AOS kernel protected reporting and recovery

Document: aos-kernel-protected-reporting-and-recovery-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.

DEC-104 adopted - 29 October 2026: Current revision 0.2. Each mandatory protected-finding category requires assessed technical-failure and implicated-person interference arrangements with an appropriately independent authorised alternative and no implicated sole release gatekeeper. Decision/amendment record (../Supporting-Specifications/aos-dec-104-protected-reporting-and-implicated-recipients-2026-10-29.md). External reporting is conditional on justified lawful authority, not a default. Exact profiles/permissions, protected_finding v0.3 compatibility and actual evidence remain gates; amended wording retains ordinary separate review and cases are planned/unexecuted. Earlier contrary or narrower baselines are history for this scope.

Version: 0.3
Date: 29 October 2026
Status: proposed logical specification; Mark approved all six action-4 directions and requested standards references. No implementation, executed verification, independent assurance, certification or readiness claim.

1. Scope and approved direction

This annex completes KR-04/05 at logical kernel-document level. It extends control coordination; a failed control withholds dependent operations while an independently authorised notification duty survives. Recovery restores demonstrably current governed state before affected operation. The source principles/architecture remain governing; standards support design and do not supply organisational powers.

Current baseline: AOS-00/Map v0.18; AOS-01-05 v0.6; Core/Shared v0.4; Exchange Register v0.3; Control Coordination v0.2. Six directions DEC-073-078 are approved; exact fields, requirements and profiles remain proposed. Earlier directions DEC-062-072 retain standing.

Table row 1
Decision / obligation: DEC-073 / KPR-01
Approved direction: Protected fallback reporting: Provide a separately authorised protected reporting route with assessed failure independence, separately governed credentials, permitted payload, recipients and custody; common dependencies stay visible and administration cannot silently remove the reporting duty.

Standard provenance: STD-05 CP-8/CP-8(2)/(3), IR-6/IR-8; STD-01/02/03/04 scope alignment

Table row 2
Decision / obligation: DEC-074 / KPR-02
Approved direction: Minimal advance reporting permission: Approve bounded minimum failure-reporting permission and independently verifiable recipients in advance. Failure of normal controls does not grant emergency access or widen processing permission.
Standard provenance: STD-05 AC-6; STD-03/04 scope alignment

Table row 3
Decision / obligation: DEC-075 / KPR-03
Approved direction: Acknowledged human handoff: Designate a functional recipient, response deadline, cover and escalation. The tracking owner retains responsibility until explicit acceptance; failed delivery creates an owned unresolved exception and approved human fallback. Affected residents receive appropriate permitted updates through agreed channels.
Standard provenance: STD-05 IR-6/IR-8; STD-01 scope alignment; AOS-specific acceptance/continuing duty

Table row 4
Decision / obligation: DEC-076 / KPR-04
Approved direction: Recoverable authoritative current-state evidence: Preserve recoverable authority withdrawals, consent/use changes, restrictions/deletions, configuration approvals and effect/reservation evidence. Prove integrity, currentness and completeness for the affected scope; a protected stale copy or gap cannot support dependent release.
Standard provenance: STD-05 CP-9/CP-9(1), AU-9; STD-02/03/04 scope alignment; AOS-specific currentness/completeness

Table row 5
Decision / obligation: DEC-077 / KPR-05
Approved direction: Isolated restoration and reconciliation: Restore in isolation with normal processing/effects disabled; apply current restrictions/deletion dispositions, validate configuration/contracts, reconcile completed/partial/unknown effects and reservations, and preserve remaining duties. Restoration cannot revive grants, hidden deleted payload or repeated known effects.
Standard provenance: STD-05 CP-10/CP-10(2)/(4)/(6); STD-01/02 scope alignment; AOS-specific current restriction/effect gate

Table row 6
Decision / obligation: DEC-078 / KPR-06
Approved direction: Scoped accepted recovery and compound verification: Require accepted evidence and approved release powers for each scope; human acceptance when compromise, unresolved consequences or the profile requires. Bounded automatic recovery needs explicit prior approval and evidence. Test compound failures including failed fallback; technical restoration does not complete service duties.
Standard provenance: STD-05 CP-4/CP-4(4); STD-01/02 scope alignment; AOS-specific release/duty gate

2. Responsibilities and continuity profiles

Table row 1
Component: AOS-01
Authoritative responsibility: Reporting/release powers, current grants/withdrawals and protected change approval
Required reciprocal evidence: Use permission, exact route/scope and accepted current-state proof; operation does not create powers.

