

Kernel Platform Crosswalk & Integration Handbook

Ownership, IAM–Axis model, principal tables, dependency order, detailed handoff contracts, MEDES integration, content automation, governance and failure recovery.

Use the current tenant, profile and permitted actions. Screenshots illustrate the application; example records and date fields may differ in your environment.

Contents

1. Kernel scope and how to use this crosswalk
2. Who owns what · complete Kernel component matrix
3. Platform relationship map
4. Terms that must remain distinct
5. IAM–Axis relationship model and runtime evaluation
6. Principal schemas and IAM table crosswalk
7. Dependency order for initial setup and controlled change
8. What to carry across every integration boundary
9. Detailed component-to-component handoff catalog
10. End-to-end MEDES crosswalk · case to reviewed communication
11. End-to-end source → dataset → content → automation crosswalk
12. Approval, publication, availability and temporal behavior
13. Recovery ownership and failure decision tree
14. Change-impact and version adoption checklist
15. Current governance and documentation handoffs

Kernel scope and how to use this crosswalk

Use this crosswalk to follow responsibilities and handoffs across Kernel Core, Tenant Engine, Tenant Control Plane, IAM, Axis, TimeVault, Regulix, Pulse, Vista, Enterprise Scheduler, Custodia, MEDES, Nexora and Kernel Atlas.

Begin with the owner of the business record. Confirm its current version, permissions, review decision and dependency references before continuing in the next module.

Who owns what · complete Kernel component matrix

Module / guide	Authoritative responsibility	Key records / output	Consumers / usage	Boundary to preserve
<u>Kernel Core</u>	Shared people/organizations, contacts, relationships, geography and published state/reason definitions	Party identity; relationship; publication/version/has h	Tenant organization selection and business reference consumers	Core party is not an IAM credential or access profile.
<u>Tenant Engine</u>	Tenant onboarding, organization binding, identity/commercial/configuration evidence and domain ownership	Request/case; tenant identity; owner evidence; reviewed configuration and subscription	TCP readiness and tenant-aware applications	Registration, DNS ownership and commercial review do not individually activate a tenant or grant a user access.
<u>Tenant Control Plane</u>	Environment registry/bindings, configuration promotion, residency/support, module grants, activation/restoration and exit	Environment/deployement receipt; effective config; grant; lifecycle result; signed truth	Current tenant/module eligibility and runtime readiness	Environment registration is not cloud provisioning; module entitlement is not an IAM permission.
<u>Kernel IAM</u>	Authentication identity, accounts, context, assignments, roles/permissions, menus, IAM-owned Axis bridges and access decisions	Selected subject/tenant/domain/profile; authorized navigation/actions; decision/audit	Every protected UI/API/business operation	Personal/KYC data belongs to application/Core; changing profile does not create an independent person.

Module / guide	Authoritative responsibility	Key records / output	Consumers / usage	Boundary to preserve
<u>Kernel Axis</u>	Screen and control presentation metadata, owner-reviewed mappings, labels, experience versions and deliveries	Screen/control identities; approved presentation/version; delivery reference	Authorized module screens through the shared renderer	IAM owns security decisions and bridge mappings. Axis appearance does not grant execution rights.
<u>Kernel TimeVault</u>	Configured effective-dated changes, preserved versions and temporal decision evidence	Proposal; effective intervals; version history; preserved approval	Country/State and explicitly integrated owner records	Not every application table is automatically temporal; approved future values may not yet be current.
<u>Kernel Regulix</u>	Governed process/case/rule definitions, assignments/events/SLA and native execution/tasks	Pinned definition; instance; task/decision; checkpoint; incident	Configured review/business process owners	Technical simulation is not live execution; workflow routing does not replace owner data validation.
<u>Kernel Custodia</u>	Document bytes, integrity, versions, admission, controlled content access and custody lifecycle	Capture/admission; document/version/hash; sharing/export/retention evidence	MEDES evidence, generated correspondence and tenant supporting documents	A stored/admitted file does not itself establish business sufficiency or permission to dispose.
<u>Kernel MEDES</u>	Member/case context, evidence exchange/intake, business review, correspondence, delivery/response work	Case; linked evidence; work decision; generated item and delivery/response references	Custodia, Regulix, Pulse and Vista integrations	MEDES is included as a Kernel module. Provider credentials/activation and case approval remain explicit dependencies.
<u>Kernel Nexora</u>	Learning content/reviews/publication, assignments, attempts, readiness evidence and credentials	Content version; learner assignment; result; reviewed evidence; credential	Authorized learners/managers and registered reporting/integration consumers	Provider-dependent mentor/SCORM/live-class/outbound features require current configuration; viewing is not completion.
<u>Kernel Pulse</u>	Communication templates/bindings, current-record preview, publication, generated output and configured channel activity	Template/version; generated email/letter; capture/delivery reference	Business correspondence, notifications and registered Scheduler generation	Generated, locally captured, provider-accepted and delivered are different outcomes.

