

Kernel R1 — UAT Handover

Evidence-based handover of the implemented Kernel scope. Business acceptance and release signatures remain open.

1. Handover purpose and current decision

This package hands the implemented Kernel scope to the UAT team for structured execution. It combines module walkthroughs, end-user procedures, source-backed implementation scope, cross-module ownership, editable test records and existing engineering evidence.

Handover state: prepared for UAT intake. UAT acceptance: not granted. Confirm the target environment and entry gates before execution. Known access/configuration/provider dependencies are listed with owners and closure criteria. No new R1 business cases have been executed by producing these documents.

“R1” is the logical handover baseline requested for this package. The application was delivered through multiple recorded component releases. This document does not invent a single new application build or deployment tagged R1. The release owner must confirm the active UI, APIs, workers, database migrations and published configuration as one frozen UAT baseline.

The scope is Kernel only, including MEDES. The reader scope contains only Kernel module procedures. Integrum, full Nexus and PGATE remain labelled architecture references; only the implemented bounded Nexus connection/source-refresh capability is included in the Studio/Scheduler paths.

2. Package map and how to use it

Deliverable	Use
Start here	Handover entry and direct links to all module documents.
Editable UAT workbook	Scope, requirements, full test procedures, screen checklist, access/data, gaps, defects, evidence, gates and signatures.
Kernel documentation library	14 walkthroughs + 14 end-user guides, two cross-module documents, retained screenshots and earlier references.

Deliverable	Use
CSV test cases	Portable execution sheet for import into your test-management system.
Screen-by-screen acceptance register	Current source/native screen catalog with unexecuted UI/security/lifecycle checks and qualified historical reads.
Component crosswalk	32 ownership and integration handoffs with source references.
Known gaps and dependencies	Actual recorded limits and entry blockers; no fabricated resolution dates.
Component release baseline	Historical release receipts plus blanks for active R1 confirmation.
Module and overall sign-off	Record decisions, exact versions, exclusions and named signatures.

1. Read the scope and gaps; agree which capabilities are in this UAT cycle.
2. Complete Environment, Access, Test Data and Entry Gates in the workbook.
3. Follow the relevant walkthrough, then use the end-user guide for field, lifecycle and recovery details.
4. Execute the linked cases and per-screen checks. Record actual results and evidence; raise defects immediately.
5. Complete cross-module and negative tests, regression, cleanup and exit gates.
6. Sign the module and overall decision against the frozen installation.

Extract the ZIP before opening files. The documentation library works offline and retains its screenshots and fonts; application links still require authorized login and network connectivity. CSVs are portable mirrors of the initial workbook. Choose one execution register as the source of truth; they do not synchronize automatically.

3. Module-by-module implementation baseline

Kernel Core

Shared business identities and reference information.

Aspect	R1 handover content
Implemented scope	Person/organization onboarding; contacts and addresses; relationships, classifications and geography; state/reason definition authoring, reviewed publication and contextual evaluation.
Prerequisites	IAM context; approved reference definitions; separate publication reviewer.
Acceptance limit	A party is not a sign-in account. Model evaluation does not execute a business transition; downstream consumers bind the exact published version/hash.
Retained evidence	E01; E11
Module cases	9 — all Not run

[Open step-by-step walkthrough](#) ·
 [Open end-user guide](#)

Tenant Engine

Tenant onboarding, subscription and configuration governance.

Aspect	R1 handover content
Implemented scope	Resumable onboarding requests; registration review; Core organization binding; identity evidence; typed configuration publication; commercial plans/subscriptions; domain ownership challenges and owner readiness steps.
Prerequisites	Core organization; IAM scope; Custodia-admitted supporting evidence where required; current commercial/configuration and domain facts.
Acceptance limit	Commercial records do not implement payment processing. Registration and DNS verification do not by themselves activate a tenant.
Retained evidence	E01; E11
Module cases	12 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Tenant Control Plane

Environment, entitlement and tenant lifecycle control.

Aspect	R1 handover content
Implemented scope	Environment registry and review; deployment-plan evidence/probes; configuration promotion; residency/support checks; module grants; lifecycle activation, suspension/restoration and exit paths.
Prerequisites	Eligible tenant and current owner evidence; known runtime placement; authorized operator and reviewer.
Acceptance limit	Registry changes do not provision Azure infrastructure. Activation remains subject to fresh owner checks; module entitlement does not grant user permissions.
Retained evidence	E01; E11
Module cases	11 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Identity and Access Management

Account authentication, selected context and access governance.

Aspect	R1 handover content
Implemented scope	Admin-created and subscribed user journeys; domains, profiles, roles, permissions and menus; user assignments; IAM-owned menu/screen and permission/control bridges; RBAC/ABAC evaluation, dynamic navigation, row review, credential/session administration and audit.
Prerequisites	Authorized IAM maker and a different checker identity; selected domain/profile; published Axis mappings; entitled tenant.

Aspect	R1 handover content
Acceptance limit	Screen-read evidence does not certify every access mutation. Security Dashboard configuration is blocked in the latest saved production evidence. Historical source-data exceptions require owner reconciliation.
Retained evidence	E01; E02; E04; E12
Module cases	42 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Axis

Screen/control rendering metadata and experience publication.