Table row 2
Component: AOS-02
Authoritative responsibility: Common records, permitted protected custody, source-coverage and integrity evidence
Required reciprocal evidence: Owner-produced current state and lifecycle disposition; custody cannot attest semantic currentness by itself.

Table row 3
Component: AOS-03
Authoritative responsibility: Minimum permitted data use, recipient assurance, current consent/basis/restrictions/deletion scope
Required reciprocal evidence: Route and disclosure content, authoritative current use state and actual applied disposition.

Table row 4
Component: AOS-04
Authoritative responsibility: Exact task/effect lineage, continuing duties, handoff and no-replay semantics
Required reciprocal evidence: Runtime effects/reservations, current controls and empowered scoped acceptance.

Table row 5
Component: AOS-05
Authoritative responsibility: Route operation/dependency assessment, isolation/restore, runtime validation and enforced scoped release
Required reciprocal evidence: Authority/use/configuration/state evidence from 01-04, human acceptance where required.

Each organisation/function needs an approved continuity profile before use, including the DEC-104 class-specific technical-failure and implicated-person interference assessment, authorised appropriately independent alternate recipient/release controls and owned inadequate-route disposition: reporting purposes/triggers; separately governed permissions/credentials/recipient-verification sources; minimal payload and custody; route dependencies and failure/compromise assumptions; route-change powers; functional tracking owner/recipient/cover/escalation; acknowledgement and escalation times; approved human fallback and resident communication; source scope and completeness/currentness acceptance criteria; restore isolation; required validators and empowered releasers; bounded automatic eligibility; recovery objectives with units and evidence; planned exercises and review. Unset fields block reliance on that profile. Functional roles are specified here; actual people, times and services are not appointed or invented.

“Independent” is assessed against the declared failure scenario, including identity, permission, connectivity, provider, keys, monitoring, custody and human availability. A different endpoint with the same failing dependency is insufficient. Route permission or disabling changes need the approved governance/change record and surviving reporting/exception duty. No single universal topology or always-working route is promised.

DEC-104 - protected reporting under failure and implicated-person interference

Each mandatory protected-finding category shall have an approved reporting arrangement assessed against both technical failure and interference by implicated people. The profile shall identify the intended recipient, possible conflicts and an appropriately independent authorised alternative; an implicated person shall not be the sole gatekeeper deciding whether the required finding reaches its authorised audience.

Authority/use permissions, minimum report content, recipient verification, custody, route/change dependencies, tracking ownership, acceptance, cover and escalation are established in advance. An external route is included where justified and lawfully authorised; external reporting is not a universal default and a finding creates no extra disclosure power. Planned exercises address failed infrastructure, unavailable/implicated recipients, apparent alternatives controlled by the same implicated gatekeeper and attempted suppression. Missing adequate arrangements remain an explicit owned gap, prevent claims of operational protected-reporting assurance and withhold affected dependent reliance under existing gates; they do not create false delivery, ownership transfer or blanket shutdown of separately authorised service. Original tracking duty persists until actual scoped acceptance.

The organisation’s profile binds each required finding class to normal/alternate authorised audiences, conflict criteria/evidence and accountable assessment, disclosure basis/minimal payload, independently verifiable recipients/permissions, credentials/custody and route/reconfiguration controls, failure/compromise assumptions, tracking/cover/escalation, human fallback, evidence and review triggers. Test both infrastructure/common-dependency independence and organisational release/recipient/custody control; neither implies the other. No administrator, executive sign-off or report-validation step may silently remove a required duty. The declared threat/governance scope and residual limitations must be visible: this is not an unlimited guarantee against every holder of legal/constitutional change powers. Inadequacy returns to an empowered accountable reviewer; the reporting agent cannot invent a recipient or grant itself onward-disclosure authority.

