed as Canonical Architecture; the Disclosure View and the Agent memory classes were labelled Candidate Canonical Patterns; RV-11 remains a Candidate Canonical Pattern; all other positions were retained as Research Positions. No position was promoted to canonical on a claim of viability, and no confidence level was raised.

D.10 Cross-paper boundary review

Engineering Cycle 2 re-read every WP06 paper for duplication of another paper's ownership. Findings resolved in WP06.10 are closed here; anything left external has an Engineering Decision in D.11.

Paper	Check	Finding	Resolution
WP06.0	Proposition duplication	WP06.10 returns technical credibility only; WP06.0 v2.0	No change; title alignment under

Paper	Check	Finding	Resolution
		cites 'WP06.10 Technical Architecture'	IA-10.01
WP06.1	Platform boundary and proof obligation	Boundary realised, not redrawn; the Section 19 proof obligation on tenancy, policy, graph, event, integration and service feasibility was not acknowledged	Answered in Section 21.1; demonstration downstream (ED-10.07)
WP06.2	Constitutional duplication	No right created or restated; the Section 6 rule that Agent-to-Agent hand-offs preserve original authority was not realised	Hand-off rule added to Section 14.4; erasure and emergency positions confirmed compatible (ED-10.02, ED-10.06)
WP06.3	Semantic duplication	No WP06.3 object redefined; Disclosure View declarations such as custodian, contributor and rights holder could be read as new semantic attributes	Declared as carriers of owner-set values; relationship types referred to WP06.3 (ED-10.04)
WP06.4	Interpretation duplication	TRD-07 supplies governed data and method-bound computation only	No change
WP06.5	Journey duplication	Journeys are executed and made accessible, not designed	No change
WP06.6	Transition duplication	Section 18 is technical migration only; originator exit could be read as organisational transition	Boundary sentence added to Section 15.5
WP06.7	Domain duplication	Domain Pack and CompatibilityManife	Normalised; IA-10.07 retained

Paper	Check	Finding	Resolution
		st used as defined; spelling variant 'Domain pack' found	
WP06.8	Role allocation	Technical roles did not state their relationship to the WP06.8 Defined DelegationGrant Authority and Agent Owner	Mapping added to Sections 14.1 and 21.1 (ED-10.01)
WP06.9	Compliance duplication	A conformance section could duplicate acceptance or add a second conformance vocabulary; one Appendix C mapping relied on analogy	Section 23 uses WP06.9 states and creates no score; mappings corrected (ED-10.08, ED-10.10)
WP06.11	Assurance duplication	Confidence vocabulary used, not defined; Section 5.2 did not mark the dependency provisional	Marked provisional (ED-10.05)
WP06.12	Economics duplication	No price or economic rule set; RV-05 concerns technical cost only; WP06.12 v1.0 boundary map omits WP06.10	No change; IA-10.06 retained

D.11 Engineering Decision register

Engineering Cycle 2 raised thirteen Engineering Decisions. Each records what WP06.10 decided locally and, where something is left to another paper, who owns it. No decision left external blocks freeze.

ID	Decision	Status	External owner
ED-10.01	Accountability roles are mapped onto WP06.8 roles without allocating people (Sections	Closed in WP06.10	WP06.8: place TRD ownership, continuity owner, Agent Principal and Agent Operator at

ID	Decision	Status	External owner
	14.1 and 21.1); the accountability model is unchanged (IA-10.03)		next revision
ED-10.02	The bounded erasure, restriction and redaction position of Section 12.2 is sufficient for freeze; erasure is a governed action by a party other than the affected actor; Agent memory class M4 is erasable (IA-10.04)	Closed in WP06.10	WP06.2: optional confirmation; final legal treatment through its specialist review gate
ED-10.03	Manifest sections and memory classes share the M prefix; every citation is qualified as 'manifest section Mn' or 'memory class Mn'; visuals unchanged	Closed	None
ED-10.04	CIP-01 clarified so that disclosure boundaries shape the form of transfer but never remove a participant's ability to evidence their own capability (FR-13.01); Disclosure View declarations carry values set by their owners (IA-10.09)	Closed in WP06.10	WP06.3: register custody, contribution and rights-holder relationship types; WP06.2: disclosure tiers (WP06.9 IA-07); WP06.12: attribution economics
ED-10.05	WP06.10 is frozen with WP06.11 dependencies explicitly provisional; no law, invariant, floor element or CC-3 or CC-4 obligation	Closed for freeze	WP06.11: reconfirm confidence vocabulary and evidence markers when frozen