Module / guide	Authoritative responsibility	Key records / output	Consumers / usage	Boundary to preserve
<u>Kernel Vista</u>	Report/dataset authoring in the supplied flow, report/dashboard composition, preview/publication and execution	Dataset/report/dashboard versions; preview; run/snapshot	Users, published dashboards and Scheduler producer operations	Dataset publication and execution authorization are required; report output is not an owner mutation.
<u>Enterprise Scheduler</u>	Governed jobs, schedules/calendars, queues/workers, occurrences/runs, batches and bounded recovery	Job/version; schedule/occurrence; run/attempt; checkpoint; producer result	Registered business operations with supported contracts	Ordering does not automatically transfer outputs or reverse effects; unsupported connectors do not become available by naming them.
<u>Kernel Atlas</u>	Structured knowledge, requirements/evidence relationships and controlled documentation editions	Module/document/section; trace relationship; source/evidence; edition	Kernel owners and permitted readers	A source-confirmed specification is not implementation or production acceptance.
Kernel Integrum · specification	Analytical onboarding, ingestion, lakehouse/quality/lineage and curated data products in the retained design	Designed analytical source/product/lineage contracts	Vista and permitted analytical consumers in the design	The catalog describes a design; this edition does not establish full runtime deployment or live operating screens.
Kernel Nexus · specification + bounded connection capability	Enterprise integration definitions/exchanges/recovery in the design; the supplied Studio guide verifies a bounded registered source-refresh path	Designed interface/connector/contract/exchange; registered source snapshot where implemented	PGATE, business owners and analytical/reporting consumers	One NEXUS_SOURCE_REFRESH_V1 operation does not establish implementation of the entire Nexus catalog.
Kernel PGATE · specification	Gateway product/route/consumer admission, policy and controlled file exchange in the retained design	Designed admission/route/request/file-transfer references	Nexus and business owner services after admitted requests	No current live gateway UI/route acceptance is inferred from the physical model or capability inventory.

CHAPTER 3

Platform relationship map

Foundation

Access & presentation

Core organization → Tenant registration & evidence → TCP environment, entitlement and lifecycle

IAM account → selected domain/profile → roles & permissions → menu ↔ Axis screen → permitted controls

Business & evidence

MEDES case ↔ Custodia document/version ↔ Regulix task/decision; TimeVault supplies configured temporal governance

Content & automation

Source → reviewed dataset → Vista report/dashboard or Pulse template → current preview → independent review → publication → Scheduler job/run → producer output

Learning & knowledge

Nexora
content/assignment/attempt/credential; Atlas
source/evidence/edition trace

Design-scope integration

PGATE admission → Nexus exchange →
business owner or Integrum analytical
preparation → Vista consumption

The arrows identify responsibility and references, not unrestricted access or automatic execution. For example, the last line is a specification-level architecture; a single implemented connection refresh does not prove the entire gateway/integration/lakehouse design is running. Every protected handoff still needs current identity, tenant and owner checks.

CHAPTER 4

Terms that must remain distinct

Term pair	Distinction	Example consequence
Tenant / IAM domain	Tenant is an operating/isolation boundary; domain is an authorization context.	A verified tenant domain/DNS claim does not grant an account a profile.
Core person / IAM account / access profile	Business identity, sign-in identity and role grouping are separate concepts.	Creating a person or changing a contact does not automatically create credentials or access.
Menu / screen / control / operation	Navigation, presentation container, presentation/action element and executable owner contract.	A menu can be visible while the screen read or an action is denied.
Draft / approved / published / active	Authoring, decision, immutable consumable version and current availability are distinct dimensions.	An approved but unpublished template may not appear in a published-content selector.
Submitted / accepted / succeeded	Request admission, producer acceptance and final completion have different evidence.	A queued job or accepted external request is not completed output.
Generated / captured / delivered	Created bytes, local receipt and actual transport result.	A READY generated email need not have been sent.