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. Protected reporting protocol

1. Record the incident/withheld scope, exact operations, known effects/uncertainty and tracking owner; block affected effects through existing CHECK/brake rules. Preserve minimal permitted evidence if normal custody is unavailable, subject to the approved profile.
2. Verify the applicable advance authority and use permission, purpose, validity and audience through independently usable approved evidence. Verify the intended recipient; select minimal permitted payload and approved route/custody. Do not send secret values. Failure of normal controls grants no additional data access. If required evidence is unavailable, withhold unauthorised transmission and retain the owned exception/approved human fallback.
3. Assess recipient/release/custody conflicts against the approved class profile. An implicated person cannot be the sole gatekeeper for the required authorised audience. Use the approved appropriately independent alternative when the normal recipient/route is implicated, unavailable, compromised or suppressing the finding; do not wait for that implicated party’s discretionary approval. Attempt only separately permitted routes within evidenced validity. Record attempt/delivery/receipt/validation separately from explicit human responsibility acceptance. Duplicate/coalesced reporting links every operation and preserves each deadline and remaining duty.
4. The functional tracking owner retains the duty until an empowered human accepts the specified responsibility with scope, identity, time, cover and remaining duties. Delivery receipts and automatic acknowledgements cannot constitute this acceptance. Missed response activates configured cover/escalation. Rejection or expired acceptance returns to an explicitly owned unresolved state; no ownerless transfer.
5. If all technical routes fail, retain an owned unresolved exception and execute the approved human fallback when permitted. Surface the failure to the accountable reviewer through any remaining approved mechanism; never record success without evidence. Arrange appropriate permitted resident updates through agreed channels via the accountable service workflow. Technical report delivery, accepted responsibility and service completion stay distinct.

4. Controlled recovery protocol

1. Restore candidate copies/configuration in an isolated environment with normal processing and external effects disabled. Minimal validation processing has its own bounded authority/use permission and protected custody. Record provider/data-flow/location constraints and unresolved compromise.
2. Establish required authoritative scope: authority/restriction/withdrawal from 01; identity/consent/basis/use/lifecycle disposition from 03; approved task/configuration/effect meaning from 04; actual applied configuration, observed effects and account/reservations from 05; common evidence/provenance from 02. A protected backup is an input, not automatically current truth.
3. Prove integrity, currentness and completeness across the restore point and every material subsequent change for the proposed scope. Identify source lineage/revisions, coverage boundaries, independent acceptance evidence and gaps. Timestamp/checksum alone is insufficient; a forged, compromised, inaccessible or incomplete source blocks dependent release. Source mechanisms, cutover fences and completeness proof are commissioned choices, not inferred from replica health.
4. Apply current withdrawals/restrictions and deletion dispositions to every declared applicable restored copy/derived index/memory before normal use. If mandatory disposition cannot yet be proved, retain permitted isolation and an owned remediation obligation. Do not retain a hidden deleted payload in history under the guise of evidence; preserve only separately permitted minimal disposition evidence.
5. Validate exact software/model/tool/schema/control/profile compatibility and accepted configuration against actual applied state. Reconcile completed, partial and unknown attempts/effects and authoritative reservations across providers and periods. Known completed effects are not replayed; uncertain residual exposure remains conservatively reserved until evidence supports release. Neither rollback nor an idempotency claim proves that an external effect did not happen. Continue service and disclosure duties.
6. Submit a scope-specific recovery evidence package to the designated validator/releaser. Record acceptance/rejection/unresolved state, actual powers, applicable human decision, limitations and remaining duties. Compromise, material unresolved consequences or profile conditions require empowered human acceptance. Human acceptance cannot waive missing mandatory current-state/use evidence. Automatic recovery is limited to explicitly preapproved eligible scope with required evidence; otherwise block dependent release.
7. Apply only accepted release scopes, record enforcement/compatible applied state and obtain fresh CHECK and necessary reservations before task continuation. Prove no material dependency for unaffected scopes released separately. No recovered queue is replayed merely because infrastructure is available. Rejected/unresolved scopes retain isolation/brakes and owners. Service duties require their own completion evidence.

5. Single common field definitions and CON views

Use the existing envelope and exact-version compatibility rules; refs carry governed identifiers, not secret/payload copies. R means required; C means conditional, with the condition explicit. Missing mandatory evidence yields unresolved/blocked, not a favourable default. These are logical fields, not approved wire schemas or new IF allocations.