Aspect	R1 handover content
Implemented scope	Screen and control inventory; labels and presentation; mapping drafts and owner/independent reviews; configuration and experience versions; profile variations; governed activation and rollback.
Prerequisites	IAM-owned security mappings; designated mapping owner and independent reviewer; eligible rendering contract.
Acceptance limit	Axis does not grant access. Unpublished mappings remain guarded; tenant-defined database fields remain parked. Earlier mapping counts are historical, not current sign-off.
Retained evidence	E01; E02; E13
Module cases	10 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

TimeVault

Effective-dated records and preserved temporal changes.

Aspect	R1 handover content
Implemented scope	Country/State authoring; current/as-of views; temporal change proposals and Slice and Dice; independent decisions; preserved versions and applicable role-version integration.
Prerequisites	Configured temporal entity and supported interval policy; separate maker/checker; controlled Country/State fixtures.
Acceptance limit	Only configured entities are temporal. Future approved values need not be current. Re-test boundary, overlap and effective-date behavior against the chosen R1 environment.
Retained evidence	E01; E14
Module cases	10 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Regulix

Business rules, workflows, cases, assignments and service levels.

Aspect	R1 handover content
Implemented scope	Rule/decision design and evaluation; process/case definitions and supported models; validation/review/publication; native runtime starts, tasks, events, timers/sentries, assignments, SLA incidents and decision/deployment history.
Prerequisites	Published exact definitions and bindings; eligible task assignees; supported events/actions; correct business key and current revision.
Acceptance limit	Simulation is separate from live execution. Imported definitions require valid canonical mappings. The retained delayed-response fix and read checks do not establish every workflow permutation.
Retained evidence	E01; E15
Module cases	12 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Custodia

Document custody, access and controlled lifecycle.

Aspect	R1 handover content
Implemented scope	Content classes and metadata; individual/batch capture; admission/scanning and processing; document/version views, search and preview; review, sharing/disclosure; classification, retention, holds, disposal, storage and audit workspaces.
Prerequisites	IAM classification/access policy; eligible storage and processing services; admitted synthetic files; authorized custodians/reviewers.
Acceptance limit	Stored bytes are not admitted evidence or business approval. Holds/retention govern disposition. External provider delivery is a separate fact.
Retained evidence	E01; E16
Module cases	31 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

MEDES

Kernel member/case evidence exchange and correspondence.

Aspect	R1 handover content
Implemented scope	66 registered source entries covering member/case context, upload and intake, indexing/splitting, review/eligibility, case tasks, secure messages, letter/fax/print-mail work, delivery/response tracking, administration and reporting.

Aspect	R1 handover content
Prerequisites	Approved MEDES profiles/grants and owner configuration; Custodia, Regulix, Pulse, Vista, IAM, Axis and Tenant dependencies; live provider setup for external transport.
Acceptance limit	Technical delivery is recorded; complete live business acceptance is not. Latest saved production role inspection found no MEDES grants for inspected profiles. Fax/print-mail activation remains parked.
Retained evidence	E03; E10; E11
Module cases	19 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Nexora

Learning authoring, assignment and completion evidence.

Aspect	R1 handover content
Implemented scope	Learning home; authored content and review/publication; assignments/enrollments; lessons, assessments/attempts and completion; session/readiness evidence; bounded certificate issue/download/expiry/revocation.
Prerequisites	Published content; assigned learner and independent content reviewer; admitted media and configured providers for optional services.
Acceptance limit	AI mentor, automatic live-class provider and isolated SCORM host remain configuration dependencies. Automatic email/SMS event integration and certificate signature/QR workflow were listed as remaining reference gaps.
Retained evidence	E01; E17
Module cases	10 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Pulse

Reusable communication content, generation and delivery operations.

Aspect	R1 handover content
Implemented scope	Letter, email and message Studio; dataset/record binding and related/repeating content; templates and reusable content; saved current-data preview; one independent review/publication; pagination/output; channel/rule configuration, generated output, notifications and delivery history; registered Scheduler email/letter generation.
Prerequisites	Published authorized datasets; saved exact-version preview; separate reviewer; configured preview worker; approved transport for sending.
Acceptance limit	Preview is not publication or delivery. Normal template workflow is Draft → independent review → Publish. Scheduler generation does not automatically send. Provider-specific delivery must be accepted separately.
Retained evidence	E01; E05; E06; E18; E19

Aspect	R1 handover content
Module cases	29 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Vista

Sources, reusable data models, reports and dashboards.

Aspect	R1 handover content
Implemented scope	Self-service supported HTTPS JSON connection flow with credential references/testing/discovery; datasets including supported modeling/calculations; reviewed publication; reports/charts/expressions and dashboard composition; blank-start/template selection, draft recovery, current-data preview and versioned runs; Scheduler report/dashboard bindings.
Prerequisites	Reachable supported connection; field discovery; tenant filter and current data permissions; published dataset; exact report/dashboard versions; separate reviewer.
Acceptance limit	Dataset independent review is required. Supported registered connections are bounded; arbitrary protocols are not implied. Stored datasets or previews do not authorize otherwise denied fields/records.
Retained evidence	E01; E05; E06; E18; E19
Module cases	22 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Enterprise Scheduler

Governed execution and operational recovery of registered work.

