UAT Execution and Defect Guide

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

Open complete handover

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
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.

Fixture	Preparation	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 Regulix 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, Regulix 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 Awaiting client validation.
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.

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.

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 _____ awaiting client validation _____

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.

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

Integrated Pre-UAT release

How to read the status: implementation delivery, engineering regression and client acceptance are separate milestones. The engineering results below describe work already tested. The editable client case results begin *Awaiting client validation* because this handover starts the client Pre-UAT phase.

Security testing and user-experience refinements continue during Pre-UAT. The final UAT decision will include closure or explicit acceptance of the relevant findings and the agreed review outcomes.

Delivered scope, current checks and client review plan · Feature register