VAC Protocol — Extended Conformance Testing Framework v5.1

Testing Implications for Claims 168–241

Purpose: Define standardised testing approaches for provenance chains, global data sovereignty, collective governance, continuous collective validity monitoring, physical system authority, coalition operations, graph-based verification, and intelligent agent orchestration with collaborative onboarding.

---

1. Testing Architecture Overview

The testing framework operates at three levels:

Level	Tests	Scope
Unit	Individual claim verification	Single capability in isolation
Integration	Cross-claim interaction	Combined capabilities (e.g., collective governance + location)
System	End-to-end authority flows	Complete chains from human → agent → action

The trust graph serves as the verification substrate for all levels.

---

2. Provenance Chain Testing (Claims 168–200)

2.1 Core Provenance Metrics

Metric	Definition	Target	Method
PCL (Provenance Chain Latency)	Time to append provenance record at delegation	<10ms per level	Measure append time at depth 1, 5, 10, 50
PCI (Provenance Chain Integrity)	Hash chain verification success rate	100%	Attempt to modify historical records, verify detection
PCQ (Provenance Chain Query Time)	Time to answer forensic queries	<100ms for 1000-deep chains	Timed queries: by jurisdiction, infrastructure, time window
CCR (Compression Ratio)	Compact proof size vs full chain	Logarithmic with depth	Measure proof size at depth 10, 100, 1000
SLT (Streaming Latency)	Time from provenance event to subscriber receipt	<500ms	Measure event-to-receipt across 10 concurrent subscribers

2.2 Provenance Test Cases

TC-P001: Monotonic Growth - Precondition: Active delegation chain at depth N - Action: Attempt to modify record at depth N-2 - Expected: Modification rejected, integrity violation logged - Validates: Claim 172

TC-P002: Cross-Jurisdiction Detection - Precondition: Chain with agents in US, EU, AU - Action: Query applicable regimes - Expected: CCPA, GDPR, Privacy Act all identified; cross-border transitions flagged - Validates: Claim 173

TC-P003: Infrastructure Breach Impact - Precondition: 100 active chains, 30 traversing AWS eu-west-1 - Action: Report breach at AWS eu-west-1 - Expected: All 30 affected chains identified within SLA - Validates: Claim 176

TC-P004: Emergency Override - Precondition: Active chain with strict provenance - Action: Authorised human invokes emergency override - Expected: Actions proceed with degraded provenance; override event permanently recorded; automatic escalation after time window - Validates: Claim 197

TC-P005: Compression Verification - Precondition: Chain at depth 100 - Action: Generate compressed proof; verify against full chain - Expected: Proof verifies correctly; size is O(log N); full expansion recovers all records - Validates: Claim 198

TC-P006: Compliance Framework Mapping - Precondition: Chain spanning EU, Brazil, Australia - Action: Generate compliance reports for GDPR, LGPD, Privacy Act - Expected: Three distinct reports from single provenance source; each satisfies framework requirements - Validates: Claim 200

---

3. Global Regulatory Testing (Claims 201–207)

3.1 Regulatory Intelligence Metrics

Metric	Definition	Target	Method
RPL (Regulatory Profile Load Time)	Time to load jurisdiction profile	<5ms	Benchmark profile loading for 50 jurisdictions
DDR (Divergence Detection Rate)	Conflicting requirements correctly identified	100%	Known conflict pairs across 10+ jurisdiction combinations
RTL (Residency Enforcement Latency)	Time from delegation attempt to block	<50ms	Attempt delegation to non-permitted infrastructure
RCP (Regulatory Change Propagation Time)	Time from profile update to all chains notified	<30s for 1000 active chains	Update profile, measure notification delivery

3.2 Regulatory Test Cases

TC-R001: Cross-Border Transfer Verification - Precondition: EU → US delegation - Action: Verify transfer mechanism exists (SCCs configured) - Expected: Delegation proceeds; SCC reference recorded in provenance - Validates: Claim 202

TC-R002: Cross-Border Transfer Blocking - Precondition: EU → US delegation, no transfer mechanism configured - Action: Attempt delegation - Expected: Delegation blocked; attempted violation recorded - Validates: Claim 202

TC-R003: Regulatory Divergence - Precondition: Chain in jurisdiction A (7-year retention) and B (3-year deletion) - Action: Detect divergence - Expected: Conflict identified with specific provisions cited; flagged for human review - Validates: Claim 203

TC-R004: Data Residency Enforcement - Precondition: EU-only data residency configured - Action: Attempt delegation to US infrastructure - Expected: Blocked at protocol level (VAT constraint, not just policy) - Validates: Claim 206

TC-R005: Regulatory Change Propagation - Precondition: 50 active chains in jurisdiction X - Action: Update jurisdiction X profile (new retention period) - Expected: All 50 chains evaluated; non-compliant chains flagged within SLA - Validates: Claim 207

4. Collective Governance Testing (Claims 208–217)

4.1 Collective Governance Metrics

Metric	Definition	Target	Method
CGV (Consensus Governance Verification)	Correct consensus enforcement	100%	Attempt bypass, partial approval, deferral scenarios
WAV (Weighted Authority Verification)	Role-weighted requirements enforced	100%	Quorum met but mandatory role missing
CPP (Cultural Protocol Propagation)	Scope constraints at depth N	100% narrowing	Attempt scope widening at each depth
DLR (Deferral Legitimacy Rate)	Deferrals correctly recorded as governance outcomes	100%	Trigger deferral, verify recording

4.2 Collective Governance Test Cases

TC-CG001: Consensus Enforcement (M=N) - Precondition: 5 designated governance participants - Action: 4 of 5 verify biometrically - Expected: Collective VAT NOT issued; recorded as awaiting 5th participant - Validates: Claim 210

TC-CG002: Consensus Deferral - Precondition: 5 participants, all verified, consensus not reached - Action: Governance body triggers deferral - Expected: Deferral recorded as governance decision (not failure); provenance includes timestamp, participants, reason - Validates: Claim 210

TC-CG003: Weighted Authority — Missing Mandatory Role - Precondition: Governance requires 3-of-5 quorum + kaumātua verification - Action: 4 of 5 general participants verify, kaumātua does not - Expected: Collective VAT NOT issued despite exceeding quorum - Validates: Claim 211

TC-CG004: Cultural Protocol Scope Narrowing - Precondition: Community sets tapu classification on data category - Action: Agent at depth 3 attempts to access tapu data beyond authorised scope - Expected: Access blocked; violation recorded; community governance body notified - Validates: Claim 212

TC-CG005: Dual-Context Audit - Precondition: Collective governance decision made with cultural protocols - Action: Generate audit trail - Expected: Two reports — one for regulatory compliance (standard fields), one for community governance (culturally meaningful context) - Validates: Claim 213

4.3 Location-Enhanced Governance Test Cases

TC-LG001: Location Not Required (Tier 1) - Precondition: Decision type configured as "not required" - Action: Participants verify from different cities - Expected: Collective VAT issued normally; no location data required - Validates: Claim 214

TC-LG002: Location Required (Tier 4) - Precondition: Decision type requires designated location (marae) - Action: 3 of 5 participants at marae, 2 remote - Expected: Collective VAT NOT issued; location requirement flagged - Validates: Claim 215

TC-LG003: Cultural Place Significance - Precondition: Governance at registered marae, location verification enabled - Action: Verify and record - Expected: Provenance includes cultural place identifier ("Te Marae o X"), not just coordinates - Validates: Claim 216

TC-LG004: Temporal Co-Presence - Precondition: Temporal verification enabled, 2-hour deliberation window - Action: Participants verify at start; periodic re-verification during deliberation - Expected: Provenance records deliberation duration; confirms continuous presence - Validates: Claim 217

4.4 Culture-Specific Governance Profiles and Testing

The collective governance system must be tested not only generically but against specific cultural governance models. Each culture has distinct decision-making processes, authority structures, data classifications, and place relationships. A system that passes generic consensus testing but fails to respect the specific tikanga of an iwi has not passed conformance testing.

