AOS kernel control coordination

Document: aos-kernel-control-coordination-v0-1 · Source revision or record: v0.3

AOS Specifications v1.0 · Edition dated 3 November 2026

Original architecture and specifications: Mark Sweeny, Governance Intelligence. © 2026 Mark Sweeny.

AOS-authored material is licensed under Creative Commons Attribution 4.0 International (CC BY 4.0).
https://creativecommons.org/licenses/by/4.0/

Preserve third-party credits. Referenced external works remain subject to their own terms.

Canonical collection: https://www.governanceintelligence.co.uk/aos

Publication copy with editorial notices, public references and disclosure edits where applicable.

DEC-105 adopted - 29 October 2026: Current revision 0.3. Operational technical-control reliance requires declared scope/limits and accepted observed enforcement/failure/recovery evidence; build/prototype and G4/live approval gates remain separate. Decision/amendment record (../Supporting-Specifications/aos-dec-105-technical-control-limits-and-evidence-2026-10-29.md). Earlier counts/baselines are dated history; current inventory and annex addendum control catalogue navigation. Existing non-waivable rules and DEC-099-104 retained; all new cases/variants remain planned/unexecuted.

Editorial edition - 29 October 2026: Mark authorised documentary corrections D-01-09. This edition reconciles navigation, count/revision pointers, conformance links and historical scope labels; existing technical meanings, requirement/IF/decision identities and proposed/planned status are retained. The internal version below identifies the retained functional baseline; this dated editorial edition identifies the corrected document. See the current document inventory (../Supporting-Specifications/aos-current-document-inventory-2026-10-29.md) and correction record (../Supporting-Specifications/aos-documentary-corrections-2026-10-29.md). Earlier dated adoption baselines are historical snapshots; exact logical family/view revisions are in Exchange Register §4.

Version: 0.3
Date: 29 October 2026
Status: proposed logical specification; directions DEC-067-078 approved by Mark; action-4 supplement §12. No wire schema, implementation, executed verification, independent review or readiness claim.

Current supplement: §12 and Protected Reporting and Recovery v0.1 (aos-kernel-protected-reporting-and-recovery-v0-1.md) complete approved action 4; §§1-11 preserve the originating action-3 baseline and fields.

1. Scope, baseline and approved directions

This annex completes action 3 at logical kernel-document level: current controls before effects, compatible activation, applied change notifications, cumulative accounting/reservation, withholding notification and controlled resumption. It supplements Kernel Exchange Register v0.2, Core/Shared Contracts v0.3 and AOS-01-05 v0.5 against AOS-00/Map v0.17. Existing source manifest and FP v4/RP v6/GT remain governing.

Mark approved recommendations 1-4 and 6, then recommendation 5 after adding accountable notification, acknowledgement/escalation, traceable coalescing, owned delivery failure and appropriate resident updates through agreed channels. DEC-067-072 record these directions. This approval creates no organisational role appointment, numerical default, emergency permission or implementation release.

Table row 1

Decision: DEC-067
Approved rule / logical section: Bind current action, actor, evidence, authority, data use, agent configuration and limits at the last enforceable point; missing/contradictory/stale required conditions withhold dependent effect. §3.

Table row 2
Decision: DEC-068
Approved rule / logical section: Activation requires compatible applied-state evidence from components needed for the affected function; partial activation visible, unaffected valid scope may continue, restrictions prevent affected execution despite incomplete wider update. §4.

Table row 3
Decision: DEC-069
Approved rule / logical section: Track relevant changes through application/no-material-dependency/unresolved results; late/duplicate/out-of-order messages reconcile current state, missing acknowledgement remains owned, significant completed consequences reviewed. §5.

Table row 4
Decision: DEC-070
Approved rule / logical section: AOS-04 defines linked work/effect accounting semantics; AOS-05 enforces authoritative shared cumulative account; AOS-02 preserves evidence. No evasion through split agents/retries/providers. §6.

Table row 5
Decision: DEC-071
Approved rule / logical section: Reserve shared capacity before parallel effects; no double spending; confirmed effects consume capacity; release only evidenced unused capacity; partial/unknown outcomes retain conservative reservation; unavailable accounting withholds and creates accountable notification/acknowledgement/escalation, including appropriate resident update. §§6-7.