Table row 1
View / declared revision: KX-19 protected_finding v0.3
Logical required fields: R finding/withheld-operation refs; affected scope; evidence/uncertainty; tracking owner; continuity-profile revision; route/dependency assessment including class-specific technical-failure and implicated-recipient/release/custody interference, approved conflict disposition and appropriately independent authorised alternative evidence; authority/use permission refs and validity result; recipient identity/verification source/result; minimal governed payload ref/classification; permitted custody; attempts and distinct receipt/validation/responsibility states; remaining duties
Conditional fields and rule: C fallback attempt and failure basis; cover/escalation; human-fallback action; resident-update/channel-agreement evidence. Unverified permission/recipient blocks transmission, not tracking duty.

Table row 2
View / declared revision: KX-20 recovery v0.2
Logical required fields: R recovery/restore/incident refs; exact proposed scope; isolated applied state; backup/source lineage and restore point; required authoritative source set/revisions; integrity/currentness/completeness result and evidence per scope; change-coverage boundaries/gaps; applied lifecycle dispositions; configuration/contract validation; effects/account/reservation reconciliation refs; outstanding duties/owners; profile; acceptance and applied-release state
Conditional fields and rule: C compromise evidence, unknown effects, source gap, human decision/powers, automatic-eligibility evidence, rejection/remediation and resident duties. Missing proof blocks dependent release; acceptance cannot erase unknown effects.

Table row 3
View / declared revision: KX-26 WHD v0.2 extension
Logical required fields: R existing operation/blocker/task/duty links, tracking owner and separately permitted notification; KX-19 report refs; distinct responsibility acceptance and remaining-duty states
Conditional fields and rule: C fallback/cover/escalation/human-fallback/resident-update refs. §3 completes its failed-route protocol; underlying operation and case states stay separate.

Other KX/REC fields retain their declared revisions. KX-15 lifecycle dispositions are consumed unchanged but gain the recovery proof obligation in §4. KX-19 health/incident and KX-20 release/supplier views retain their earlier fields; only named protected_finding/recovery views add these required fields. Compatibility assessment must identify views and exact versions.

Table row 1
Kernel endpoint: AOS-01
Existing CON views: AOS-01-CON-001/002/003/004
Reciprocity: See §2: semantic owner produces current scope evidence; protected/recovery consumers validate and acknowledge actual application/responsibility; 02 preserves permitted records, 05 returns enforced release evidence to 01-04.

Table row 2
Kernel endpoint: AOS-02
Existing CON views: AOS-02-CON-001/003/004/005/006
Reciprocity: See §2: semantic owner produces current scope evidence; protected/recovery consumers validate and acknowledge actual application/responsibility; 02 preserves permitted records, 05 returns enforced release evidence to 01-04.

Table row 3
Kernel endpoint: AOS-03
Existing CON views: AOS-03-CON-002/003/004/005/006/007
Reciprocity: See §2: semantic owner produces current scope evidence; protected/recovery consumers validate and acknowledge actual application/responsibility; 02 preserves permitted records, 05 returns enforced release evidence to 01-04.

Table row 4
Kernel endpoint: AOS-04
Existing CON views: AOS-04-CON-003/004/005/006/007/008
Reciprocity: See §2: semantic owner produces current scope evidence; protected/recovery consumers validate and acknowledge actual application/responsibility; 02 preserves permitted records, 05 returns enforced release evidence to 01-04.

Table row 5
Kernel endpoint: AOS-05
Existing CON views: AOS-05-CON-001/002/004/005/006/007
Reciprocity: See §2: semantic owner produces current scope evidence; protected/recovery consumers validate and acknowledge actual application/responsibility; 02 preserves permitted records, 05 returns enforced release evidence to 01-04.

Non-kernel AOS-13/20/25/30/service-resident endpoints remain named dependencies: read their current materials and perform explicit adoption before claiming end-to-end conformance. An annex does not appoint a staffed recipient.