Aspect	R1 handover content
Implemented scope	Jobs, once/interval/cron schedules, calendars, queues/workers, runs/attempts, bounded backfills, static dependency batches/checkpoints/resume; current-data preview and independent publication; service identity, leases/fencing, retries/cancellation/reruns and audit; registered Nexus source refresh, Vista report/dashboard, Pulse email/letter and recovery cleanup operations.
Prerequisites	Published job/artifact versions; eligible Run as identity; registered operation contract; current dataset permissions; live worker/queue and calendar where used.
Acceptance limit	Deployed implemented scope is recorded. Arbitrary operation/protocol self-registration, conditional fanout/automatic batches, Pulse actionable operational alerts and Vista operations datasets remain roadmap items. One dataset input binding is not a fanout engine.
Retained evidence	E07; E08; E09; E01
Module cases	21 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

Kernel Atlas

Structured knowledge, linked evidence and documentation editions.

Aspect	R1 handover content
Implemented scope	Retained document/knowledge baseline, claim/source linkage, implementation/evidence cross-reference and controlled edition/export procedures.
Prerequisites	Administrator-confirmed Atlas workspace and current access; authoritative source and implementation/evidence records.
Acceptance limit	Current Atlas portal acceptance is unverified. Historical synthetic Document View evidence is illustrative. Integrum, Nexus and PGATE full catalogs are specification references, not accepted operational modules.
Retained evidence	E11
Module cases	7 — all Not run

[Open step-by-step walkthrough](#) · [Open end-user guide](#)

4. Platform boundaries and cross-module flow

The application owner retains business data and business decisions. IAM owns identity, selected context, authorization and cross-boundary security bridges. Axis owns presentation metadata and rendering. Tenant Engine/TCP own tenancy and readiness; Regulix owns governed orchestration; TimeVault governs configured temporal records; Custodia owns evidence custody; Vista/Pulse own content/output; Scheduler dispatches registered owner operations.

Relationship	Required interpretation
Domain ↔ Profiles	Many-to-many; resolve account context through eligible profile assignments and applicable domain mappings.
Profiles ↔ Roles ↔ Permissions	Many-to-many at each step; selected context and effective dates matter.
Permissions ↔ Menus	Many-to-many authorization links; optional Role ↔ Menu is an additional constraint/checksum, not a security bypass.
Menu ↔ Axis Screen	One-to-one through the IAM-owned bridge.
Permissions ↔ Axis controls/fields	Many-to-many through IAM-owned bridges; enforce execution/data access as well as visibility.
Axis Screen → controls/fields	One-to-many presentation definition; labels/formats do not grant authority.
User account ↔ application user profile	Personal/KYC information is an application/Core concern; a complete historical migration is not asserted here.
Maker ↔ Checker	Independence is based on identity and policy. Switching profiles on one account does not create another person.

Execute in dependency order: Core references → tenant/subscription/configuration → environment and entitlements → IAM context → Axis rendering → owner definitions and datasets

→ business authoring → independent decisions → publication → execution/delivery → audit and recovery. Read-only browsing can proceed in parallel where prerequisites already exist; blocked mutations must retain their dependency reason.

- 1. **Organization to access:** Core organization → Tenant evidence/subscription → TCP environment/grants → IAM account/profile/roles → Axis screen/control rendering.
- 2. **Data to content:** define/pick source → build/pick related datasets → independently review/publish dataset → name/basic details → report/template/dashboard Studio → saved current-data preview → independent review → publication.
- 3. **Content to automation:** published artifact/version → registered Scheduler job/Run as/binding → preview → independent review → publish → schedule/calendar/queue → owner output → attempts/audit.
- 4. **MEDES:** member/case → Custodia evidence/admission → Regulix work/review → Pulse correspondence → provider-specific delivery → response → Vista reporting and audit.

Open cross-module walkthroughs · Open ownership and integration handbook

5. Existing evidence and what it establishes

The latest retained production screen report is dated **2026-10-19T22:58:35.010392+00:00**. It records **306 unique actual-user screens passing** within a rendered-menu union of 307, and 394 passing profile/screen checks with 1 failed check. These are different denominators. They are not percentages of completed business UAT.

The remaining failed screen is Security Dashboard: the recorded configuration guard required publication of a reviewed security page. MEDES access inspection separately found no relevant grants in the inspected profiles. Later configuration changes have not been re-queried during packaging.

Earlier native and fixture tests cover presentation, authorization boundaries, migrations, worker behavior and selected business paths. Their scope is retained in the evidence register. Documentation verification covers file rendering, links and downloads only. New UAT cases remain unexecuted.

ID / retained record	Boundary
E01 · Production screen-read and navigation acceptance	Authenticated production reads and available record navigation, 19 October 2026. Retains known gaps; not full mutation/approval acceptance.
E02 · Record review and presentation acceptance	Isolated fixtures and native test profiles; both themes, controls and originating-record reviews.
E03 · MEDES production profile coverage	Read-only production catalog inspection; inspected profiles had zero MEDES permissions/menus.