Term pair	Distinction	Example consequence
Effective date / decision date	Business validity and the time of review.	An approved future Country name need not appear in today's view.
Retire / deactivate / delete / disposition	Lifecycle or visibility changes differ from physical destruction.	is_active=false neither cancels accepted jobs nor authorizes destruction of held documents.

CHAPTER 5

IAM–Axis relationship model and runtime evaluation

Relationship	Cardinality / ownership	Administration meaning
IAM Domain ↔ Profiles	M:M; IAM	Assign profiles to their eligible domain scope.
Profiles ↔ Roles	M:M; IAM	Define the roles available through the selected access profile.
Roles ↔ Permissions	M:M; IAM	Grant explicit functional/read/action authority.
Permissions ↔ Menus	M:M; IAM	Connect navigation eligibility to registered permissions.
Account ↔ Profiles	Assignments in eligible domain context; IAM	Account uses an assigned, current selected profile.
Account ↔ Domain	Additional membership/scope binding where needed; IAM	Do not invent redundant direct assignments when domain is resolved through profile context.
Role ↔ Menu	Optional/additional relationship or constraint where implemented	Inspect current governing mappings; the proposed optional edge is not assumed to bypass permission/menu evaluation.
IAM Menu ↔ Axis Screen	1:1 intended bridge; bridge owned by IAM	Navigation targets the registered screen through IAM-owned mapping.
IAM Permissions ↔ Axis Controls	M:M bridge owned by IAM	Controls/actions are authorized through IAM, not an independent Axis policy model.
Axis Screen → Fields / Controls	1:M; Axis	Axis owns presentation metadata and its child control inventory.
Application user profile ↔ Account	1:1 intended business identity linkage	Personal/KYC profile is distinct from IAM access_profile; separate profile-boundary migration is not claimed complete here.

1. Authenticate and establish the current subject/session. A valid session does not itself select an authorized working profile.

- 2. Resolve eligible tenant/domain/profile assignments and select the intended context. Evaluate effective role membership for that profile.
- 3. Evaluate permissions and menu mappings with active/effective state, menu availability and applicable ABAC constraints. Construct authorized navigation from these results.
- 4. Follow the IAM-owned menu-to-Axis screen bridge and fetch the permitted screen/control metadata.
- 5. Apply field/control visibility, read-only and executable-action restrictions according to IAM decisions. Render labels/layout/formats from Axis.
- 6. Recheck authorization and current business state at the owner API. Client hiding or disabling a button is not the final authorization boundary.
- 7. Record attributable owner effects and decisions. If independent review is required, compare subject identities rather than only profile names.

The table expresses the requested relationship model and the source-reviewed principal mappings. It does not assert an unverified database constraint or a completed personal-profile migration. Use the actual principal-table reference below for implemented names.

CHAPTER 6

Principal schemas and IAM table crosswalk

This reference is for administrators and support engineers. Use the application’s governed APIs and screens for maintenance; table names are not instructions to edit authorization or review data directly. Physical names can differ from the conceptual model; the domain concept, for example, is represented by resp_scope in the supplied IAM reference.

Concept	Implemented tables	Boundary
Account identity	kh_iam.digital_subject kh_iam.user_account	IAM
Tenant membership	kh_iam.tenant_membership	IAM
Domain	kh_iam.resp_scope	IAM
Profile	kh_iam.access_profile	IAM
Domain ↔ Profile	kh_iam.access_profile_scope	IAM
Role / Profile ↔ Role	kh_iam.role kh_iam.access_profile_role	IAM
Permission / Role ↔ Permission	kh_iam.permission kh_iam.role_permission_grant	IAM
Registered operation	kh_iam.resource_action	IAM
User ↔ Profile in domain context	kh_iam.access_profile_asgn kh_iam.membership_scope_binding	IAM