ID	Decision	Status	External owner
	depends on WP06.11 (IA-10.05, IA-10.08)		
ED-10.06	The Emergency and Protective Action pattern is standard architecture, not a Candidate Canonical Pattern; review by a person other than the actor and a no-envelope rule added (IA-10.10)	Closed in WP06.10	WP06.2: optional confirmation against rights and jurisdiction principles
ED-10.07	The WP06.1 Section 19 proof obligation is answered at architecture level (Section 21.1); demonstration in running technology is implementation evidence, not a freeze condition	Closed for freeze	Implementation programme: implementability review of Section 22.1
ED-10.08	Appendix C mappings validated; TRI-05 cites FR-05.03 instead of FR-05.01; TR-L8 adds FR-11.01; TR-L4 adds WP06.9 Section 5.3; TR-L1, TRI-01, TR-L2 and TR-L16 state why no anchor requirement exists (IA-10.11)	Closed	WP06.9: optional Core requirement on semantic fidelity at next revision
ED-10.09	IA-10.01, IA-10.02, IA-10.06 and IA-10.07 are downstream editorial or confirmation actions and are not freeze-blocking	Retained externally	WP06.0 to WP06.9, WP06.11, WP06.12 at next revision
ED-10.10	Architecture	Closed	None

ID	Decision	Status	External owner
	Conformance added as Section 23, using WP06.9 conformance states, with no score, maturity model or certification		
ED-10.11	Research register reclassified: CIP construct canonical; Disclosure View and Agent memory classes Candidate Canonical Patterns; RV-03, RV-04 and RV-06 narrowed; no position promoted to canonical on claims of viability	Closed	None
ED-10.12	VA-10 and VA-11 relabelled into reading order; no new visual	Closed	None
ED-10.13	Canonical terminology frozen (Appendix B.2); variants normalised across body, tables, appendices and decision record	Closed	None

D.12 Freeze readiness assessment

The assessment below answers the eleven freeze-readiness questions set for Engineering Cycle 2. Each answer cites the evidence in this paper; none relies on a research position as proven.

Question	Evidence in WP06.10 v1.0	Assessment
Coherence: does the architecture tell one story?	One realisation chain (Section 6.1); every frozen law traced through invariants to sections, TRDs, floor elements and WP06.9 (Appendix C) with no orphan; Cycle 2 found	Met

Question	Evidence in WP06.10 v1.0	Assessment
	no contradiction requiring redesign (D.9)	
Ownership: does every major construct have one owner?	Each construct defined once (Section 6; Appendix B.2); the cross-paper boundary review found no unresolved duplication (D.10)	Met
Realisability: could an architecture team implement this?	Planes, TRDs, manifest sections M1 to M12, interface elements G1 to G8, minimum-scale floor realisations (Section 19.3) and conformance obligations (Section 23); WP06.1 proof obligation answered at architecture level (Section 21.1)	Met at architecture level; demonstration is downstream evidence (ED-10.07)
Replaceability: could a stack change without changing commitments?	TRI-02, TRI-16, XP-04, XP-05 and the Section 18.4 tests; no construct or visual names a technology (A.3)	Met
Accountability: does accountability survive automation?	TR-L4, TRI-10 and the five roles of Section 14.1, mapped to WP06.8 and WP06.9 (Section 21.1); emergency actions now reviewed by someone other than the actor (Section 13.10)	Met
Federation: can autonomy survive federation?	TRI-12, FD-01 to FD-09, eleven declared federation terms, one logical control plane per Deployment; cross-federation revocation reliability remains RV-06	Met, with a registered research position
Continuity: can commitments survive disruption?	MRCS layers R1 to R5, protective routes restored first (Section 17.2), F6 and F8, TR-L14 under partition (Section 13.8)	Met
Portability: can capability move?	TR-L11, CIP-01 to CIP-06 with the FR-13.01 clarification, and an F7	Met