Table row 6
Decision: DEC-072
Approved rule / logical section: Scoped brakes and resumption require reconciled evidence, current controls and applicable human approval; no restart/recovery-driven replay; irreversible effects retained and followed up under authorised powers. §8.

2. Responsibilities and authoritative sources

Table row 1
Component: AOS-01
Owns / supplies: Current authority/restriction state, grant/instrument applicability, constitutional activation/approval and brake-release powers
Consumes / limitation: Identity/use, exact requests, applied-state and effect evidence; platform operation cannot create authority.

Table row 2
Component: AOS-02
Owns / supplies: Common record structure, exact evidence/assurance revisions, dependency/reference register and preserved change/accounting evidence
Consumes / limitation: Semantic-owner state; custody does not determine permissions or issue capacity.

Table row 3
Component: AOS-03
Owns / supplies: Current identity/representation, processing basis/consent/use/restrictions and permitted notification payload/audience/channel
Consumes / limitation: Authority is separate; consent cannot waive constitutional constraints.

Table row 4
Component: AOS-04
Owns / supplies: Exact task/action/attempt and configuration meaning; linked-work/effect units/grouping; effect estimates and continuing

obligations
Consumes / limitation: Current controls and runtime accounting; model estimates alone cannot establish available capacity or actual effect.

Table row 5
Component: AOS-05
Owns / supplies: Independent final gate, applied deployment/control evidence, authoritative concurrent cumulative account, reservation enforcement and observed runtime effects
Consumes / limitation: Approved authority/use/agent/profile meaning; cannot enlarge a budget or grant via administration.

Semantic owners identify exact current-state sources per organisation/function: authority/restriction from 01; identity/basis/use from 03; task/configuration from 04 plus actual applied manifest from 05; evidence/assurance revisions from 02 and source steward; balances/reservations from 05. Sources may be implemented together but their roles and evidence stay distinguishable. A replica/cache is acceptable only under an explicit currentness/fencing profile demonstrating required limits; no favourable reliance is inferred from connectivity or a timestamp alone. Role appointments, service mechanisms and clock/propagation/race settings must be commissioned before dependent conformance.

DEC-105 - declared technical control limits and observed assurance

Operational reliance on implemented technical controls requires explicit scope, limits and failure/recovery behaviour supported by accepted observed evidence. The evidence must cover all enabled action paths within the declared control/threat scope, independently of the acting agent; permission-change enforcement points and timing uncertainty; shared cumulative bounds under concurrency; conservative treatment of unknown effects/reservations; and recovery that applies current restrictions without reviving withdrawn authority or repeating completed effects.

The approved control profile fixes exact functions/paths/dependencies/versions, threat assumptions, effect boundary, currentness and revocation/fencing mechanism, timing/uncertainty bounds and units, accounting scopes/consistency and admission, uncertain exposure/release evidence, recovery source/currentness/completeness, permitted fallback/continuing duty, observability/oracle, assessors and objective acceptance conditions. Timeout, cancellation, worker retirement or failover alone cannot prove no effect, release possibly used capacity or permit consequential repetition. No instantaneous global revocation or recall of an irreversible disclosure is promised. Limits are assessed under actual constraints and powers, not silently accepted as waivers of non-waivable safeguards. Missing/failed evidence blocks affected operational-reliance claims with an owned remedy; separately authorised service/reporting duties remain owned and do not acquire extra permissions.

G3 remains authorisation of a bounded build with fixed scope, explicit dependencies/profiles and required separate review; G4 requires implemented observations, and actual operational approval is separate. An explicitly authorised bounded prototype can investigate the mechanisms before operational assurance exists; this decision itself authorises neither a prototype nor live effects. A failed prototype requires investigation of the implementation, assumptions and alternatives; it is not alone proof of architectural impossibility. Model refusal, a generated explanation, intended configuration, an old checkpoint or retrospective log alone is not evidence that all effect paths were enforced or recovery was current. Actual acceptance must link observations to the exact requirement/local-case/variant/profile and endpoint scope, with limitations and competent assessor disposition.