Concept	Implemented tables	Boundary
Selected context	kh_iam.session kh_iam.session_access_profile_context	IAM
Menu master	kh_iam.menu	IAM
Permission ↔ Menu	kh_iam.menu_permission	IAM
Menu ↔ Axis Screen	kh_iam.menu_axis_screen	IAM-owned bridge
Menu availability window	kh_iam.menu_schedule	IAM
Screen / published version	kh_axis.page_def kh_axis.page_version	Axis
Screen → Controls / Fields	kh_axis.screen_control_registry	Axis
Permission ↔ Control	kh_iam.permission_axis_control	IAM-owned bridge
Field restrictions	kh_iam.field_access_rule	IAM
ABAC rules	kh_iam.policy_rule	IAM
Proposal and decision	kh_iam.access_request kh_iam.access_request_item kh_iam.access_approval_decision	IAM
Initial-access approval rule	kh_iam.client_approval_rule	IAM
Personal/business profile	Application/Core person and contact data; separate application-user-profile linkage migration	Application boundary; not access_profile

Owner	Schema / principal inspected objects	Use in diagnosis
Core	kh_core; model_publication; state_dimension/state_value/state_transiti on; reason_domain/reason_def/reason_applic ability	Compare exact captured model publication to the source definitions and bound consumer hash.
Tenant / TCP	kh_tenant; tenant_registration_request and tenant_registration_event in the onboarding implementation	Trace registration separately from lifecycle/environment/commercial evidence.
Axis	kh_axis; page_def, page_version, screen_control_registry	Find the presentation object independently of the IAM-owned bridges.
Regulix	kh_regulix native owner	Use canonical definition/instance IDs and current checkpoints; do not substitute uncorrelated legacy numeric IDs.
TimeVault	kh_timevault	Trace configured effective intervals, proposals and preserved decisions.
Custodia	kh_custodia	Trace custody identity/version/hash and protected lifecycle.

Owner	Schema / principal inspected objects	Use in diagnosis
Pulse / Vista	kh_pulse / kh_vista	Identify template/report/data definitions separately from generated results.
MEDES	kh_medes; exchange_case, case_command_receipt in member-case evidence	Trace case identity and immutable command receipts without exposing direct owner-table access.
Nexora	kh_nexora	Trace learning content, assignment and evidence under current authorization.
Scheduler	kh_ops_gov in the inspected enterprise manifest	Reuse owner job/version/trigger/queue/lease/run/attempt/checkpoint/retry/audit responsibilities; do not assume a new kh_scheduler schema.
Atlas / design-only modules	Use the accepted owner's current deployment/model reference	A specification physical model is not proof its tables are installed on the target environment.

CHAPTER 7

Dependency order for initial setup and controlled change

Stage	Owner work	Ready to proceed when	Next consumer
1 · Identity and tenant context	Confirm existing authorized administrators, current tenant scope and available module access.	An accountable operator can read the relevant master/configuration screens.	Core and configuration owners
2 · Shared business references	Create/select organization/person and controlled reference values; publish required state/reason models.	Stable authorized references and exact required publications exist.	Tenant, IAM/application profile and business owners
3 · Tenant onboarding	Registration, runtime/organization binding, identity, commercial, configuration and domain steps.	Owner evidence is current and attributable.	TCP
4 · Environment and lifecycle	Review deployment/configuration/placement/support; approve module grants; execute activation/restoration.	Current lifecycle and truth evidence support intended tenant/module use.	Protected business modules
5 · Access and presentation	Configure domain/profile/role/permission/menu relationships and Axis bridges/metadata.	Maker, reader and independent checker behavior is tested for the selected screen.	Module authoring and review

Stage	Owner work	Ready to proceed when	Next consumer
6 · Shared governed dependencies	Review native workflow/rules/assignments, custody classes/metadata and temporal masters as needed.	Exact eligible dependencies are available to the target business flow.	MEDES, content and learning work
7 · Data and content	Define/test source; create/review/publish dataset; compose report/dashboard/template; preview and review exact revision.	Consumer sees the published version and current authorized preview.	Execution and Scheduler
8 · Automation	Publish job, schedule/calendar or batch; confirm worker and execution identity.	One actual controlled run produces an inspected result.	Recurring operation
9 · Business journey and evidence	Run the intended MEDES/Nexora/content journey with distinct required identities.	Owner result, review, output and configured delivery evidence agree.	Operational handover and documentation

This order describes dependencies, not a requirement to recreate an existing installation. Reuse approved masters and published versions. If only a template changes, review the template successor and explicitly rebind its downstream jobs where intended; do not repeat tenant onboarding or recreate unrelated IAM masters.