6. Planned verification and source allocation

Table row 1
Case: KPV-01
Adversarial fixture and required evidence: Primary runtime, identity lookup and reporting fail; normal recipient/release controller is implicated or attempts suppression. Present a supposed alternative sharing the failed technical dependency or implicated sole release gatekeeper, then a valid appropriately independent authorised alternative. Assess class-specific authority, minimal content, verified audiences, custody/change controls, actual attempts and distinct acceptance. No shared-failure/sole-implicated gate is accepted as independent; missing adequate arrangements are owned gaps with no operational assurance claim, false delivery or widened disclosure.
Kernel linked requirement / VER ranges: 01: REQ-058/VER-035; 02: REQ-061/VER-039; 03: REQ-056/VER-040; 04:

REQ-060/VER-045; 05: REQ-064/VER-053; DEC-104

Table row 2
Case: KPV-02
Adversarial fixture and required evidence: Reporting permission and recipient invalid: Expired/wrong-scope advance permission, unverified recipient or excessive content; refuse unauthorised payload, retain minimal permitted fallback if valid, otherwise owned unresolved duty; no emergency grant.
Kernel linked requirement / VER ranges: 01: REQ-059/VER-036; 02: REQ-062/VER-040; 03: REQ-057/VER-041; 04: REQ-061/VER-046; 05: REQ-065/VER-054

Table row 3
Case: KPV-03
Adversarial fixture and required evidence: No human accepts and fallback also fails: Receipt without responsibility acceptance, absent cover, escalation failure and repeated linked reports; original tracking owner persists, all affected work traceable, approved human fallback/owned exception and resident-channel duty remain visible.
Kernel linked requirement / VER ranges: 01: REQ-060/VER-037; 02: REQ-063/VER-041; 03: REQ-058/VER-042; 04: REQ-062/VER-047; 05: REQ-066/VER-055

Table row 4
Case: KPV-04
Adversarial fixture and required evidence: Protected backup is stale or incomplete: Valid integrity check but omitted withdrawal/consent/deletion/change or uncertain source coverage; dependent release blocked until scope-specific currentness and completeness are established from authoritative evidence.
Kernel linked requirement / VER ranges: 01: REQ-061/VER-038; 02: REQ-064/VER-042; 03: REQ-059/VER-043; 04: REQ-063/VER-048; 05: REQ-067/VER-056

Table row 5
Case: KPV-05
Adversarial fixture and required evidence: Restore contains old permission and uncertain effects: Isolated old snapshot with deleted/restricted payload, completed/partial/unknown effects, uncertain reservation and incompatible config; no normal effects, apply dispositions and reconcile exposure, no repeated known effect or hidden retained payload.
Kernel linked requirement / VER ranges: 01: REQ-062/VER-039; 02: REQ-065/VER-043; 03: REQ-060/VER-044; 04: REQ-064/VER-049; 05: REQ-068/VER-057

Table row 6
Case: KPV-06
Adversarial fixture and required evidence: Premature selective release under compound failure: Combine compromise, incomplete current-state evidence, outstanding handoff and provider failover; reject unsupported automatic/human release, accept only evidenced approved unaffected scope, preserve unresolved duties and require fresh CHECK/reservation for continuation.
Kernel linked requirement / VER ranges: 01: REQ-063/VER-040; 02: REQ-066/VER-044; 03: REQ-061/VER-045; 04: REQ-065/VER-050; 05: REQ-069/VER-058

All cases are planned. Use authorised synthetic data and approved exercises; record exact fixture/profile/source versions, expected and observed outcomes, validator, limitations, human capacity and retained evidence. Whole-route acceptance needs compound-failure exercises, including loss/compromise of normal identity/use/custody/reporting, stale protected evidence, missing human acceptance and failed fallback. No document check proves actual independent continuity or recovery.

7. Standards reference and derivation register

Checked against primary publisher sources on 6 October 2026. No paid ISO full text was available for clause verification. ISO edition/scope references below are alignment references, not assertions that a specific ISO clause mandates the AOS mechanism. Full licensed clause mappings, applicability/tailoring and organisational adoption remain owned work for the standards reviewer before any conformance claim. Do not import an ISO obligation or a crosswalk as operational authority.

Table row 1

Reference: STD-01
Exact publication / primary source: ISO 22301:2019 (https://www.iso.org/standard/75106.html), Business continuity management systems - Requirements; catalogue also identifies Amd 1:2024
Use and verification boundary: Continuity-management scope alignment; full clause mapping pending. Amendment does not substantiate these particular reporting/recovery mechanisms.

Table row 2
Reference: STD-02
Exact publication / primary source: ISO/IEC 27031:2025 (https://www.iso.org/standard/27031), Cybersecurity - Information and communication technology readiness for business continuity
Use and verification boundary: ICT readiness/recovery scope alignment. Use 2025 edition, not withdrawn 2011; full clause mapping pending.