ID / retained record	Boundary
E04 · Dynamic menu provenance	Saved navigation provenance inspection; does not establish all role/ABAC permutations.
E05 · Studio deployment receipt	18 October Studio-only deployment, including preview/connection workers; Scheduler excluded from this older release.
E06 · Studio deployment verification	Historical deployment/public boundary checks; later read checks are in E01.
E07 · Scheduler and lifecycle deployment receipt	19 October Scheduler release, worker heartbeat and native profile checks; not human production business acceptance.
E08 · Scheduler migration and native acceptance	Rehearsal, rollback, service identity, native/browser tests and lifecycle columns; evidence boundary retained.
E09 · Scheduler implementation and remaining scope	Deployed implemented subset with explicit remaining roadmap. Older queue summaries may predate deployment.
E10 · MEDES technical completion and activation limit	14 October technical delivery; activation and live business acceptance were explicitly incomplete. E03 is later access evidence.
E11 · Documentation verification	Offline documentation links/rendering/downloads only. No application business tests.
E12 · IAM historical migration exceptions	Historical legacy classifications/audit data and specialist-permission exceptions; recheck before treating counts as current.
E13 · Axis implementation and review dependencies	Historical delivery and mapping-review/tenant-field limits; later read evidence in E01.
E14 · TimeVault workspace delivery	Historical Country/State UI and authenticated query evidence with later-flow-repair reference.
E15 · Regulix connected HTTP acceptance	Isolated native acceptance; later production navigation in E01.
E16 · Custodia reference implementation	Historical batch capture, dashboard, document tab delivery and evidence boundaries.
E17 · Nexora implementation and provider dependencies	Historical core integration delivery with explicit provider and remaining reference gaps.
E18 · Studio implementation acceptance	Mixed historical implementation ledger. Deployment state must be read with E05/E07 and later E01, not stale priority text.
E19 · Qbox fonts and icons evidence	Saved production font/icon inspection. Not a fresh screenshot run.
E20 · MEDES parked activation decision	Parked native approvals, provider activation and dependent business acceptance. No approval waiver.
E21 · Application source-route inventory	484 source routes and 32 native IAM screens; route existence is not availability or business acceptance.

6. Environment, identities, fixtures and entry gates

Use the known MediFlex deployment URL only after the environment owner confirms the intended UAT target. Do not assume the public production portal is a disposable test environment. Record the actual release and context in the workbook; do not put passwords, session cookies, tokens or provider secrets in test evidence.

Gate	Criterion	Accountable role
ENT-01 · Release scope and exclusions accepted	R1 scope, gaps, applicable modules and deferred cases approved.	Release owner
ENT-02 · Exact environment frozen	Component hashes, migrations/configurations, tenant/domain and browser matrix recorded.	Release / operations
ENT-03 · Access prepared	Named authorized makers, distinct checkers, readers, service identities and MEDES roles where required.	IAM owner
ENT-04 · Owner publications ready	Required Axis mappings, definitions, bindings and entitlements published; gates remain explicit.	Module owners
ENT-05 · Fixtures prepared	Synthetic data IDs, expected outcomes, bounded run windows and cleanup plan recorded.	Data owners
ENT-06 · Provider scope confirmed	Live channels/providers configured and authorized, or explicitly excluded with dependent cases marked Blocked.	Integration owner
ENT-07 · Workers and operational smoke	Current required workers/queues healthy; owner output smoke recorded.	Operations
ENT-08 · Testers and triage owners assigned	Module ownership, evidence rules and issue escalation known.	UAT lead
ENT-09 · Recovery baseline approved	Backup/restore evidence and change-specific rollback procedure available.	Operations
ENT-10 · Known gaps disposition agreed	MEDES access, security mapping, Atlas and provider-dependent cases explicitly gated.	Business owner

Functional actors

Actor	Duties	Boundary
IAM configuration maker	IAM masters, assignments, mappings; create and submit	No own approval; no automatic tenant-wide administrator grant
IAM independent checker	Read proposed/current access and decide eligible rows	Different identity from maker/affected beneficiary where required
Axis owner / independent reviewer	Inspect and decide owned mappings; publish eligible experience	Owner approval and independent decision may require separate participants
Core / reference steward	Manage parties, references, controlled model proposals	Business identity creation does not grant IAM access
Tenant maker / commercial administrator	Onboarding, evidence, configuration and subscription proposals	Registration does not authorize lifecycle execution
Tenant/TCP reviewer and operator	Eligible owner review, readiness checks, environment/lifecycle operations	Operator scope limited to assigned tenants
Data / Studio maker	Supported source/dataset authoring, report/dashboard/template authoring, preview and submit	No self-review; use only authorized sources and fields
Data / content checker	Current saved preview and eligible row decisions	Separate identity; review does not imply execute/send authority
Scheduler maker / reviewer / operator	Governed jobs/schedules and authorized runs, cancellation/recovery	Run as identity separately authorized; review and execution are distinct
Scheduler service identity	Execute exact registered operations with required dataset permissions	No interactive credential sharing; expiry/revocation checked