CHAPTER 8

What to carry across every integration boundary

Information	Why it matters	Operator verification
Actor and scope	Identifies who requested work and the tenant/domain/profile or approved execution identity.	Check the current context and the producer's authorization; never trust a user-supplied tenant override as authority.
Business reference	Keeps case/member/request/record identity stable across modules.	Compare the same case/record at every handoff; similar names are insufficient.
Source artifact/version/hash	Pins the approved content or contract.	Compare published version and saved binding; diagnose drift rather than silently adopting a newer artifact.
Expected revision	Prevents decisions based on stale state.	Reload and reconcile if the current record changed.
Request/receipt/retry identity	Supports duplicate detection and attributable recovery.	Read an existing receipt after a lost response before submitting again.
Decision context	Explains who approved what and under which policy.	Check exact reviewed subject/version and independent identity.

Information	Why it matters	Operator verification
Producer result	Establishes the owner's actual outcome.	Follow the result reference; queue or transport acceptance is not final success.
Time and validity	Separates effective interval, expiry, schedule time and execution timestamps.	Compare UTC/local time and current evidence validity explicitly.
Failure/correlation reference	Connects UI symptom to owner/server diagnosis.	Capture safe error code, timestamp and correlation without credentials or private content.

These are conceptual evidence requirements, not a promise that all APIs use identical JSON property names. Each registered operation owns its actual input/result schema. Use its supplied selector and form instead of hand-entering invented identifiers or payload fields.

CHAPTER 9

Detailed component-to-component handoff catalog

Select a handoff to see the owner boundary, required checks and evidence. The scope label distinguishes a documented implementation path from a conditional registration or an architecture specification.

▼ 1. Kernel Core → Tenant Engine · Implemented guide flow

Contract aspect	Detail
Passed information	Responsible organization and contact references
Ownership rule	Core maintains party facts; Tenant associates the accountable organization.
Required checks	Eligible authorized lookup, correct kind/reference and current organization binding.
Evidence to retain	Party ID + tenant request/case + organization-binding result.
Evidence scope	Implemented guide flow

[Kernel Core](#) · [Tenant Engine](#)

▼ 2. Tenant Engine → Tenant Control Plane · Implemented guide flow

Contract aspect	Detail
Passed information	Approved tenant identity and current owner evidence
Ownership rule	Tenant supplies registration/identity/commercial/configuration facts; TCP evaluates lifecycle prerequisites.

Contract aspect	Detail
Required checks	Current evidence/version/validity, managed target scope and required environment facts.
Evidence to retain	Tenant/case + evidence versions + lifecycle readiness/result.
Evidence scope	Implemented guide flow

[Tenant Engine](#) · [Tenant Control Plane](#)

▼ 3. Tenant Control Plane → Kernel IAM · Ownership boundary; verify each consumer

Contract aspect	Detail
Passed information	Tenant/module eligibility and operating context
Ownership rule	Tenant entitlement establishes eligible module use; IAM determines the current user's authority.
Required checks	Current tenant state, grants, account/session and selected-profile assignments.
Evidence to retain	Current context + relevant entitlement + screen/action decision.
Evidence scope	Ownership boundary; verify each consumer

[Tenant Control Plane](#) · [Kernel IAM](#)

▼ 4. Kernel IAM → Kernel Axis · Implemented IAM/Axis guide

Contract aspect	Detail
Passed information	Authorized menu/screen/control identities
Ownership rule	IAM-owned bridges bind menu to screen and permission to controls; Axis supplies metadata.
Required checks	Selected profile role closure, read/action grants, ABAC, current mapping/active/effective state.
Evidence to retain	Menu/screen/control identity + current permit/deny response.
Evidence scope	Implemented IAM/Axis guide

[Kernel IAM](#) · [Kernel Axis](#)

▼ 5. Kernel Axis → Kernel MEDES · Shared-platform integration

Contract aspect	Detail
Passed information	Controlled screen presentation and operation bindings
Ownership rule	Axis renders labels/formats/controls; MEDES validates case action semantics.
Required checks	Published compatible presentation, IAM control decision and case state/scope.
Evidence to retain	Screen experience/delivery + case action/readback.
Evidence scope	Shared-platform integration

[Kernel Axis](#) · [Kernel MEDES](#)