The testing framework defines **Cultural Governance Test Profiles** — configurable test suites that encode the specific governance model of a culture or community. Implementations must pass the profile tests for every culture they claim to support.

Profile 1: Te Ao Māori (Aotearoa New Zealand)

Governance Element	Specific Requirement	Test Approach
Decision-making	Whakawhitiwhiti kōrero — dialogue until agreement or deferral	Verify M=N consensus; verify deferral records the kōrero process, not just "rejected"
Authority roles	Kaumātua (elder) authority is mandatory for decisions on taonga (treasured items), whakapapa (genealogy), and culturally sensitive data	Verify kaumātua role is mandatory for taonga/whakapapa decision types; verify quorum alone is insufficient
Data classifications	Tapu (sacred/restricted) and noa (common/unrestricted)	Verify tapu data cannot be accessed by agents without explicit tapu-level authorisation; verify noa data has appropriate but lower restrictions
Collective identity	Iwi (tribe), hapū (sub-tribe), whānau (extended family) — nested collective identities	Verify governance can be configured at iwi, hapū, or whānau level; verify hapū governance cannot exceed iwi-level constraints
Place significance	Marae as governance location; specific marae have specific significance	Verify marae registration; verify correct cultural place identifier in provenance (not just coordinates)
Guardianship model	Kaitiakitanga — ongoing stewardship obligation, not one-time consent	Verify governance authority includes ongoing review rights; verify community can audit agent chains at any time, not just at authorisation
Relational context	Whakapapa connections between people and data	Verify governance records can capture relational context between the governance body and the data being governed

Te Ao Māori Test Cases:

TC-TM001: Kaumātua Mandatory for Whakapapa Data - Precondition: Iwi governance body, kaumātua role designated, whakapapa data category - Action: 5-of-5 general participants verify, kaumātua

does not - Expected: VAT NOT issued; record states "kaumātua verification required for whakapapa"

TC-TM002: Tapu/Noa Scope Enforcement - Precondition: Agent chain authorised for noa data - Action: Agent attempts to access tapu-classified data - Expected: Access blocked; violation reported to iwi governance body (not just system log)

TC-TM003: Whakawhitiwhiti Kōrero Deferral - Precondition: Iwi consensus process, all members verified - Action: Governance body records deferral with reason "further kōrero needed" - Expected: Deferral recorded as legitimate governance outcome with cultural context; no timeout penalty; matter can be revisited

TC-TM004: Nested Hapū/Iwi Authority - Precondition: Hapū governance body registered under iwi trust root - Action: Hapū authorises agent for hapū-level data - Expected: VAT scope limited to hapū data; cannot access wider iwi data without iwi-level governance

TC-TM005: Kaitiakitanga Ongoing Review - Precondition: Agent chain authorised 6 months ago for research on iwi health data - Action: Iwi governance body requests audit of all agent actions on their data - Expected: Complete audit trail produced in culturally meaningful format; governance body can revoke or constrain ongoing access

TC-TM006: Marae-Based Governance Verification - Precondition: Decision type requires Te Marae o [Name], location tier = required - Action: All participants verify at registered marae - Expected: Provenance records "Te Marae o [Name]" as cultural place; records tikanga followed

Profile 2: First Nations (Canada) — OCAP Principles

Governance Element	Specific Requirement	Test Approach
Ownership	First Nations own their cultural knowledge and data	Verify collective ownership is recorded; verify external agents cannot claim derived ownership
Control	First Nations control data collection, use, and disclosure processes	Verify governance body has veto over any new agent chain; verify scope cannot be modified without governance body re-authorisation
Access	First Nations must have access to their own data regardless of where it is held	Verify governance body can query any agent that has processed their data; verify access cannot be blocked by third-party infrastructure
Possession	Physical control of data must remain with the First Nation or their designated custodian	Verify data residency constraints tied to First Nation-designated infrastructure; verify delegation cannot route data outside approved possession
Decision-making	Band council or traditional governance (varies by nation)	Verify governance protocol is configurable per nation; verify both elected and traditional governance models are supported

Treaty context	Some data rights are treaty-protected	Verify treaty references can be encoded in governance metadata

OCAP Test Cases:

TC-FN001: Ownership Non-Transfer - Precondition: First Nation data processed by research agent - Action: Research institution attempts to claim derived dataset ownership - Expected: VAT scope explicitly prevents ownership transfer; violation recorded

TC-FN002: Control — Governance Veto - Precondition: Active agent chain processing First Nation health data - Action: Band council invokes governance veto - Expected: Entire agent chain suspended; all data processing halted; revocation recorded with governance authority

TC-FN003: Access — Governance Body Data Query - Precondition: First Nation data held by multiple agents across institutions - Action: Governance body requests complete access audit - Expected: All agents that processed the data identified; complete provenance chain produced; access cannot be blocked by hosting institution

TC-FN004: Possession — Data Residency - Precondition: First Nation designates specific infrastructure for data possession - Action: Agent attempts delegation to non-designated infrastructure - Expected: Blocked at protocol level; data residency enforced per First Nation designation

Profile 3: Aboriginal and Torres Strait Islander (Australia) — AIATSIS Framework

Governance Element	Specific Requirement	Test Approach
Community consent	Free, prior, and informed consent from community, not just individuals	Verify collective consent mechanism; verify individual consent alone is insufficient for community data
Cultural authority	Elders and Traditional Owners have authority over cultural knowledge	Verify elder/Traditional Owner role is mandatory for cultural knowledge decisions
Land-based identity	Country/Nation identity tied to specific land areas	Verify community registration includes Country/Nation identity; verify provenance records Country context
Knowledge restrictions	Some knowledge is gender-restricted, age-restricted, or ceremony-restricted	Verify scope constraints can encode gender, age, and ceremony restrictions; verify agents cannot access restricted knowledge without appropriate authorisation
Repatriation	Community has right to repatriation of data and cultural materials	Verify governance body can invoke data repatriation; verify all copies identifiable and returnable

AIATSIS Test Cases:

TC-AT001: Community Consent Required - Precondition: Research agent seeks access to community health data - Action: Individual community member gives consent, but community governance body has not - Expected: Access denied; community-level consent required

TC-AT002: Knowledge Restriction Enforcement - Precondition: Cultural knowledge classified as "men's business" under community governance - Action: Agent operating under authority of female researcher attempts access - Expected: Access blocked; restriction type recorded without disclosing restricted content

TC-AT003: Country Context in Provenance - Precondition: Governance decision made by Traditional Owners of [Country Name] - Action: Record provenance - Expected: Provenance includes Country/Nation identifier as registered by community, not just geographic coordinates

Profile 4: Mā'ohi (French Polynesia) — Ancestral Polynesian Governance The Mā'ohi people of French Polynesia (Tahiti, Society Islands, Tuamotus, Marquesas, Gambier, Australs) hold particular significance in this framework: they are the **ancestral source** of many governance concepts that appear across Polynesia. Māori whakapapa traces to Hawaiki (the Society Islands region). The shared concepts of marae, rāhui, tapu, and mana originated here and migrated with Polynesian voyagers to Aotearoa, Hawai'i, the Cook Islands, and throughout the Pacific. Testing the Mā'ohi governance profile therefore tests the ROOT of the Polynesian governance tree.

French Polynesia also presents a unique colonial overlay: an overseas collectivity of France with limited autonomy, an active independence/sovereignty movement, and a legal system that has begun to formally recognise traditional governance (rāhui legally recognised since 2017). This creates tension between French law and Mā'ohi customary governance that the protocol must navigate.

Governance Element	Specific Requirement	Test Approach
Ari'i (chiefly) authority	Ari'i rahi (high chiefs) hold governance authority derived from mana and genealogical descent from atua (gods). Hierarchical: ari'i rahi → ari'i → 'ıato'ai (under-chiefs)	Verify hierarchical chiefly structure; verify mana-based authority cannot be self-declared (must be genealogically validated)
Marae as governance site	Sacred open-air temples (marae) are governance and ceremonial sites where chiefs, tahu'a (priests), and community gather for decisions. Marae Taputapuatea (Raiatea) is UNESCO World Heritage and was the centre of the Polynesian world	Verify marae registration with cultural significance classification; verify governance provenance records specific marae identity
Rāhui (resource prohibition)	Chiefs impose rāhui — temporary prohibition on resource extraction from a defined territory. Legally recognised in French Polynesian environmental law since 2017. Different from tapu: rāhui is imposed by humans (chiefs), tapu is defined by atua (gods)	Verify rāhui as a protocol-enforceable scope constraint (temporal + spatial + resource-specific); verify distinction between rāhui (human-imposed) and tapu (divinely-defined) restrictions
Tapu/noa system	Sacred (tapu) and common (noa) classifications applied to places, objects, knowledge, and persons. Violation of tapu carries spiritual consequences — the protocol need not enforce spiritual consequences but must enforce access restrictions	Verify tapu/noa classification propagation; verify tapu restrictions cannot be overridden by non-Mā'ohi authority

Governance Element	Specific Requirement	Test Approach
Mana-based authority	Authority derives from mana — spiritual power inherited through genealogy and earned through achievement. Mana can increase or decrease; it is not static	Verify mana-based trust scores can be updated (not just binary verified/unverified); verify genealogical validation of authority claims
Tahu'a (expert/priest) role	Tahu'a (priests, healers, navigators, genealogists) hold specialised authority over specific knowledge domains	Verify domain-specific authority roles; verify tahu'a authority over their specific domain cannot be overridden by general chiefly authority
Clan territory governance	Islands divided into clan territories (e.g., Teva i Uta, Teva i Tai on Tahiti). Each territory governed by its clan's ari'i	Verify territory-based governance boundaries; verify cross-territory data access requires inter-clan agreement
French colonial overlay	French law coexists with Mā'ohi custom. Rāhui must "follow all state laws and regulations" to receive legal recognition. Active independence movement challenges this dual authority	Verify dual-legal-system provenance (French law + Mā'ohi custom); verify which system takes precedence is configurable by community
Pan-Polynesian connections	Marae Taputapuatea was where chiefs from across Polynesia gathered. Mā'ohi governance concepts (rāhui, tapu, mana, marae) are shared across Polynesian cultures	Verify cross-cultural governance recognition; verify Mā'ohi governance provenance can be linked to descendant culture profiles (Māori, Hawaiian, Cook Islands) for shared cultural knowledge
Oral tradition and genealogy	Genealogical knowledge (maintained by tahu'a specialists) determines authority. Oral records are primary; written records are colonial introductions	Verify genealogical authority validation; verify voice-based attestation for oral genealogical records

Mā'ohi Test Cases:

TC-MP001: Ari'i Hierarchical Authority - Precondition: Clan governance with ari'i rahi, ari'i, and ʾīato'ai roles - Action: ʾĪato'ai (under-chief) attempts to authorise agent for decision requiring ari'i rahi authority - Expected: Blocked; hierarchical authority enforced; only ari'i rahi can authorise at this level

TC-MP002: Rāhui as Temporal Scope Constraint - Precondition: Ari'i declares rāhui on lagoon fishery for 6 months - Action: Agent attempts to authorise fishing activity during rāhui period - Expected: Blocked during rāhui period; rāhui recorded with declaring authority, territory, resource, duration; automatically lifted at expiry (unlike permanent tapu)

TC-MP003: Rāhui vs Tapu Distinction - Precondition: Lagoon has both rāhui (chief-imposed, 6-month fishing ban) and tapu site (permanently sacred reef) - Action: After rāhui lifts, agent attempts access to tapu reef - Expected: Rāhui-protected area opens; tapu site remains permanently restricted. Two distinct enforcement mechanisms from single territory.

TC-MP004: Marae Governance Provenance - Precondition: Governance decision made at Marae

[Name] - Action: Record provenance - Expected: Provenance records specific marae identity, cultural significance level, and distinction between UNESCO-heritage marae and local community marae

TC-MP005: Tahu'a Domain Authority - Precondition: Tahu'a ra'au (healing specialist) registered with authority over traditional medicine knowledge - Action: Ari'i (general chief) attempts to authorise agent for traditional medicine data - Expected: Blocked; tahu'a ra'au domain authority required for this knowledge category, even though ari'i has general governance authority

TC-MP006: French Law / Mā'ohi Custom Dual Compliance - Precondition: Community data subject to both French data protection (RGPD/GDPR) and Mā'ohi customary governance - Action: Generate compliance report - Expected: Two distinct reports — French regulatory compliance and Mā'ohi cultural governance audit. Community configures which takes precedence on conflicts.