Actor	Duties	Boundary
Custodia custodian / reviewer	Capture, metadata, evidence review and authorized custody actions	Classification, retention and legal holds constrain actions
MEDES business roles	Member/case/evidence/correspondence duties under approved MEDES grants	Missing grants currently block the recorded production profiles
Nexora author / reviewer / learner	Content governance, assigned learning, assessment/completion	A learner is not a publisher; viewing is not completion
Reader / denied-context tester	Read only assigned data; deliberate negative control account	Must lack tested mutation or other-domain permission
Release / UAT / operations owners	Confirm baseline, run evidence, triage and sign-off	Named owners to be assigned in workbook; signatures are not prefilled

Data preparation

Fixture	Preparation	Cleanup
R1_ORG_<run> · Core organization and person	Use synthetic names and internal training addresses; reuse IDs across Tenant tests.	Retire through owner workflow; keep approved audit evidence.
R1_TENANT_<run> · Tenant, environment, domain and commercial plan	Controlled non-production tenant, eligible type, exact plan/config versions and DNS name only if owned.	Do not deactivate shared production tenant to test failure.
R1_ACCOUNT_A / B / READ · Maker, independent checker, restricted reader	Distinct natural-person identities or approved separate test accounts; two profiles on one account do not establish independence.	Revoke temporary grants after UAT; retain governance receipts.
R1_COUNTRY / STATE · Temporal test masters	Disposable codes with agreed date-boundary, overlap and future-period fixtures.	Preserve temporal history; no hard-delete cleanup.
R1_SOURCE_<run> · Supported JSON endpoint and dataset	Controlled fixture endpoint; secret references supplied privately; positive/denied rows, zero rows, nulls, long text and related records.	Remove temporary connection only through supported lifecycle.
R1_CONTENT_<run> · Report, dashboard, letter, email	Distinct draft/published versions; long multi-page content and authorized current row keys.	Retire drafts/jobs and retain output/version/hash evidence.
R1_DOC_<run> · Synthetic admitted and rejected document	PDF/text/image allowed by class policy; no personal/medical data; use approved scanner rejection fixture if available.	Respect retention/hold rules; do not force disposal.
R1_CASE_<run> · Member/case and response	Fictional case with permitted scope and configured owner workflow; no real member contact details.	Close or retire through business lifecycle; preserve task history.
R1_JOB_<run> · Job/schedule/calendar/batch	One-time small window, explicit timezone and version pins; bounded failure fixture and controlled recipient for any delivery.	Pause/retire schedule; reconcile accepted work before cleanup.
R1_LEARN_<run> · Learning content/assignment	Small text lesson and assessment with known pass/fail answers; configured bounded certificate flow.	Retain accepted learning evidence and retire temporary content.
R1_KNOWLEDGE_<run> · Atlas document and claim links	Non-sensitive source, known implementation artifact, evidence record and intended audience.	Close draft edition or retain approved knowledge record.

7. UAT execution plan and evidence rules

The execution register contains **280 cases**: 245 retained module procedures and exceptions plus 35 dedicated cross-module, security, lifecycle, output and operational cases. The screen register

contains 554 entries: 484 application source routes, 32 native IAM screens, 37 separate Regex entries and one explicitly unverified Atlas portal entry. A route is not proof of a deployed usable feature; use the scope and gate columns.

Order	Work	Completion evidence
1	Entry gates, environment, access and test data	Signed scope; versioned baseline; named test identities; fixtures.
2	Core, Tenant, TCP, IAM and Axis	Account and context setup; correct allow/deny rendering and APIs; exact owner publications.
3	TimeVault, Regex and Custodia	Temporal boundary, workflow and evidence lifecycle outcomes.
4	Sources, datasets, Vista and Pulse	Current authorized preview; independent dataset/content review; published exact versions and output consistency.
5	Scheduler and integration chains	Version-pinned execution, attempts/results, service denial, retries, batches, backfills and calendar evidence.
6	MEDES, Nexora and Atlas where gates permit	Business-role journeys; provider-dependent cases gated; current portal confirmation.
7	Remaining per-screen coverage and nonfunctional checks	UI/control/lifecycle evidence for every agreed screen, including N/A rationale.
8	Regression, cleanup and exit decision	Affected tests rerun; defects dispositioned; controlled sign-off.

How to record a result

1. Assign tester and selected profile, tenant/domain, environment and build before acting.
2. Read preconditions, exact screen and expected result. Use the walkthrough's numbered steps and screenshots; capture current evidence for UAT.
3. Execute once. Record created record IDs, versions, output references and request correlation where relevant.
4. Compare actual behavior to expected behavior. Choose Pass, Fail, Blocked or Not applicable. A planned case stays Not run.
5. Attach evidence and defect/dependency ID. Blocked is not Pass. Not applicable needs a release-owner scope decision.
6. For a fix, preserve the original failure, record fix baseline and a separate retest result.