▼ 6. Kernel IAM → Kernel MEDES · Implemented owner API/tests

Contract aspect	Detail
Passed information	Current subject/domain/profile and member/case authority
Ownership rule	IAM supplies access context; MEDES checks current linked business context and assignment.
Required checks	Tenant isolation, native permission, eligible member source and case relationship.
Evidence to retain	Authorized member/case result or denial; native operation correlation.
Evidence scope	Implemented owner API/tests

[Kernel IAM](#) · [Kernel MEDES](#)

▼ 7. Kernel TimeVault → Kernel Regulix · Configured Country/State flow

Contract aspect	Detail
Passed information	Pending effective-dated master proposal
Ownership rule	The configured native handoff routes independent review; the temporal owner applies the decision.
Required checks	Exact base version/interval, eligible reviewer and current request state.
Evidence to retain	Temporal request + native review/decision + resulting intervals.
Evidence scope	Configured Country/State flow

[Kernel TimeVault](#) · [Kernel Regulix](#)

▼ 8. Kernel IAM → Kernel TimeVault · Configured role governance

Contract aspect	Detail
Passed information	Role definition requiring preserved approval
Ownership rule	Role governance uses exact preserved definition evidence where configured.
Required checks	Current role revision/hash and required independent preservation decision.
Evidence to retain	Role reference/hash + temporal review history.
Evidence scope	Configured role governance

[Kernel IAM](#) · [Kernel TimeVault](#)

▼ 9. Kernel Core → Kernel Regulix · Explicit consumer binding required

Contract aspect	Detail
Passed information	Published state/reason model for a bound consumer
Ownership rule	Core evaluates the exact model; workflow/business owner decides and executes its transition.
Required checks	Current publication ID/hash, valid action/state/reason/narrative and owner binding.
Evidence to retain	Model evaluation + separate owner action/decision result.
Evidence scope	Explicit consumer binding required

[Kernel Core](#) · [Kernel Regulix](#)

▼ 10. Kernel Regulix → Kernel Custodia · Configured custody review

Contract aspect	Detail
Passed information	Version-bound document review task
Ownership rule	Regulix routes review; Custodia retains exact protected version and applies its owner lifecycle.
Required checks	Current assignee, different eligible reviewer, content/version and owner guards.
Evidence to retain	Task/decision + document/version + post-decision state.
Evidence scope	Configured custody review

▼ 11. Kernel Custodia → Kernel MEDES · Implemented MEDES guide

Contract aspect	Detail
Passed information	Admitted document/version/hash
Ownership rule	Custodia owns bytes/admission; MEDES records case association and sufficiency.
Required checks	Current case access, eligible class, current admitted version and integrity.
Evidence to retain	Case document link + custody receipt + business review.
Evidence scope	Implemented MEDES guide

▼ 12. Kernel MEDES → Kernel Regulix · Implemented MEDES review

Contract aspect	Detail
Passed information	Case/document/correspondence review context
Ownership rule	MEDES supplies the exact business subject; native workflow coordinates independent decision.
Required checks	Current business revision, assignment, submitting/reviewing subject and task state.
Evidence to retain	Case/item + native review task + decision + owner readback.
Evidence scope	Implemented MEDES review

▼ 13. Kernel MEDES → Kernel Pulse · Implemented correspondence guide

Contract aspect	Detail
Passed information	Published template and case data/recipient/channel intent
Ownership rule	MEDES owns case communication purpose; Pulse supplies versioned content and rendering.
Required checks	Current authorized case/dataset, exact eligible template version and recipient/attachment checks.

Contract aspect	Detail
Evidence to retain	Correspondence request + template/version + generated output/hash.
Evidence scope	Implemented correspondence guide

[Kernel MEDES](#) · [Kernel Pulse](#)

▼ 14. Kernel Pulse → Kernel Custodia · Configured output archival

Contract aspect	Detail
Passed information	Generated document bytes and integrity reference
Ownership rule	Custodia archives/admit/indexes exact output when the owner flow invokes the handoff.
Required checks	Hash/version integrity, custody policy and current access.
Evidence to retain	Generated output/hash + custody document/version receipt.
Evidence scope	Configured output archival

[Kernel Pulse](#) · [Kernel Custodia](#)

▼ 15. Kernel MEDES → Kernel Vista · Implemented MEDES reports

Contract aspect	Detail
Passed information	Authorized intake/review/correspondence/delivery projections
Ownership rule	MEDES remains the record owner; Vista presents permitted report results.
Required checks	Current tenant/profile/case scope, registered source and field eligibility.
Evidence to retain	Report source/filter + rows traceable to case/owner records.
Evidence scope	Implemented MEDES reports