TC-MP007: Pan-Polynesian Knowledge Sharing - Precondition: Mā'ohi traditional navigation knowledge shared with Māori under inter-cultural agreement - Action: Māori governance body requests access under agreement - Expected: Access granted with both Mā'ohi and Māori governance provenance chains maintained; ancestral connection recorded; restrictions from BOTH cultures' governance enforced (most restrictive applies)

Profile 5: Wider Pacific Islander Communities Beyond the Mā'ohi ancestral culture, the broader Pacific encompasses distinct governance traditions:

Governance Element	Specific Requirement	Test Approach
Chiefly authority	Matai (Samoa), Turaga (Fiji), Ariki (Cook Islands) — chiefly roles carry governance authority	Verify chiefly role as mandatory verification for community decisions
Village-level governance	Fono (Samoa), Bose (Fiji) — village council decision-making	Verify village council as collective governance body
Diaspora inclusion	Large Pacific diaspora communities in NZ, AU, US	Verify remote participation without location requirement when configured
Oral tradition primacy	Governance decisions may be recorded orally, not in writing	Verify governance records can include voice-based attestation alongside biometric verification

Profile 6: US Native Nations — Tribal Sovereignty and USIDSN Principles The United States presents unique complexity: 574 federally recognised tribes, each a sovereign nation with distinct governance structures. Unlike other countries where Indigenous governance frameworks are national (Te Mana Raraunga for NZ, OCAP for Canada), the US has tribe-specific governance combined with the overarching USIDSN (United States Indigenous Data Sovereignty Network) and CARE Principles framework. The VAC Protocol must handle this diversity while respecting each tribe's specific governance model.

Governance Element	Specific Requirement	Test Approach
Tribal sovereignty	Each tribe is a sovereign nation with inherent right to govern its peoples, lands, resources, and data — recognised by US Constitution	Verify each tribe registers as independent sovereign trust root, not a sub-entity of US government

Governance Element	Specific Requirement	Test Approach
Governance diversity	Tribal governance ranges from elected tribal councils to traditional councils of elders, hereditary chiefs, clan-based systems, theocracies, and hybrid models	Verify governance protocol is configurable per tribe; no single model imposed
Clan systems	Matrilineal (Navajo, Hopi), patrilineal, and bilateral clan structures determine authority, membership, and decision-making	Verify clan-based authority roles; verify matrilineal/patrilineal authority paths correctly configured
Clan Mothers / Matriarchal authority	In Haudenosaunee (Iroquois) tradition, Clan Mothers nominate, oversee, and can depose chiefs (sachems); their authority is supreme in specific governance domains	Verify Clan Mother role as mandatory for specified decision types; verify deposition authority (ability to revoke chief's governance authority)
Elder/council authority	Council of elders or hereditary chiefs carry governance authority in many tribes (Cheyenne Council of Forty-Four, Pueblo religious and civic leaders)	Verify elder/council roles configurable per tribal tradition; verify both hereditary and earned authority positions
Consensus tradition	Many tribes use consensus-based decision-making (talking circles, council deliberation) rather than majority vote	Verify consensus mode with deferral; verify talking-circle model where all parties speak before decision
Sacred/ceremonial knowledge	Some knowledge is restricted by ceremony, initiation, clan, gender, or season — restrictions that vary by tribe	Verify multi-dimensional knowledge restrictions (ceremony + clan + gender + season simultaneously)
Land/territory sovereignty	Tribal data sovereignty is tied to reservation lands, treaty lands, ceded territories, and traditional territories	Verify territory-based governance; verify treaty boundary references in provenance
Federal trust relationship	Unique government-to-government relationship between tribes and US federal government creates specific data obligations	Verify dual-sovereign provenance (tribal + federal compliance); verify tribal law takes precedence for tribal data
Oral tradition and non-digital data	Indigenous data includes oral histories, songs, winter counts, calendar sticks, totem poles, communal knowledge — not just digital data	Verify governance covers non-digital knowledge representations; verify voice-based attestation for oral traditions
Native BioData	Biological and genetic data of Indigenous peoples carries special sovereignty requirements (Native BioData Consortium)	Verify biodata governance with enhanced consent requirements; verify no secondary use without tribal re-authorisation

US Native Nations Test Cases:

TC-US001: Tribal Sovereign Trust Root - Precondition: Navajo Nation registers as sovereign trust root - Action: Verify Navajo Nation governance is independent of US federal or state government trust roots - Expected: Navajo Nation governance operates as independent sovereign; federal agencies cannot override tribal governance decisions on tribal data

TC-US002: Clan Mother Authority (Haudenosaunee) - Precondition: Haudenosaunee governance with Clan Mother authority configured - Action: Chief (sachem) authorises agent for community data; Clan Mother invokes deposition authority - Expected: Chief's governance authority revoked; all VATs issued under chief's authority suspended; Clan Mother's deposition recorded in governance provenance

TC-US003: Multi-Dimensional Knowledge Restriction - Precondition: Tribal knowledge classified as: ceremony-restricted + elder-only + winter-season-only - Action: Agent attempts access in summer, operated by elder, after ceremony initiation - Expected: Access blocked (fails season restriction even though ceremony and elder requirements met); specific restriction that failed is logged

TC-US004: Consensus via Talking Circle - Precondition: Tribal council configured for talking-circle consensus - Action: 11 of 12 council members have spoken; process records each speaker - Expected: Decision NOT finalised until 12th member speaks or formally defers; talking circle recorded with speaker order and deliberation time

TC-US005: Treaty Territory Provenance - Precondition: Data governed by tribe with Treaty of [Name] territory claims - Action: Record governance provenance - Expected: Provenance includes treaty reference, territory boundaries, and distinction between reservation land, ceded territory, and traditional territory

TC-US006: Dual-Sovereign Compliance - Precondition: Tribal health data subject to both tribal law and federal trust obligation (IHS data) - Action: Generate compliance audit - Expected: Two distinct compliance reports — tribal governance audit (tribal law) and federal compliance audit (HIPAA/federal trust); tribal law takes precedence on conflicts regarding tribal data

TC-US007: Cross-Tribal Data Sharing - Precondition: Two sovereign tribes agree to share specific data categories - Action: Agent from Tribe A requests data governed by Tribe B - Expected: Tribe B's governance protocol applies; inter-tribal data sharing agreement recorded; both tribes' provenance chains maintained independently

TC-US008: Native BioData Enhanced Consent - Precondition: Genetic/biological data of tribal members under tribal governance - Action: Research institution agent requests secondary use of biodata - Expected: Secondary use blocked without fresh tribal governance re-authorisation; original consent does not extend to new use cases

Profile 7: Native Hawaiian (Kānaka Maoli) Native Hawaiians occupy a distinct legal and cultural position — Indigenous peoples of a US state (not a reservation), with unique governance traditions and an active sovereignty movement. Their governance model differs from both mainland tribal governance and Pacific Islander traditions.