AOS-05 produces control-boundary/dependency observations and declares the implemented limits with authoritative semantic/control owners. AOS-40 evaluates scoped acceptance and preserves build, implementation-verification and operational approval distinctions. Approved profile/instrument owners determine legitimate settings; accountable human assessors disposition limitations without waiving non-waivable constraints.

3. Combined effect-boundary checkpoint

The executor supplies exact request revision, attempt identity, proposed observable effect, material payload/target/recipient/channel/amount/context, agent/deployment revision and all applicable cumulative scopes. The runtime gate validates the following combined evidence immediately before the defined point at which the effect can no longer be

prevented:

1. The request/actor/organisation and attempted arguments match the evaluated binding.
2. Each required authority/use/identity result is favourable for that operation, remains valid, and cites authoritative current restrictions under the accepted freshness profile.
3. The current evidence/assurance and material facts still satisfy the intended-use profile; a changed material input requires reassessment.
4. Agent/deployment/lifecycle and policy/control versions form a compatible applied set for this function.
5. Applicable cumulative scopes have valid reserved capacity and current account/fence state; all other action conditions hold.
6. The required pre-effect record and permitted observation/reconciliation path are available under the approved profile.

The output is an action/attempt-bound checkpoint receipt: pass, withhold or unresolved, with reasons and exact evidence/version vector. It is not a new organisational grant. A pass may be consumed only for its exact operation/attempt under the declared profile; duplicate receipt use cannot authorise a second effect. Every later effect/attempt requires its own valid check; multi-step workflow approval cannot cover substituted arguments. Original REC-A/D remains historical evaluation evidence; REC-X links the receipt and observed consequences.

Table row 1
Condition: All required current bindings, compatible applied state and reservations established
Gate outcome / required evidence: Pass for exact operation/attempt; record before effect; record actual outcome afterwards.

Table row 2
Condition: Authority or use denies, is unresolved/unavailable, expired or invalidated
Gate outcome / required evidence: Withhold/unresolved; identify each blocker, preserve separately authorised referral duty.

Table row 3
Condition: Material request, source fact, actor, channel or configuration changes
Gate outcome / required evidence: Reassess affected dependencies; no reuse of earlier favourable binding.

Table row 4
Condition: Partial activation, stale/contradictory current evidence or unestablished compatibility
Gate outcome / required evidence: Withhold affected scope; separately evidenced unaffected valid scope may continue.

Table row 5
Condition: Accounting/reservation state unavailable, conflicting, insufficient or not bounded
Gate outcome / required evidence: Withhold; reserve remains unresolved where prior effect possible; §7 notification.

Table row 6
Condition: Recording/checkpoint integrity unavailable
Gate outcome / required evidence: Withhold unless a separately approved equivalent boundary supplies all required evidence; no log-later default.

Table row 7
Condition: Restriction arrives before last enforceable point
Gate outcome / required evidence: Invalidate receipt/reliance and prevent affected effect under approved fence/profile; applied result evidenced.

Table row 8
Condition: Restriction/change after last enforceable point or during irreversible effect
Gate outcome / required evidence: Stop still-preventable dependent continuation, preserve crossing time/uncertainty, reconcile actual effect and initiate accountable impact review. No claim to recall a disclosure.

Each profile declares the actual boundary for each effect type, source freshness, validity/consumption, fencing/invalidation relation, interrupted-operation behavior and accepted residual race uncertainty. There is no instantaneous global revocation guarantee. If required currentness or residual race treatment is unconfigured/unevidenced, the dependent path cannot pass. Restrictive state takes precedence over old favourable checkpoint evidence; increasing permission requires the governed

approval and activation route.

4. Compatible activation and restriction fencing

An activation plan identifies affected functions, exact approved versions, required component/path set, compatibility evidence, old still-valid scope and necessary acknowledgements. Components independently report validation and actual application. The release coordinator records applied version vector for each function/path; identical revision numbers across unrelated families are not required.

State: proposed → approved → applying → compatible_active / incomplete / blocked → superseded. Approval requires empowered exact-revision human evidence where applicable. compatible_active requires every dependency needed for that function/path to attest applied compatible scope. A quorum cannot omit a required enforcement path. Failed/unreachable/inconsistent members leave affected functions incomplete/blocked; other functions can continue only with independently evidenced valid old/current scope. An approval receipt or deployment request is not application.