Evidence naming: R1_<case-id>_<profile>_<step>_<UTC-date-time>. Retain screen/record state before and after, exact decision/output reference, selected context and the relevant response/correlation ID. Mask personal data and secret values. A screenshot of an empty grid is evidence of that read state, not proof of create/approve success.

For screen checks, inspect standard header and Back placement, actual font/icon/theme, dynamic menus, control/data authorization, originating-row review, create/edit/concurrency,

explicit active/inactive behavior and responsive/SPA navigation. Mark review or lifecycle checks N/A only when the screen has no such operation and document why.

8. Known gaps, parked work and exclusions

The following are carried forward from dated source records and the established scope. They are not all software defects: some are owner approvals, data/provider setup, roadmap scope or unexecuted acceptance. Assign named owners and dispositions before UAT begins.

ID / category	Scope and impact	Disposition	Owner and closure
R1-G01 · Configuration gate	IAM / Axis Security Dashboard: Security Dashboard cannot be used until a reviewed experience is published.	Open at latest saved inspection	Axis owner and independent reviewer. Approved current security-page mapping/version and successful permitted/denied UAT. Evidence: E01
R1-G02 · Access gate	MEDES: Inspected profiles cannot begin MEDES business UAT.	Open at latest saved inspection	IAM access owner and independent checker. Approved MEDES role/profile/menu/control chain, user assignments and allow/deny browser evidence. Evidence: E03; E10; E20
R1-G03 · Owner configuration gate	MEDES integrations: Native owner publications and business-role journeys cannot be assumed live.	Parked dependency	MEDES and platform owner reviewers. Current approved configuration/publication references for each of the seven platform handoffs. Evidence: E10; E20
R1-G04 · Provider activation	Pulse / MEDES fax and print-mail: Live fax/print-mail delivery is not accepted.	Parked by user	Provider administrator and business owner. Secret references configured, approved sender/recipient and actual provider/delivery receipts for controlled destinations. Evidence: E20
R1-G05 · Acceptance gap	All modules: Historical screen reads do not establish all create/edit/deactivate/review/execute journeys.	Open	UAT lead and module business owners. Completed R1 cases and applicable screen/control checklist with evidence, defect disposition and sign-off. Evidence: E01; E02
R1-G06 · Record setup	Vista / Pulse preview: Missing row bindings or denied datasets prevent the affected preview.	Record-dependent gate	Content maker and data owner. Exact saved version, authorized current row, successful preview and fresh review acknowledgement. Evidence: E01
R1-G07 · Roadmap	Scheduler connectors and operations: Arbitrary protocols and business operations cannot be enabled by entering a name.	Outside implemented R1 subset	Integration product owner. Supported adapter and registered typed contract, independent governance and execution/deny evidence. Evidence: E09
R1-G08 · Roadmap	Scheduler orchestration: Conditional fanout, automatic batch triggers and broader EOD/control totals are not accepted features.	Outside implemented R1 subset	Scheduler product owner. Approved extension scope and implementation/acceptance evidence. Evidence: E09
R1-G09 · Roadmap	Scheduler → Pulse / Vista operations: Actionable operational alerts and dedicated Vista operations datasets remain listed extensions.	Open extension	Scheduler, Pulse and Vista owners. Registered event/data contracts, configured authorized targets and end-to-end success/failure evidence. Evidence: E09

ID / category	Scope and impact	Disposition	Owner and closure
R1-G10 · Provider / feature gap	Nexora: Mentor, automatic live classes, isolated SCORM hosting, outbound events and signature/QR credential flow have stated limits.	Recorded dependencies; current recheck needed	Learning owner and integration administrator. Configured provider contracts and accepted relevant learner/author/reviewer journeys. Evidence: E17
R1-G11 · Availability gap	Atlas: Historical captures do not prove the current workspace can be used.	Current portal not verified	Atlas owner. Confirmed environment/access and executed document/link/export UAT. Evidence: E11
R1-G12 · Source-data exception	IAM historical records: Legacy classification/effective-start/audit values and specialist provider links cannot be fabricated.	Historical open items; recheck required	IAM data owner. Authoritative reconciliation or signed exception against the current records. Historical counts are in E12. Evidence: E12
R1-G13 · Governance dependency	Axis mappings: Unpublished mappings are not eligible for unrestricted rollout. Tenant-defined database fields remain parked.	Scope-specific review remains required	Axis designated owner and reviewer. Exact accepted mapping versions and governed publications for the agreed R1 screens. Evidence: E13; E01
R1-G14 · Release baseline gate	R1 target environment: Historical component receipts do not uniquely identify the current combined R1 installation.	To confirm at UAT entry	Release owner / operations. Signed environment record with current UI, APIs, workers, migration and configuration versions. Evidence: E05; E07; E01
R1-G15 · Operational acceptance	Recovery and nonfunctional targets: Business load, recovery targets and supported environment matrix require owner acceptance.	Not signed off	Operations and UAT lead. Agreed targets, controlled rehearsal results and operational sign-off for this exact baseline. Evidence: E13; E08
R1-G16 · Specification boundary	Integrum / full Nexus / PGATE: Full specification catalogs are not added as implemented operating modules. Bounded Nexus HTTPS/source refresh remains included.	Reference only	Architecture / release owner. Future release scope with implementation and operational acceptance evidence. Evidence: E11; E09