Table row 3
Reference: STD-03
Exact publication / primary source: ISO/IEC 27001:2022 (https://www.iso.org/standard/27001), Information security, cybersecurity and privacy protection - Information security management systems - Requirements; catalogue identifies Amd 1:2024
Use and verification boundary: ISMS scope alignment; no certification or clause-level compliance inference.

Table row 4
Reference: STD-04
Exact publication / primary source: ISO/IEC 27002:2022 (https://www.iso.org/standard/75652.html), Information security, cybersecurity and privacy protection - Information security controls
Use and verification boundary: Control-guidance scope alignment; full control wording/number mapping pending, not a certification claim.

Table row 5
Reference: STD-05
Exact publication / primary source: NIST SP 800-53 Rev. 5 (https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final), September 2020 with December 2020 updates; public control text (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf); publisher notes Release 5.2.0, 27 August 2025
Use and verification boundary: Direct design-source controls checked in public text: AC-6; AU-9; CP-4/CP-4(4); CP-8/CP-8(2)/(3); CP-9/CP-9(1); CP-10/CP-10(2)/(4)/(6); IR-6/IR-8. Publisher release notes identify related-control updates to IR-6/8, rather than changed base obligations. Voluntary design reference; no complete NIST baseline adoption.

Table row 1
KPR direction: 01 / DEC-073
Standard-derived design principle (STD-05): CP-8 and (2)/(3): alternate communications and shared-failure assessment; IR-6/8: planned reporting
AOS-specific approved extension / ISO alignment: Separate reporting permission/custody, anti-suppression duty; STD-01/02/03/04 scope alignment.

Table row 2
KPR direction: 02 / DEC-074
Standard-derived design principle (STD-05): AC-6: least privilege
AOS-specific approved extension / ISO alignment: Advance failure permission and independently evidenced recipients under separate authority/use; STD-03/04 scope alignment.

Table row 3
KPR direction: 03 / DEC-075
Standard-derived design principle (STD-05): IR-6/8: designated reporting and response organisation
AOS-specific approved extension / ISO alignment: Explicit responsibility acceptance, owner retention, cover/escalation, failed-fallback exception and agreed resident channels; STD-01 scope alignment.

Table row 4
KPR direction: 04 / DEC-076
Standard-derived design principle (STD-05): CP-9/(1): protected backups and integrity testing; AU-9: audit protection
AOS-specific approved extension / ISO alignment: Authoritative currentness/completeness across withdrawals, consent and deletion as

release precondition; STD-02/03/04 scope alignment.

Table row 5
KPR direction: 05 / DEC-077
Standard-derived design principle (STD-05): CP-10/(2)/(4)/(6): known-state restoration, transaction recovery and protected recovery components
AOS-specific approved extension / ISO alignment: Isolated no-revival/no-hidden-payload/no-repeat-effect gate and conservative unknown reservations; STD-01/02 scope alignment.

Table row 6
KPR direction: 06 / DEC-078
Standard-derived design principle (STD-05): CP-4/(4): contingency and full recovery testing
AOS-specific approved extension / ISO alignment: Per-scope empowered acceptance, bounded automatic eligibility and continuing human service duties; STD-01/02 scope alignment.

Standard-derived principles guide the design; the complete AOS direction is an architectural choice recorded in the decision register. A source crosswalk is not equivalence. Future standards changes require controlled review; historical derivation retains the exact edition consulted.

8. Current disposition and residual work

KR-04/05 are reconciled at logical kernel-document level by this annex, component REQ/VER adoption and common register revisions. Added 30 proposed REQs and 30 planned VERs: kernel totals 324/237. Author structural checks do not execute cases or establish independent assurance.

Commissioning owners remain required: AOS-01 powers/release instruments; AOS-02 source coverage/custody mechanisms; AOS-03 reporting permissions/recipient assurance and lifecycle scope; AOS-04 task/human-duty profiles; AOS-05 dependency/isolation/restore/release mechanisms. Organisation appoints actual recipients/cover and numerical settings. Standards reviewer verifies licensed ISO clauses and applicability. Non-kernel adopters and independent reviewers remain unassigned. No missing owner/parameter is silently defaulted. Read current GI/human-handoff documents before proposing further drafting.