Restrictions and withdrawals are a separate priority path: their effective scope/version updates authoritative controls and invalidates affected reliance. The effect gate checks that restrictive state even while wider rollout is incomplete; any path unable to establish it withholds. Expansion/new permission is not activated by restrictive-first delivery. Rollback/restart cannot decrease the known restriction state or reinstate a withdrawn grant. Detection of mixed versions records an owned exception and triggers scope containment plus permitted notification.

Fences are logical current-state/version barriers or equivalent evidenced mechanisms, not a mandated database/lock topology. Their concrete race boundaries, partition behavior and propagation targets remain selected implementation/profile work.

5. Change delivery, dependency impact and application

Every governed change has exact previous/new revisions, change basis/powers, effect scope/time, semantic owner, accountable impact owner, dependency coverage and notification obligations. AOS-02 maintains the governed dependency/reference structure; semantic owners determine materiality. The impact owner cannot be inferred from an unacknowledged inbox.

Track each registered dependent consumer/path through pending → received → validated → applied / no_material_dependency / unresolved. applied names affected tasks, queues, projections/caches and actual resulting version/restriction state. no_material_dependency cites the examined scope and basis; it is not a convenient silent ignore. unresolved, rejected or overdue remains an owned exception with approved response window/cover/escalation. Human acceptance of the exception duty is separate KX-21 responsibility evidence.

Changed/corrected evidence pauses materially dependent pending work for reassessment. Completed effects retain permitted history; significant consequences have a separate impact-review owner and disposition. Unrelated valid work continues only where dependency scope is established. If materiality/coverage cannot be established, contain uncertain dependent scope and refer; do not assert no impact.

Receivers deduplicate identical revision/event content, preserve same-ID conflicting content as conflict, and compare causal/effective/current-state scope rather than arrival order. A late permissive event cannot override a later effective restriction. Unavailable consumers reconcile against authoritative state and pending obligations before renewed dependent use; sender retransmission is not proof of application. Backups/restored copies remain subject to action-4 recovery isolation/proof. Applicable consumers include AOS-05 and affected non-kernel endpoints; non-kernel commissioning/adoption is explicitly unfinished.

6. Shared cumulative account and concurrent reservations

AOS-04 profiles define linked-work identity and applicable contact/commitment/resource/scope-growth measures, independently of which worker/provider performs them. AOS-01/03 approve governing authority/use constraints; AOS-05 maintains and

enforces the authoritative account; AOS-02 retains permitted immutable revision/event evidence. Grouping cannot create otherwise prohibited resident profiling. A limit is an additional bound, never proof of ethical acceptability.

An operation may belong to several scopes simultaneously: task, case, resident/recipient, delegated agent group, commitment class and period. The exact relevant list is profile-defined. All applicable bounds must pass. AOS-04 supplies assessed effect demand with units and a conservative upper bound where outcome is uncertain; the estimate needs approved method/evidence. Missing bounded demand cannot become zero or unlimited.

For every scope, the governing invariant is confirmed consumed capacity + outstanding reserved capacity ≤ approved limit, interpreted using the profile's precise period/time and units. Unknown potential consumption remains reserved, not silently removed. Reservations across overlapping scopes must be admitted as one indivisible logical decision or equivalent mechanism preventing partial-authorisation/double-spend; a partly accepted vector grants no execution. No database transaction mechanism is imposed.

Reservation state: requested → reserved / rejected / unresolved → dispatched → committed / partially_committed / uncertain / released. Each request binds exact intended effect, attempt, linked-work identity, demand vector, account revisions, validity/fence and action profile. Only the authoritative accounting function creates valid reservation evidence. Duplicate same-identity requests return original disposition; conflicting content is rejected. Retry/provider substitution uses the same intended-effect lineage; a new attempt cannot hide outstanding prior demand.

Before effect, the gate validates the reservation remains applicable, unconsumed for a second effect and compatible with current controls/account epoch. Confirmed outcome converts corresponding reserved quantity to consumed quantity; it does not count both for the same portion. Partial effect consumes confirmed portion and retains conservatively bounded remainder until reconciled. Capacity may be released only on evidence of unused capacity under the approved rule. Expiry, cancellation, timeout, worker retirement or failover alone cannot release capacity when an effect may have occurred. An expired unused reservation still needs evidence establishing the absence of dispatched/possible effect before release.