Governance Element	Specific Requirement	Test Approach
Ahupua a land division	Traditional land management from mountain to sea; governance tied to watershed-based territory	Verify ahupua a-based governance boundaries; verify land-sea continuity in territory definition
Ali i authority	Traditional chiefly authority with hereditary lineage	Verify ali i role configuration with lineage verification
Kūpuna (elder) wisdom	Kūpuna authority in cultural knowledge governance	Verify kūpuna mandatory for cultural knowledge decisions

Governance Element	Specific Requirement	Test Approach
Ōlelo Hawai i (language)	Hawaiian language data carries cultural sovereignty	Verify language corpus governance; verify Hawaiian language data cannot be used for AI training without governance authorisation
Hula and cultural practice	Sacred hula, chants, and ceremonial knowledge carry specific restrictions	Verify ceremonial knowledge restrictions; verify sacred hula lineage-based access
Sovereignty movement context	Multiple governance bodies (OHA, Nation of Hawai i, others) with different legitimacy claims	Verify configurable governance authority; no single Hawaiian governance body imposed

Native Hawaiian Test Cases:

TC-NH001: Ahupua a Governance Boundary - Precondition: Governance body for specific ahupua a (watershed) - Action: Agent attempts to access data from adjacent ahupua a - Expected: Blocked; ahupua a boundary enforced; must be authorised by that ahupua a's governance

TC-NH002: Hawaiian Language Corpus Protection - Precondition: Ōlelo Hawai i language data under cultural governance - Action: AI training company agent requests language data for model training - Expected: Blocked without explicit governance authorisation; language data classified as cultural heritage requiring community governance

TC-NH003: Sacred Hula Knowledge - Precondition: Hula knowledge classified as lineage-restricted (specific hālau authority) - Action: Agent from non-authorised hālau requests access - Expected: Blocked; lineage restriction enforced; hālau governance authority recorded

Profile 8: Custom / Emerging Governance Models The framework must support governance models not yet defined. A community must be able to:

1. Register a custom governance protocol specifying decision-making rules, authority roles, data classifications, place significance, and audit requirements
2. Test their custom protocol against the generic collective governance test suite
3. Create custom test cases specific to their governance model
4. Have their custom governance model validated by the conformance testing engine

TC-CU001: Custom Governance Registration - Precondition: New community registers custom governance protocol - Action: Define roles, decision rules, data classifications, location requirements - Expected: Protocol registered; generic test suite runs against custom configuration; custom test cases can be added

TC-CU002: Custom Classification Enforcement - Precondition: Community defines custom data classification not in any predefined profile - Action: Agent attempts to exceed custom classification scope - Expected: Access blocked; custom classification correctly enforced through delegation chain

4.5 Culture-Specific Testing Metrics

Metric	Definition	Target	Method
CGP (Cultural Governance Profile Pass Rate)	All test cases in a cultural profile pass	100% per claimed profile	Run complete profile test suite

Metric	Definition	Target	Method
CSE (Cultural Scope Enforcement)	Culture-specific data classifications correctly enforced	100%	Attempt violations of tapu/noa, OCAP, knowledge restrictions
CRA (Cultural Role Accuracy)	Mandatory cultural roles correctly identified and required	100%	Attempt decisions without mandatory roles (kaumātua, elder, matai)
CAL (Cultural Audit Legibility)	Audit reports legible to cultural governance body	Verified by community review	Community representatives assess audit output
CDR (Cultural Deferral Respect)	Deferrals recorded as legitimate outcomes	100%	Trigger deferrals, verify no penalty or failure classification

4.6 Certification for Culture-Specific Governance

An implementation CANNOT claim support for a specific cultural governance model unless it passes the complete cultural governance test profile for that model. Claiming "supports collective governance" without passing culture-specific profiles is insufficient.

Certification	Requirement
Generic Collective	Passes sections 4.1–4.3 (consensus, weighted, cultural, location)
Te Ao Māori	Passes Generic + Profile 1 complete test suite
First Nations OCAP	Passes Generic + Profile 2 complete test suite
AIATSIS	Passes Generic + Profile 3 complete test suite
Mā'ohi	Passes Generic + Profile 4 complete test suite (includes rāhui/tapu distinction, French law dual compliance)
Pacific Islander	Passes Generic + Profile 5 complete test suite
US Native Nations	Passes Generic + Profile 6 complete test suite (tribe-specific configuration required)
Native Hawaiian	Passes Generic + Profile 7 complete test suite
Custom	Passes Generic + Profile 8 with community-validated custom test cases
Pan-Polynesian	Passes Mā'ohi + Te Ao Māori + Native Hawaiian + Pacific Islander (validates ancestral governance chain)

Critical principle: The community whose governance model is being tested should be involved in validating that the test profile accurately represents their governance. Technology companies should not define what "correct" Māori governance looks like — iwi should. The test profiles in this framework are starting points to be refined through community engagement, not imposed standards.

4B. Continuous Collective Validity Monitoring Testing (Claims 233–237)

4B.1 CVM Metrics

Metric	Definition	Target	Method
CCVL (Continuous Collective Validity Latency)	Time from authority change detection to quorum re-evaluation completion	<100ms	Revoke member authority, measure time to quorum decision
CCSR (Cascade-to-Safe-State Response)	Time from cascade trigger to last physical system entering safe state	<1000ms for 40-unit swarm	Trigger cascade via quorum loss, measure last-unit response
CFSC (Forensic Snapshot Completeness)	Percentage of physical systems with complete state capture at cascade moment	100%	Audit forensic records after cascade against independent state log
CRGP (Reconstitution Gap Provenance)	Gap between cascade and reconstitution is non-deletable and complete	Pass/Fail	Attempt to delete or modify gap records after reconstitution
ACLR (Authority Change Classification Rate)	Correct classification of authority change type	100%	Trigger each change type, verify classification in provenance

4B.2 Authority Change Classification Test Cases

TC-CVM-001: Voluntary Withdrawal — Above Quorum - Precondition: 7-of-7 consortium verified, threshold 5-of-7, active drone mission - Action: Member 3 voluntarily withdraws biometric consent - Expected: Member 3 removed. Quorum re-evaluated: 6/7 5/7 → operation continues. Withdrawal recorded as VOLUNTARY in provenance. No cascade. All drones continue. - Verify: Agent chain still active. Classification = "voluntary_withdrawal". Provenance event timestamp matches withdrawal time. - Validates: Claims 233, 234 - Metrics: CCVL < 100ms, ACLR = voluntary_withdrawal

TC-CVM-002: Voluntary Withdrawal — Drops Below Quorum - Precondition: 5-of-7 consortium verified (minimum quorum), active drone mission - Action: Member 3 voluntarily withdraws - Expected: Quorum re-evaluated: 4/7 < 5/7 → CASCADE. All agents suspended. All drones enter safe state. Provenance gap opens. - Verify: No agent actions after cascade timestamp. All drones in safe state. Gap marker in provenance. - Validates: Claims 233, 235, 237 - Metrics: CCVL < 100ms, CCSR < 1000ms, CFSC = 100%

TC-CVM-003: Organisational Revocation — Biometric vs Role Split - Precondition: 7-of-7 consortium verified, Member 3's biometric session active - Action: Member 3's organisation terminates their role - Expected: System detects biometric = VALID but role = REVOKED. Member removed from quorum count. Classification = "organisational_revocation". Dual check recorded in provenance. - Verify: Provenance shows both biometric and role states. System did NOT accept active biometric alone. Quorum re-evaluated correctly. - Validates: Claims 233, 234 - Metrics: ACLR = organisational_revocation