9. Defect management and regression

Severity	Meaning	Required handling
Sev1 — critical	Unauthorized data/execution, loss/corruption, or system-wide unavailability.	Stop affected activity; preserve evidence; notify security/operations/release owner immediately.
Sev2 — high	Critical in-scope business path blocked with no acceptable workaround.	Block acceptance of affected scope; prioritize correction and cross-module regression.
Sev3 — medium	Functional error with a controlled acceptable workaround.	Owner decides whether to fix before exit or accept a documented condition.
Sev4 — low	Cosmetic or minor usability/documentation defect without material workflow impact.	Record and prioritize; no automatic waiver.

Use New → Triaged → In progress → Ready for retest → Closed, or Reopened / Deferred with accepted-risk reference. Priority P0/P1/P2 indicates execution or fix urgency; it is not severity. Capture reproducible steps, expected and actual outcomes, exact baseline, profile/context and evidence. Never “fix” a failed authorization test by granting an unrelated broad administrator role.

After correction, rerun the failing case, a neighboring positive case, its permission-denied counterpart and affected downstream handoff. For data or publication fixes, verify old immutable history and current version binding. For retry fixes, verify no duplicate owner side effect. Keep original and retest records.

10. Operations, support and safe recovery

Symptom	First checks	Owner / next step
Missing menu or screen denied	Selected tenant/domain/profile, active/effective assignment, role/permission/menu and IAM – Axis bridges, module entitlement.	IAM and owner configuration; preserve denial/correlation.
Screen opens but action absent	Record state/revision, control permission, review independence and record-specific eligibility.	Owning module plus IAM/Axis; do not bypass review.
Preview fails or stale content	Saved artifact version, published dataset, authorized row key/fields, current source and preview worker.	Vista/Pulse/data owner; refresh preview after a content change.
Job queued or worker unavailable	Published job, queue/calendar window, Run as authority, current heartbeat/lease and dispatch result.	Scheduler operator; distinguish queued, accepted, running and completed.
Uncertain execution result	Owner receipt/output reference and idempotency key before dispatching again.	Scheduler and producer owner; cancellation may not reverse accepted external work.
Generated email/letter not delivered	Generation receipt versus channel/mode/recipient/provider attempts and final status.	Pulse/provider administrator; no claim of delivery from local capture.
MEDES menu absent	Approved MEDES role/profile and menu/control grants plus owner configuration.	IAM/MEDES; current recorded gate is R1-G02.
Document not available	Admission/scanning/classification, processing/version, custody permission and retention/hold state.	Custodia; quarantined bytes are not approved business evidence.
Tenant activation blocked	Fresh identity, commercial, configuration, placement/residency/support and entitlement evidence.	Failed owner step; registration progress is not activation authority.
Slow workflow response	Request correlation, server error/status, current deployment, task/definition identity and supported timeout behavior.	Regulix/runtime owner; inspect receipt before repeating a mutation.

Release and rollback boundary

Before UAT freeze, the release owner reconciles the historical receipts with the active installation and signs the environment record. If a correction is needed, build a bounded candidate, rehearse exact migrations/configuration and rollback in isolation, obtain required release authorization, deploy the reviewed artifact, verify health plus affected authenticated journeys and issue a new UAT baseline. This package itself deploys nothing.

Rollback must use the matching component receipt, verified backup and change-specific procedure. A UI rollback does not roll back database/configuration changes. A database restore or job cancellation does not undo a provider's accepted delivery. Stop new dispatch as

authorized, record in-flight work, reconcile owner outcomes and then follow the approved recovery sequence. Keep immutable attempts and audit history.

Complete the support roster in Environment. Route identity/access failures to IAM, presentation metadata to Axis, tenant facts to Tenant/TCP, data connections to the data/integration owner, content/output to Vista/Pulse, execution to Scheduler, and business case decisions to MEDES/Regulix. Escalation contacts and service targets must be assigned; no names or SLAs are invented here.

11. Exit criteria and formal acceptance

Gate	Acceptance criterion	Owner
EXIT-01 · Coverage complete	All agreed cases and applicable screen checks executed; N/A/Blocked have signed disposition.	UAT lead
EXIT-02 · Critical paths pass	All in-scope P0 cases pass on frozen baseline; no unresolved data leak, unauthorized execution or integrity failure.	Business / security
EXIT-03 · Defects resolved or accepted	No open Sev1/Sev2 blocking release; lower defects have explicit owner acceptance, workaround and target.	Release owner
EXIT-04 · Integration evidence complete	Exact versions and source → output → run → audit references retained; provider states distinguished.	Module owners
EXIT-05 · Independent review verified	Distinct-identity review and forbidden self-approval confirmed for applicable workflows.	IAM / business
EXIT-06 · Regression after fixes	Affected positive, negative and cross-module cases rerun against corrected baseline.	QA lead
EXIT-07 · Operational acceptance	Agreed load, recoverability, worker operation and support procedures accepted.	Operations
EXIT-08 · Data/access cleanup	Temporary schedules/grants/fixtures cleaned through governed flows, with receipts retained.	Owners
EXIT-09 · User handover accepted	Walkthroughs, end-user guides and support routes accepted; discrepancies recorded.	Business owner
EXIT-10 · Release decision signed	Named approvers sign Accept / Accept with conditions / Reject with exact baseline and exclusions.	Sponsor / release owner

Allowed decisions are **Accept**, **Accept with conditions**, or **Reject**. Conditional acceptance must list exact modules/capabilities excluded, defect/gap IDs, workaround, responsible owner and target decision/date. The presence of manuals or historical engineering passes does not satisfy an exit gate.