If exposure has exceeded a bound, retain the true total/uncertainty and breach evidence, brake affected work and notify; do not adjust historical accounting to appear compliant. Period rollover carries outstanding/uncertain exposure according to an approved rule preventing reset evasion. Unconfigured rollover rules block affected admission. Human review can authorise a separately valid next action or formally governed parameter change; it cannot erase actual effects, invent capacity or waive core constraints.

When accounts are unavailable, contradictory or split across unverified replicas, withhold dependent operations and invoke §7. Independently evidenced unrelated scopes may continue. No alternate provider/account starts with an empty balance. Restored/recovered authoritative inputs and reconciliation proof remain action 4.

7. Withholding is an accountable notification duty

Every withheld consequential/dependent operation creates a governed withholding record, not merely a queue status. The approved operational profile names a functional owner, authorised minimal payload/audience/route, acknowledgement deadline, cover/escalation, service duty and disposition rights. Missing appointments/routes are commissioning blockers; runtime inability to notify remains an explicitly owned exception, not a reason to execute the blocked operation.

Record operation/task/case identity, cause, current blockers, any known/unknown previous effects, still-live reservations, time/required duty, notification owner/recipient and next review. Send through a separately authorised route; unavailable accounting must not circularly require a new successful reservation from that failed account just to record/report the failure. The fallback/reporting mechanism needs its own approved bounded authority, use scope and resource/contact treatment; no blanket reporting exemption is invented. An independently usable route and actual cover/capacity remain action-4 prerequisites.

Track attempted delivery, receipt and actual human acceptance separately. Until authorised ownership transfer is evidenced, the originating service's designated duty owner retains tracking responsibility. Missing acknowledgement invokes approved cover/escalation. Notification failure/unknown delivery creates an owned delivery exception, with permitted retained evidence and an approved human fallback where available. Logging attempted delivery does not discharge the audience obligation.

Repeated notifications may be coalesced under the approved materiality/urgency profile, but each affected operation remains linked, count/scope/oldest duty visible, and material deterioration or expiry cannot be suppressed. Coalescing is not case closure or removal of obligations.

Where withholding affects resident service, the responsible resident workflow determines and arranges an appropriate update using resident-agreed channels plus independent authority/use checks, minimum necessary content, accessible approved alternatives, actual delivery evidence and remaining duty. Do not automatically disclose sensitive blockers, promise resolution or contact via an unagreed channel. If the update cannot be delivered, retain the owned contact exception.

8. Brake and resumption

Brake states: active → braked / awaiting_reconciliation / awaiting_human → eligible_for_resume → active, or stopped/retired under existing lifecycle powers. Scope includes exact work/account/control dependencies; a brake does not automatically suspend unrelated grants. Trigger, owner, reason, restrictions, continuing duties and evidence are recorded. AOS-05 applies technical withholding within approved powers; AOS-01/03 remain authoritative for permission and processing; AOS-04 coordinates task disposition.

Resume eligibility requires authoritative current control state, compatible applied configuration, corrected dependencies, reconciled prior effects and reservations, reliable accounting, valid duty/notification disposition and necessary approval by an empowered human. Human approval is required where the approved profile reserves it; safe automatic resumption is possible only when that same profile explicitly permits it and all evidence is present. A previously valid checkpoint/reservation is not a new resume authority.

Each held operation gets fresh exact binding/checkpoint/account admission before execution. Already confirmed effects are not repeated. Unknown effects remain awaiting authorised reconciliation; compensation/status queries/contact each need their own permissions. Service restoration or restart alone cannot replay the queue. Irreversible effects and unresolved service/resident duties stay visible to authorised follow-up; an acknowledged notification is not completion of the underlying work.

9. Single common records and field mappings

REC-X / CHECK ownership clarification - 29 October 2026: AOS-04 owns the enclosing REC-X execution meaning; AOS-05 owns/supplies the runtime combined CHECK evidence. The existing REC-X.final_control_check references CHECK, while observed effects are recorded separately. AOS-02 supplies common structure/custody. See the current Exchange Register §4 (aos-kernel-exchange-register-v0-1.md) for family/view revisions and owners. No field, owner or runtime obligation is changed by this cross-reference.