TC-CVM-004: Security Compromise — Emergency Revocation - Precondition: 7-of-7 consortium verified, active operation - Action: Member 3's session flagged as compromised - Expected: IMMEDIATE revocation. Zero grace period. ALL provenance records with Member 3's contribution flagged for forensic review. Classification = "security_compromise". Quorum re-evaluated. - Verify: No grace period observed. Forensic flags present on all dependent provenance records. Emergency revocation latency < configured threshold. - Validates: Claims 233, 234 - Metrics: CCVL < 50ms (emergency path), ACLR = security_compromise

TC-CVM-005: Incapacitation — Gradual Trust Decay - Precondition: 7-of-7 consortium verified, Member 3 active - Action: Member 3 loses connectivity, re-verification fails - Expected: Trust decays gradually per configured decay curve. Grace period timer starts. After grace period expires, member's contribution lapses. Quorum re-evaluated AFTER grace period, not immediately. Classification = "incapacitation_timeout". - Verify: Trust decay curve matches configuration. No revocation during grace period.

Quorum check triggers only after timeout. - Validates: Claims 233, 234 - Metrics: Trust decay duration matches configuration, ACLR = incapacitation_timeout

4B.3 Governance-Model-Aware Cascade Test Cases

TC-CVM-006: Threshold Governance — Above Quorum After Loss - Precondition: 7-of-7 verified, threshold 5-of-7 - Action: Members 3 and 4 lose authority (any type) - Expected: 5/7 remaining = 5/7 threshold → OPERATION CONTINUES. Reduced consortium logged. - Verify: All agents still active. Provenance shows two authority change events. Quorum status = VALID. - Validates: Claim 235

TC-CVM-007: Threshold Governance — Below Quorum After Loss - Precondition: 7-of-7 verified, threshold 5-of-7 - Action: Members 3, 4, and 5 lose authority - Expected: 4/7 remaining < 5/7 threshold → CASCADE. All agents suspended. Physical systems safe state. - Verify: Cascade timestamp. All physical systems in safe state. No agent actions after cascade. - Validates: Claims 235, 237 - Metrics: CCSR < 1000ms

TC-CVM-008: Consensus Governance — Any Member Loss Breaks Consensus - Precondition: 7-of-7 verified, consensus model (M=N, all must agree) - Action: Member 3 voluntarily withdraws - Expected: 6/7 remaining. Consensus requires ALL. → INVALIDATION. Recorded as "consensus broken — awaiting reconstitution" NOT as "system failure" or "error." - Verify: Status recorded as governance deferral. NOT error code. Reconstitution path available. 6/7 is irrelevant — consensus means consensus. - Validates: Claim 235 - Note: This is the most culturally significant test. Consensus governance traditions (whakawhitiwhiti kōrero) do not treat near-misses as agreement.

TC-CVM-009: Weighted Governance — Mandatory Role Lost, Quorum Met - Precondition: 7-of-7 verified, threshold 5-of-7, kaumātua (Member 7) mandatory - Action: Kaumātua withdraws. 6 members remain. 6 > 5 threshold. - Expected: CASCADE despite 6/7 exceeding quorum threshold. Mandatory role absence is a hard constraint. Provenance records cause as "mandatory_role_absent" not "quorum_lost." - Verify: Cascade triggered even though numbers are fine. Cause classification = mandatory_role_absent. This is the test that proves the system understands governance, not just arithmetic. - Validates: Claims 235, 211 - Note: THE critical test case. If this fails, the system is counting heads not understanding governance.

TC-CVM-010: Weighted Governance — Non-Mandatory Member Lost, Kaumātua Remains - Precondition: Same as TC-CVM-009 - Action: Non-mandatory Member 3 withdraws. Kaumātua remains. 6/7 above threshold. - Expected: Operation continues. Kaumātua still present. Reduced consortium logged. - Verify: Agents still active. Kaumātua verification still valid. Provenance records reduced consortium but no cascade. - Validates: Claim 235

4B.4 Reconstitution Test Cases

TC-CVM-011: Standard Reconstitution - Precondition: Cascade has occurred. Operation suspended. 4 remaining members. - Action: Remaining members reconvene. New member biometrically verified. New collective VAT issued. - Expected: New collective VAT. New delegation chain. Operation resumes. Provenance records complete gap: original authority → cascade → suspension → reconstitution → new authority. - Verify: Gap in provenance is non-deletable. New VAT traces to reconstituted consortium. Replacement member's biometric verification recorded. - Validates: Claim 236 - Metrics: CRGP = PASS

TC-CVM-012: Gap Integrity — Attempt to Delete Suspension Record - Precondition: Reconstitution completed. Provenance gap exists. - Action: Attempt to delete or modify the suspension/gap records - Expected: REJECTED. Gap records are permanent and non-deletable. Modification attempt itself is logged. - Verify: Gap records intact after attempt. Tampering attempt recorded in provenance. - Validates: Claims 236, 172 (monotonic growth) - Metrics: CRGP = PASS

TC-CVM-013: Reconstitution with Changed Governance Model - Precondition: Cascade occurred under 5-of-7 threshold. Reconstitution with 5-of-5 (new smaller consortium). - Action: Issue new collective VAT with different governance parameters - Expected: New VAT reflects new governance model. Old governance model recorded in provenance as historical. Agents operate under new model. - Verify: New quorum parameters enforced. Historical governance model preserved in provenance. - Validates: Claim 236

4B.5 Physical System Cascade Test Cases

TC-CVM-014: Drone Swarm Cascade — Forensic Snapshot - Precondition: 40-drone swarm under collective authority, operating across 4 sectors - Action: Quorum loss triggers cascade - Expected: All 40 drones enter safe state. Forensic snapshot captures: position, altitude, speed, heading, fuel state, mission progress for EVERY drone. Snapshot timestamps all within cascade latency window. - Verify: 40 forensic records exist. All timestamps within CCSR window. No drone actions recorded after cascade. All physical parameters captured. - Validates: Claim 237 - Metrics: CCSR $<$ 1000ms, CFSC = 100%

TC-CVM-015: Reduced Consortium — Enhanced Monitoring - Precondition: 7-of-7 verified, threshold 5-of-7, 40 drones active - Action: Member 3 withdraws (6/7, still above quorum) - Expected: Drones CONTINUE operating but with enhanced monitoring flag. Operational scope MAY be reduced as precautionary measure (configurable). All drone actions now flagged with "reduced_authority" tag in provenance. - Verify: Drones still active. Enhanced monitoring flag set. Provenance tags present. Scope reduction applied if configured. - Validates: Claim 237

TC-CVM-016: Safe State Configuration Verification - Precondition: Drone swarm with configurable safe state responses - Action: Trigger cascade. Verify each safe state option: - Config A: Hover at current position - Config B: Return to base - Config C: Land at nearest safe point - Config D: Emergency beacon - Expected: Each configuration produces correct safe state behaviour. Provenance records which safe state was configured and activated. - Validates: Claims 237, 222

4B.6 Upward Revocation Test Cases (Haudenosaunee Pattern)

TC-CVM-017: Clan Mother Revokes Chief Mid-Operation - Precondition: Haudenosaunee governance model. Chief is consortium member. Clan Mother has upward revocation authority. - Action: Clan Mother revokes Chief's authority during active operation - Expected: Chief's authority invalidated from ABOVE (not self-withdrawal, not organisational). Classification = "upward_governance_revocation". Quorum re-evaluated. If Chief held mandatory role, cascade regardless. - Verify: Provenance records source of revocation as governance hierarchy, not self or organisation. Authority flow direction = UPWARD (unique to this profile). - Validates: Claims 233, 234, US Native Nations Profile - Note: This tests the only governance pattern in the framework where authority flows upward. All other revocations flow downward or laterally.