Question	Evidence in WP06.10 v1.0	Assessment
	minimum realisation that does not depend on RV-03	
Challengeability: can consequential action be challenged?	F1, G8, TRD-09, challenge of laws (Section 4.3), challenge of conformance claims (Section 23.3), emergency notification and challenge (Section 13.10)	Met
Minimum infrastructure: can small participants participate?	F1 to F8 with minimum-scale realisations and no floor element dependent on a research position; viability for informal Communities remains RV-07	Met in design; small-scale viability registered as research
Architecture identity: does WP06.10 occupy a unique role?	WP06.3 Section 18, WP06.7, WP06.8 and WP06.9 each assign technical realisation to WP06.10; no other paper defines planes, TRDs, the Composition Manifest or the Governed Capability Interface	Met

Decision: READY FOR v1.0 FREEZE. Freeze approved by the owner on 23 September 2026; this document is v1.0 FINAL. No integration action requires a change to WP06.10 before freeze. Every retained action is a downstream alignment in another paper and has an Engineering Decision (D.11). No floor element and no CC-3 or CC-4 obligation depends on a research position. The only standing qualification is the one recorded in the document control: dependencies on WP06.11 remain provisional until WP06.11 is frozen.

Appendix E. Illustrative Composition Manifest skeleton

The skeleton below is illustrative and technology-neutral. It shows the content a manifest declares, not a file format. Values in square brackets are illustrative entries to be replaced by the declaring Composition.

Section	Illustrative entry
M1 Purpose and context	Purpose: [supported capability pathway for a Community]. Participation Context: [Community context identifier]. Domain references: [Domain identifiers]. Beneficiaries: [participant classes]. Federation terms relied on: [Contractual Federation with partner Deployment].

Section	Illustrative entry
M2 Services	[Pathway service: primary TRD-04, contributing TRD-09, v2.3, owner, dependencies, shared controls, systemic consequences, continuity dependency, replacement path]; [record service: primary TRD-02, v1.8]; [matching Agent service: primary TRD-06, contributing TRD-07, v0.9].
M3 Interfaces	[Enrol command, v2, automated and assisted modes]; [evidence exchange, v1]; [allocation command, v1]; [challenge command, v1, automated, human-mediated and offline modes].
M4 Policy and authority	Policies: [policy identifiers and versions]. Authority sources: [decision rights under WP06.8]. Grants: [authority record references]. Emergency authority: [declared envelope and holders].
M5 Consistency classes	Enrol: CC-2 in the practice context (compensation: withdraw enrolment and notify). Opportunity allocation: CC-3. Exclusion from pathway: CC-4, pre-commit hold where circumstances permit.
M6 Agents and roles	[Matching Agent]: identity [reference]; Agent Principal [pathway lead role]; Human Authority Holder [named decision-right holder]; Agent Operator [operating organisation]; Accountable Party [the organisation, a legal person]; ceiling CC-2; memory classes M0 to M2; containment C1.
M7 Records and evidence	Records: [list]. Evidence supplied to WP06.11 methods: [list]. Retention, restriction and erasure treatment: [per WP06.3 lifecycle, WP06.2 and Section 12.2].
M8 Floor, law and invariant conformance	F1 to F8: [how each is met]. Law and invariant conformance statement: [TR-L1 to TR-L17 through TRI-01 to TRI-16].
M9 Degradation and recovery	Degraded mode: [behaviour; protective routes kept]. MRCS: R1 to R5 [stores]. Last recovery test: [date].
M10 Exit and replacement	Participant package or Disclosure View route: [accessible route; Disclosure View declarations]. Service replacement: [path]. Retirement plan: [plan].
M11 Accountable Party and status	Accountable Party: [organisation]. Accountable owner: [role]. Continuity owner: [role]. Status: [Active]. Acceptance Records: [references].
M12 Compatibility	CompatibilityManifest references: [Domain Pack versions]. Deprecations in force: [list].