All records use Core v0.3 header and Register v0.2 §3 types: R required scalar, C conditionally required, refs exact revision collections, scope approved typed boundary, time precision-preserving date/timestamp, quantity value/unit/range. Collections are R 0..n unless explicitly 1..n; empty requires a profile-allowed reason. No record carries secret values or unrestricted private payloads.

Table row 1
Record / owner: CHECK / AOS-05, KX-04 checkpoint view
Required logical fields: checkpoint_id/ref, exact request/attempt, actor/organisation, actual argument binding, control result refs 1..n, source-currentness evidence refs 1..n, applied version vector, relevant evidence/assurance refs, profile, boundary/time, outcome (pass/withhold/unresolved), reasons/limits
Conditional fields / result and linkage: Reservation refs for every governed cumulative scope; pre-effect recording ref where consequential; known restriction/change refs. REC-X.final_control_check references CHECK, later effect separate.

Table row 2
Record / owner: ACT / AOS-01, KX-05 activation view
Required logical fields: plan_id/ref, exact approved change, affected function/path scope, required member refs 1..n, compatibility refs

1..n, requested/applied version vectors, status (proposed/approved/applying/compatible_active/incomplete/blocked/superseded), owner/time
Conditional fields / result and linkage: Exact KX-06 approval; KX-21 validation/application from each required member; restrictive fence and still-valid old scope; unresolved-duty refs.

Table row 3
Record / owner: CHG / AOS-02 structure, KX-13
Required logical fields: exact change/event ref, old/new refs, semantic owner, impact owner, effective scope/time, powers/basis refs 1..n, dependent target refs, coverage/limitations, disposition
Conditional fields / result and linkage: Per-target receipt/validation/application/no-material-dependency/unresolved records; reassessment links for pending effects; significant completed consequence human review; notification/cover obligations.

Table row 4
Record / owner: ACC / AOS-05, new KX-24
Required logical fields: account_id/ref/revision, organisation, scope vector with keys/period boundaries/profile refs 1..n, approved limits/demand units, consumed/reserved/unknown exposure vectors, authority/use constraints, source/fence state, reconciliation evidence, status (current/unavailable/conflicted/breached/reconciling)
Conditional fields / result and linkage: Rollover/overlap rule; source predecessor/transfer for changed provider/account; unknown exposure owner and permitted evidence. Balance is not permission.

Table row 5
Record / owner: RSV / AOS-05, new KX-25
Required logical fields: reservation_id/ref, intended-effect identity, task/attempt/delegation lineage, exact scopes/account revisions, demand vector/upper-bound evidence, fence/validity, result/state, transaction/equivalent admission evidence
Conditional fields / result and linkage: Dispatch/effect refs; confirmed consumption, residual reserved quantity, release evidence and reconciliation; no release solely on expiry/cancellation.

Table row 6
Record / owner: WHD / AOS-04 duty meaning, new KX-26
Required logical fields: operation/task/case refs, withheld reason/time, blocker/effect uncertainty refs, reservation status, operational owner, authorised notification profile/recipient, remaining service duty, acknowledgement/cover deadlines, tracking owner and disposition
Conditional fields / result and linkage: Coalesced notification membership; KX-07 handoff/KX-21 receipt/responsibility; failed/unknown delivery exception; resident-update need/basis/agreement/attempt refs; no-route limitation.

Table row 7
Record / owner: BRK / AOS-04, KX-16 lifecycle/task view
Required logical fields: brake_id/ref, exact affected scope, trigger/control/account evidence, owner/power, state, remaining obligations
Conditional fields / result and linkage: Resume criteria/evidence/profile, empowered human decision when required, fresh checkpoint/reservation or continued withholding; no automatic queue replay.

Existing REC-A/D contain current-state source/evaluated profile refs; actual combined-state CHECK is REC-X-linked, not a rewrite of original determination. REC-E/Q corrections use CHG. KX-21 application identifies target scope/version and evidence; responsibility identifies an empowered human/duty scope. KX-24/25/26 are local controlled definition keys, not newly approved IF numbers.