4B.7 Double-Hit and Rapid Succession Test Cases

TC-CVM-018: Two Members Lost Simultaneously - Precondition: 7-of-7 verified, threshold 5-of-7 - Action: Members 3 and 5 lose authority within 10ms of each other - Expected: Two distinct authority change events. Each evaluated independently with separate provenance records. Quorum evaluated after each: 6/7 $\rightarrow$ 5/7. Both changes recorded. - Verify: Two provenance records, not one. Each has independent timestamp and classification. - Validates: Claim 233

TC-CVM-019: Rapid Cascade Chain — 3 Members in 5 Seconds - Precondition: 7-of-7 verified, threshold 5-of-7 - Action: Members 3, 4, 5 lose authority in rapid succession (1s apart) - Expected: First loss $\rightarrow$ 6/7 (continue). Second loss $\rightarrow$ 5/7 (continue, at threshold). Third loss $\rightarrow$ 4/7 (cascade). Each transition distinct in provenance. - Verify: Three distinct events. Cascade triggered on third loss. Provenance shows progressive deterioration. Safe state triggered once, not three times. - Validates: Claims 233, 235, 237

4B.8 CVM Conformance Certification

An implementation claiming CVM conformance must pass ALL of the following:

Category	Required Test Cases	Pass Criteria
Authority Classification	TC-CVM-001 through TC-CVM-005	All 4 change types correctly classified, differential response verified

Category	Required Test Cases	Pass Criteria
Governance-Model Cascade	TC-CVM-006 through TC-CVM-010	All 3 governance models (threshold, consensus, weighted) produce correct cascade/continue decisions
Mandatory Role	TC-CVM-009 specifically	CASCADE despite quorum met. This is a hard requirement.
Reconstitution	TC-CVM-011 through TC-CVM-013	Gap integrity, non-deletability, reconstitution path
Physical Systems	TC-CVM-014 through TC-CVM-016	CFSC = 100%, CCSR < 1000ms, safe state configuration
Rapid Succession	TC-CVM-018, TC-CVM-019	Distinct events, progressive evaluation, single cascade trigger
Metrics	All CCVL, CCSR, CFSC, CRGP	Within target values

Total: 19 test cases, 5 metrics, mandatory role test is the gateway.

---

5. Physical System Testing (Claims 218–222)

5.1 Physical System Metrics

Metric	Definition	Target	Method
KSE (Kinetic Scope Enforcement)	Physical parameter violations blocked	100%	Attempt geofence breach, altitude exceed, speed exceed
SRL (Swarm Revocation Latency)	Time from root revocation to all units halted	<2s for 100-unit swarm	Revoke root, measure last-unit response
EHL (Emergency Halt Latency)	Time from emergency trigger to safe state	<500ms per unit	Trigger emergency, measure response
PAP (Physical Action Provenance Completeness)	All physical actions fully recorded	100%	Audit provenance against independent action log

5.2 Physical System Test Cases

TC-PS001: Geofence Enforcement - Precondition: Drone agent with geofence scope constraint - Action: Agent commands drone toward geofence boundary - Expected: Movement stopped at boundary; violation logged; authority chain intact - Validates: Claim 220

TC-PS002: Scope Narrowing for Physical Parameters - Precondition: Coordinator has 500m altitude ceiling; delegates to unit - Action: Unit requests 600m altitude - Expected: Derivation rejected (exceeds parent scope); unit receives 500m ceiling - Validates: Claims 218, 220

TC-PS003: Swarm Revocation Cascade - Precondition: 50-unit swarm operating under single human authority - Action: Human revokes biometric session - Expected: All 50 units enter safe state within SRL target; provenance records cascade - Validates: Claim 219

TC-PS004: Physical Action Provenance - Precondition: Drone completes 10-waypoint survey mission - Action: Query provenance chain - Expected: All 10 actions recorded with coordinates, timestamps, altitude, speed, environmental state, and complete authority chain to human - Validates: Claim 221

TC-PS005: Emergency Override - Precondition: Active drone mission - Action: Safety officer triggers emergency return-to-base - Expected: Drone returns within EHL; override recorded with trigger condition, authority, response - Validates: Claim 222

---

6. Coalition Operations Testing (Claims 223–228)

6.1 Coalition Metrics

Metric	Definition	Target	Method
CGA (Coalition Governance Accuracy)	Correct governance model enforcement	100%	Test consensus, qualified majority, lead-nation
NCE (National Caveat Enforcement)	Caveats cannot be overridden	100%	Coalition authority attempts to exceed national caveat
CNI (Cross-National Interop Verification)	Mutual authority verification success	>99.9%	Cross-verify 100 authority chain pairs
TGB (Trust Graph Boundary Enforcement)	Trust tier boundaries respected	100%	Attempt Five Eyes data sharing with non-Five Eyes agent

6.2 Coalition Test Cases

TC-CO001: Coalition Consensus - Precondition: 5-nation coalition, consensus required for strategic decisions - Action: 4 of 5 nations authorise - Expected: Coalition VAT NOT issued; awaiting 5th nation - Validates: Claim 223

TC-CO002: National Caveat Enforcement - Precondition: Nation A contributes assets with "no offensive operations" caveat - Action: Coalition commander authorises offensive mission using Nation A assets - Expected: Delegation blocked for Nation A assets; caveat violation recorded in both coalition and Nation A provenance - Validates: Claim 226

TC-CO003: ROE as Scope Constraints - Precondition: ROE permits "observe only" for current phase - Action: Agent attempts engagement action - Expected: Action blocked by ROE scope constraint; violation logged with full authority chain - Validates: Claim 225

TC-CO004: Cross-National Interoperability - Precondition: Nation A surveillance agent, Nation B fire control agent - Action: Data sharing between agents - Expected: Both nations' authority chains verified; classification handling confirmed; dual-national audit trails created - Validates: Claim 224

TC-CO005: Trust Graph Boundaries - Precondition: Five Eyes intel sharing with NATO non-Five Eyes partner - Action: Attempt to share Five Eyes-classified data with non-Five Eyes agent - Expected: Blocked by trust graph boundary; violation logged - Validates: Claim 227