Appendix F. Scenario traces

The traces below walk representative situations through the planes to show how the laws and invariants operate together. They are illustrative and assume no particular technology.

F.1 An irreversible exclusion

1. A steward initiates exclusion of a participant from a pathway. The operation is declared CC-4 in its context in M5.
2. The enforcement point sends a decision request; the control plane verifies the steward's authority against the authoritative record and returns Escalate for confirmation.
3. A Human Authority Holder with the decision right confirms, acting for the organisation that is the Accountable Party, with visibility of the evidence and the practical ability to refuse. Because circumstances permit notice, a pre-commit hold begins and the participant is notified with a challenge route (F1).
4. The participant challenges during the hold; TRD-09 records the challenge and the action remains held.
5. After review the exclusion is withdrawn. Every step is recorded with actor, authority, Accountable Party and manifest version (F5; TRI-09).

F.2 An Agent reaching its ceiling

1. A matching Agent with a CC-2 ceiling proposes an opportunity allocation, which M5 declares CC-3 in this context.
2. TRD-06 detects that the action exceeds the grant ceiling and holds it; the control plane returns Escalate.
3. The Agent Principal reviews the Agent's evidence, with lineage to its sources, and decides as a Human Authority Holder. The decision, not the Agent's proposal, is the authority for the allocation, and the organisation remains the Accountable Party (TR-L4).

F.3 A correction reaching a package holder

1. A capability evidence record is found to be wrong. A CorrectionRecord supersedes it.
2. Lineage identifies two projections, one allocation decision, an Agent's delegated operational memory (memory class M2) and a Capability Information Package issued to a partner Deployment under Contractual Federation.
3. Projections are rebuilt, the decision is flagged for Decision Contamination Review, the Agent memory is corrected and the partner is notified through the package correction channel declared in its Disclosure View.
4. The participant is informed, and their own Disclosure View shows the corrected element and its prior dispute state. Propagation completion is recorded; any unreachable dependant is recorded as residual risk.

F.4 A partition

1. A Deployment loses contact with its control plane's authority store.
2. Challenge and exit requests continue to be accepted and recorded locally (TR-L14; TRI-11).
3. CC-2 actions proceed where authority was verified within the class window; CC-3 actions queue; CC-4 actions are refused.
4. On heal, locally recorded protective requests are processed first, queued CC-3 actions are re-verified rather than replayed, and a reconciliation record is produced.

F.5 An emergency protective action under partition

1. During the same partition, a safeguarding concern arises that requires an Agent's access to a participant's records to be suspended immediately.
2. A locally present Human Authority Holder, named in the emergency envelope declared in M4, suspends the access. No federated authority is relied on; the local authority record is used.
3. The action is the minimum necessary (suspension rather than deletion), is recorded locally, and a Containment Consequence Assessment is made immediately (WP06.9 FR-16.01).
4. On reconnection, the action is reviewed and accepted, and affected parties are notified and able to challenge. Had the suspension proved excessive, remedy would have been owed.

F.6 An assisted, offline participation route

1. A participant without reliable connectivity asks a Community steward to submit a challenge on their behalf.
2. The steward uses the challenge interface's assisted and offline modes: the steward's identity and authority, the participant's instruction, the purpose and the content are recorded in a controlled log.
3. On reconnection the log is reconciled into the authoritative record with lineage. The challenge carries the same obligations as one submitted online, so the route is a conformant Governed Capability Interface (Section 11.1).

End of WP06.10 Capability Infrastructure Architecture v1.0 FINAL.