Table row 1
Definition revision: KX-24 v0.1 cumulative account
Owner / producer → reciprocal kernel consumers: AOS-05 accounting control → 01/02/03/04/05 within permitted scope
Supporting CON views / full allocation: AOS-01-CON-001/004; 02-CON-005; 03-CON-002/004; 04-CON-002/003/004; 05-CON-002/006.

Table row 2
Definition revision: KX-25 v0.1 reservation/effect reconciliation
Owner / producer → reciprocal kernel consumers: AOS-05 authoritative registrar, 04 demand/effect semantics → 01/02/03/04/05
Supporting CON views / full allocation: Same dependent control/execution CONs as KX-24; 04-CON-007 and 05-CON-007 consume cancellation/failover state.

Table row 3

Definition revision: KX-26 v0.1 withholding notification
Owner / producer → reciprocal kernel consumers: AOS-04/service duty workflow plus 05 blocker evidence → 01/02/03/04/05 as permitted; 13/30 accountable human and resident workflow dependencies
Supporting CON views / full allocation: AOS-01-CON-004; 02-CON-005; 03-CON-007; 04-CON-005; 05-CON-004; KX-07/14/21.

10. Obligations, source traceability and planned verification

KCR obligations are proposed annex records, not approved component REQ wording. Sources: FP v4 §4 transparency/§5 imperfection/§6 humility/§7 no-exit/§10 emergence; RP v6 domain 1 accountable follow-up, domain 7 audit/uncertainty, domain 8 contextual explicit authority, domain 9 purpose limits; GT M1.13; DEC-028-030/041/056 and DEC-067-072. Component v0.5 §19.3 supplies exact new REQ/VER/CON/field chains; matrix v0.3 records these allocations without promoting original source status.

Table row 1
Obligation: KCR-01
Single required behaviour / common field: The effect gate shall withhold a dependent operation without exact current compatible CHECK evidence. CHECK binding/source/version/outcome; DEC-067.
Planned case: KCV-01/02

Table row 2
Obligation: KCR-02
Single required behaviour / common field: Affected activation shall require applied compatible evidence from every required function/path dependency, with restrictive state enforced during incomplete rollout. ACT/CHG; DEC-068.
Planned case: KCV-02

Table row 3
Obligation: KCR-03
Single required behaviour / common field: A material change shall track every dependent consumer through evidenced application/no-material-dependency or an owned unresolved exception. CHG/KX-21; DEC-069.
Planned case: KCV-03/04

Table row 4
Obligation: KCR-04
Single required behaviour / common field: Each cumulative scope shall use authoritative accounting covering linked work across agents/attempts/providers. ACC scope/demand/account refs; DEC-070.
Planned case: KCV-05/06

Table row 5
Obligation: KCR-05
Single required behaviour / common field: Concurrent admission shall reserve all applicable capacity without double spending before the dependent effect. RSV scope/vector/admission; DEC-071.
Planned case: KCV-05

Table row 6
Obligation: KCR-06
Single required behaviour / common field: Partial/unknown effects shall retain conservatively bounded exposure until unused capacity is evidenced. RSV effect/residual/release/ACC rollover; DEC-071.
Planned case: KCV-06

Table row 7
Obligation: KCR-07
Single required behaviour / common field: Withholding shall create an owned notification/handoff duty with acknowledged responsibility, cover/escalation and appropriate permitted resident update. WHD/KX-07/14/21; DEC-071.
Planned case: KCV-07/08

Table row 8
Obligation: KCR-08
Single required behaviour / common field: Resumption shall require reconciled evidence/current permissions and applicable approval without automatic replay. BRK/CHECK/RSV; DEC-072.
Planned case: KCV-04/08

Table row 1
Planned case: KCV-01 Action substitution and restriction race
Input / required expected result / evidence: Alter recipient/payload/configuration, withdraw permission before/after enforceable boundary and lose a current-state source. Before-boundary affected effects blocked; irreversible crossing/limitations and follow-up recorded; no claim of global instantaneous revocation. CHECK/REC-X/CHG evidence.