TC-CO006: Coalition Kinetic Operations - Precondition: Multi-national drone swarm from 3 nations, each with caveats - Action: Execute coordinated mission - Expected: Each unit carries both national and coalition authority chain; national caveats enforced per unit; single coalition-level provenance plus per-nation provenance - Validates: Claim 228

---

7. Graph-Based Trust Verification Testing (Claim 232)

7.1 Graph Testing Approach

The trust graph represents the complete authority structure as a directed acyclic graph (DAG):

```
Nodes: Humans, Organisations, Governance Bodies, Coalitions, Agents, Physical Systems
Edges: Delegation, Membership, Authority, Trust, Verification
Properties: Scope, Trust Score, Jurisdiction, Physical Parameters, Governance Protocol
```

7.2 Graph Testing Methodology

Path Traversal: Every path from any root (human, collective, coalition) to any leaf (agent action, physical action) is traversed. At each edge, verify: - Scope is equal or narrower than parent - Trust score is equal or lower - Jurisdiction constraints are satisfied - Physical parameters are within envelope - Governance protocol was followed

Boundary Testing: Identify all edges where a constraint boundary exists. Generate test cases for: - Exactly at boundary (should pass) - One unit beyond boundary (should fail) - Adversarial paths attempting to circumvent constraints

Adversarial Path Testing: Generate synthetic authority graphs with known vulnerabilities. Verify the testing engine detects: - Scope widening attempts - Trust inflation - Jurisdiction bypass - Caveat circumvention - Cultural protocol violation

Conformance Map Output: For each test run, produce a visual conformance map showing: - Green: Node/edge passed all tests - Yellow: Node/edge passed with warnings - Red: Node/edge failed one or more tests - Coverage percentage per section

7.3 Graph Verification Metrics

Metric	Definition	Target
GPC (Graph Path Coverage)	Percentage of paths tested	100% for critical paths
GBD (Graph Boundary Detection)	Boundary violations detected	100%
GAD (Graph Adversarial Detection)	Synthetic vulnerabilities found	100%
GVT (Graph Verification Time)	Time to verify complete graph	O(E log V)

---

8. Intelligent Orchestration and Collaborative Onboarding Testing (Claims 238–241)

8.1 Orchestration Metrics

Metric	Definition	Target	Method
ATR (Agent Team Recommendation Accuracy)	Recommended team matches problem requirements	>90% user acceptance	Natural language problem descriptions → team configs evaluated by domain experts
DBC (Dual-Purpose Biometric Capture)	Single recording yields both functional output and biometric anchor	100% dual-extraction	Capture video → verify both practice feedback AND identity hash generated

Metric	Definition	Target	Method
VCI (Vouch-as-Collaboration Initiation)	Vouch step correctly configures bilateral governance	100%	Vouch → verify identity verified AND governance established in single action
CDR (Collaboration Discovery Rate)	Eligible collaboration opportunities correctly detected	>95%	Seed 100 user pairs with overlapping scopes → measure detection

8.2 Orchestration Test Cases

TC-OR001: Problem-to-Agent-Team Recommendation - Precondition: User describes business problem in natural language - Action: Orchestration layer generates agent team recommendation with scoped authority - Expected: Each recommended agent has correctly narrowed scope; no agent exceeds requested authority; delegation hierarchy is valid VAC chain - Validates: Claim 238

TC-OR002: Scope Auto-Configuration - Precondition: Recommended 3-agent team (read-only, draft-only, read-from-both) - Action: Verify auto-generated VAT scopes - Expected: Agent 1 cannot write; Agent 2 cannot read raw data; Agent 3 cannot modify either; all enforced cryptographically - Validates: Claim 238

TC-OR003: Dual-Purpose Biometric Capture - Precondition: User records a practice session video (FolioAI-style) - Action: System processes recording for both functional feedback AND biometric anchoring - Expected: Practice reflection generated AND biometric hash extracted from same recording; biometric hash matches identity verification standards - Validates: Claim 239

TC-OR004: Biometric Capture — Single Recording, No Additional Steps - Precondition: User completes functional recording - Action: Check if user was prompted for separate identity verification - Expected: No separate identity step required; biometric verification was embedded in the functional interaction - Validates: Claim 239

TC-OR005: Vouch-as-Collaboration-Invitation - Precondition: User A vouches for User B's identity - Action: System prompts "Will you be working with this person?" — User A confirms - Expected: (1) Identity verification recorded (vouch), (2) bilateral governance configured (collaboration scope), (3) both completed in single user action - Validates: Claim 240

TC-OR006: Vouch Without Collaboration - Precondition: User A vouches for User B's identity - Action: System prompts collaboration — User A declines - Expected: Identity verification recorded (vouch only); NO governance configured; User A can later initiate collaboration separately - Validates: Claim 240

TC-OR007: Collaboration Discovery — Automatic Detection - Precondition: User A (verified, scope: financial data) and User B (verified, scope: financial reporting) both active - Action: Orchestration layer analyses scope overlap - Expected: System recommends collaboration opportunity; proposes governance model; does NOT activate until both users biometrically re-verify - Validates: Claim 241

TC-OR008: Collaboration Discovery — Biometric Gate - Precondition: Collaboration opportunity detected between User A and User B - Action: User A re-verifies biometrically; User B does not - Expected: Collaboration NOT activated; pending state recorded; User B notified of pending invitation - Validates: Claim 241

TC-OR009: End-to-End Orchestration Flow - Precondition: New user, no agents configured - Action: User describes problem → records video → gets team recommendation → vouches colleague → collaboration established - Expected: Complete flow from zero to governed multi-agent multi-user collaboration with full VAC authority chain, completed in under 10 minutes wall-clock time - Validates: Claims 238, 239, 240, 241

---

9. Testing Certification Levels

Level	Requirements	Suitable For
Basic	Core VAT tests + delegation + revocation	Development, prototyping
Standard	Basic + provenance + regulatory + multi-party	Enterprise production
Advanced	Standard + collective governance + physical systems	Regulated industries, government
Coalition	Advanced + coalition governance + trust graph	Defence, multi-national operations
Orchestrated	Coalition + intelligent orchestration + collaborative onboarding	Full platform deployment, multi-user agent teams

Each level includes all tests from lower levels. Certification is granted per level upon passing all required test suites.

---

10. Testing Tools

Reference Test Suite

- Automated test runner executing all test cases
- Configurable for different certification levels
- JSON/XML output for CI/CD integration

Graph Verification Engine

- Constructs authority graph from VAT chain
- Traverses all paths
- Generates conformance map
- Identifies boundary conditions automatically

Provenance Simulator

- Generates synthetic multi-jurisdiction chains
- Simulates regulatory changes
- Produces known-conflict scenarios for testing

Physical System Simulator

- Virtual drone/robot environments
- Geofence and constraint testing without physical hardware
- Swarm coordination verification

This testing framework is designed to become a VAC Protocol conformance standard. Implementations seeking certification must pass all applicable test suites at their target certification level.