Release / environment / UI / API / worker / configuration baseline:

Cases: executed _____ passed _____ failed _____ blocked _____ not applicable
_____ not run _____

Applicable screen checks completed: _____ / _____

Open defects / gaps / accepted conditions:

Decision and business rationale:

Business owner / signature / date:

QA / UAT lead / signature / date:

Operations / security / release owner / signature / date:

Use the workbook Sign Off tab for each module and the overall decision. The printed form is a signature aid; store its approved copy and reference it in the same controlled register.

12. Traceability, package integrity and document control

There are 90 requirement/journey entries mapped to 280 cases. Each retained module case links to its precise walkthrough/manual chapter; the workbook includes the procedure text and expected result. The screen catalog and 34 originating-record review commands complement journey coverage. These inventories provide a test allocation baseline, not a claim that every path or policy permutation has passed.

Evidence snapshots retain source SHA-256. Selected large records are reduced to their relevant summary fields; originals remain identified by their source hash. Historical production reads are provided in a separate CSV, not merged into R1 execution results. The Kernel reader revision retains earlier procedures in HTML. Infrastructure references outside the reader scope use operator reference IDs; resolve those IDs against the controlled source baseline before executing a command.

The final ZIP has an integrity receipt and file SHA-256 manifest. Keep the issued ZIP unchanged. Make a dated working copy of the workbook/registers for execution; its changed hashes are

expected. Archive the completed workbook, evidence and signed decision as a new UAT outcome edition.

Prepared by: Kernel engineering documentation handover. Document date: . Business signatories: pending. Application build: confirm in Environment and Release Baseline. New deployment during packaging: none. New business acceptance during packaging: none.

Deployment, gateway and regression handover — Revision 2

The deployment pipeline is the implemented operator-driven Azure release process. These annexes document its scripts, stages, artifacts, migrations, service activation, verification and rollback, together with Kong and recorded regression results.

- [Azure deployment pipeline](#) · PDF
- [Kong and gateway operations](#) · PDF
- [Regression suites and recorded results](#) · PDF

Historical results retain their test environment and date. No application regression or live gateway readback was performed by this documentation revision.

Kernel R1 UAT package • Prepared • Documentation and evidence consolidation only. No application deployment, access grant or business approval was performed by this packaging run.

Current release additions and acceptance

The following changes update the earlier handover baseline. Earlier results retain their original scope. The additional business UAT cases start Not run and require actual tester evidence.

Feature	Module	Change	Operating impact
F01	IAM	Explicit domain/profile mapping	Approved domain creation starts with zero profile links; pending mappings do not grant eligibility.
F02	Axis	Governed screen authoring	Create Screen, source/field definitions, access mapping, draft, preview and originating-record review.
F03	IAM / Axis	Reviews on the owning record	Review pending master, mapping, screen and control changes in their originating workspace.
F04	IAM	Named Super Administrator	Explicit scoped same-person review with administrator evidence; ordinary profiles retain independence checks.

Feature	Module	Change	Operating impact
F05	Axis	Screen and control metadata	Screen title/help and control label/help/format maintained through governed presentation changes.
F06	Axis	Owning screen controls	Controls list owning screens first; details and controls share context, refresh and Back behavior.
F07	Pulse / IAM	Notification outcome links	Published notification OPEN contract restored; recipient/context checks retained.
F08	MEDES	Activation qualification	Installed technical package; role grants, enabled APIs and review-route activation remain pending.
F09	Kernel	Documentation hub	Master index, separate manuals/demos/UAT, linked modules, current supplement and offline downloads.
F10	Axis	Consistent screen authoring and explicit header help	Shared record tabs, responsive form grid, Cancel/Save footer and multiline screen-header help stored in existing metadata.
F11	Axis	Bounded authorized editor options	Prepared authorization context eliminates repeated source checks; source and permission results remain unchanged.

[Feature register](#) · [Additional UAT cases](#) · [New evidence index](#)

MEDES entry gate: technical installation is complete; target activation is incomplete. Role grants, enabled APIs and document-review route must be verified before a live business demo. Provider-based delivery additionally requires approved provider setup and authorized destinations.

Verification boundary: the Axis screen-context release records 35 rollback-only database checks, 12 UI tests and 15 fixture-browser checks. The notification contract correction records 11 schema checks and 17 rollback-only database checks. These are not a complete authenticated production journey or a new client UAT sign-off.