Table row 2
Planned case: KCV-02 Partial activation
Input / required expected result / evidence: Required dependency applies wrong/new/old/unreachable version; impose a restriction during rollout. Affected path blocked, compatible unaffected scope alone continues; every required applied state evidenced. ACT/KX-21/CHECK.

Table row 3
Planned case: KCV-03 Delivery versus application
Input / required expected result / evidence: Duplicate/conflicting/out-of-order changes, missing receiver and validation without application. Old permission not revived; per-consumer application/no-dependency basis or owned exception, timeout/cover visible. CHG/duty evidence.

Table row 4
Planned case: KCV-04 Pending and completed impact
Input / required expected result / evidence: Correct evidence affecting one queued operation and one significant completed effect; restart paused work. Selective pending reassessment, completed history/impact review, no automatic replay; new CHECK and approval where required.

Table row 5
Planned case: KCV-05 Concurrent overlapping limits
Input / required expected result / evidence: Two workers attempt to consume the same remaining allowance across case/group/period scopes; include duplicate reservation and provider switch. Only admissible vector proceeds; no partial-capacity grant/double spend/reset evasion; ACC/RSV attribution and observations.

Table row 6
Planned case: KCV-06 Partial/unknown accounting
Input / required expected result / evidence: Cancel/expire/failover an attempt after possible effect; cross period boundary with outstanding reservation. Confirmed portion consumed, uncertain remainder held; no timeout/cancellation release or zero-balance replacement account; bounded estimates and actual release proof.

Table row 7
Planned case: KCV-07 Withheld operation notification
Input / required expected result / evidence: Accounting fails; notify operational owner, omit acknowledgement and fail primary route; repeat failures coalesced. Dependent effect blocked, separate permitted reporting attempted, owner/cover/escalation and every affected operation visible; failed delivery remains owned. No assertion that independently usable route exists until action 4 commissioned.

Table row 8
Planned case: KCV-08 Resident update and resume
Input / required expected result / evidence: Service affected, notification acknowledged but task unresolved; attempted unagreed channel or sensitive over-disclosure; then propose restart/resume with unresolved effects. Only appropriately permitted agreed-channel update; contact failure owned; acknowledged handoff not service completion; no replay without current controls/reconciliation/required approval.

11. Author review and remaining commissioning

Logical action-3 responsibility/record/failure rules are drafted and reciprocally adopted by AOS-01-05 v0.5. KR-02/03/06 are reconciled at that document level, subject to review. No test was executed, concrete implementation selected or role/time value invented. Checkpoint source/epoch/profile values, actual distributed admission mechanism, effect estimates and period rules, permitted operational/resident notification routes/people/capacity, privacy assessment, wire schemas and measured acceptance remain build/activation dependencies. Record/notification/recovery common-failure handling and authoritative recovered state proof remain action 4 (KR-04/05). Non-kernel endpoint adoption remains item 6. Author structural/source/REQ/VER/reciprocal-reference checks supply document evidence only.

12. Action-4 protected reporting and recovery supplement

Baseline at this dated adoption step: AOS-00/Map v0.18; AOS-01-05 v0.6; Core/Shared v0.4; Exchange Register v0.3; Control Coordination v0.2. Protected Reporting and Recovery v0.1 (aos-kernel-protected-reporting-and-recovery-v0-1.md) is the single current protocol/dictionary for approved DEC-073-078. It completes §7 failed-reporting duty and §8 restored-state proof; former action-4 dependencies in §§1-11 are historical logical-design gaps, while actual commissioned mechanisms and evidence stay open. WHD v0.2 adds protected route/handoff references, KX-19 protected_finding v0.2 adds separately permitted route/recipient/custody and distinct responsibility states, KX-20 recovery v0.2 adds integrity/currentness/completeness and scoped acceptance. Other CHECK/ACT/CHG/ACC/RSV semantics and declared definitions retain standing.

An unavailable route cannot waive tracking duty or permit extra processing. Recovery cannot release uncertain reservation, revive prior powers or replay known effects. Fresh CHECK/reservation and empowered scoped acceptance remain required. Sources/derivation, planned compound cases, fields and reciprocal CONs are the reporting/recovery annex §§5-7; ISO scope alignment is explicitly distinguished from verified clause derivation. No actual route or recovery case has been executed.