[Kernel MEDES](#) · [Kernel Vista](#)

▼ 16. Kernel Pulse → Kernel IAM · Configured notification flow

Contract aspect	Detail
Passed information	Notification recipient and destination reference

Contract aspect	Detail
Ownership rule	The notification links to a target; IAM evaluates identity/context again after navigation/sign-in.
Required checks	Recipient match, current target permission and safe login return path.
Evidence to retain	Notification/item + authorized target or denial.
Evidence scope	Configured notification flow

[Kernel Pulse](#) · [Kernel IAM](#)

▼ 17. Kernel Pulse → Kernel Regulix · Configured task notifications

Contract aspect	Detail
Passed information	Notification task reference
Ownership rule	Pulse informs the recipient; Regulix owns assignment and task completion.
Required checks	Current recipient, assignee/delegate, task state and execution permission.
Evidence to retain	Task opens in authorized context; decision has a separate receipt.
Evidence scope	Configured task notifications

[Kernel Pulse](#) · [Kernel Regulix](#)

▼ 18. Kernel Vista → Kernel Pulse · Implemented Studio binding

Contract aspect	Detail
Passed information	Published dataset contract and current selected record/related rows
Ownership rule	Data owner retains facts; Pulse saves bindings and renders authorized values.
Required checks	Published eligible dataset, allowed fields, unique parent key, supported related binding.
Evidence to retain	Saved template binding + current-record preview/output.
Evidence scope	Implemented Studio binding

[Kernel Vista](#) · [Kernel Pulse](#)

▼ 19. Enterprise Scheduler → Kernel Vista · Registered operations

Contract aspect	Detail
Passed information	VISTA_REPORT_V1 / VISTA_DASHBOARD_V1 with pinned artifact
Ownership rule	Scheduler coordinates; Vista creates the actual report/snapshot.
Required checks	Published job/content, current Run as authority, data access and every dashboard tile.
Evidence to retain	Run/attempt + successful producer result + inspected output.
Evidence scope	Registered operations

[Enterprise Scheduler](#) · [Kernel Vista](#)

▼ 20. Enterprise Scheduler → Kernel Pulse · Registered generation operations

Contract aspect	Detail
Passed information	PULSE_EMAIL_V1 / PULSE_LETTER_V1 with record and inputs
Ownership rule	Scheduler coordinates generation; Pulse owns render/output.
Required checks	Matching channel, published template, exact record key and runtime authorization.
Evidence to retain	Run + READY output reference; no implied sending.
Evidence scope	Registered generation operations

[Enterprise Scheduler](#) · [Kernel Pulse](#)

▼ 21. Enterprise Scheduler → Kernel Nexus · specification + bounded connection capability · Bounded registered capability

Contract aspect	Detail
Passed information	NEXUS_SOURCE_REFRESH_V1 with published connection pin
Ownership rule	Registered source operation refreshes authorized snapshot.
Required checks	Current connection version/authentication reference, scope and supported contract/limits.
Evidence to retain	Run + actual refreshed snapshot result/time.
Evidence scope	Bounded registered capability

▼ 22. [Enterprise Scheduler](#) → [Kernel IAM](#) · Implemented Scheduler guide

Contract aspect	Detail
Passed information	Run as identity and execution context
Ownership rule	IAM supplies current authorization; the producer rechecks it at execution.
Required checks	Eligible execution identity/domain and operation/source permissions.
Evidence to retain	Job preview/execution context + current authorization result.
Evidence scope	Implemented Scheduler guide

[Enterprise Scheduler](#) · [Kernel IAM](#)

▼ 23. [Kernel Nexora](#) → [Kernel IAM](#) · Implemented learning guide

Contract aspect	Detail
Passed information	Learner/author/manager subject and permissions
Ownership rule	IAM controls role/context; Nexora checks content/audience/attempt ownership.
Required checks	Published content and eligible audience in the current scope.
Evidence to retain	Authorized learning/manager result or explicit denial.
Evidence scope	Implemented learning guide

[Kernel Nexora](#) · [Kernel IAM](#)

▼ 24. [Kernel Nexora](#) → [Kernel Vista](#) · Only where source is registered

Contract aspect	Detail
Passed information	Learning evidence through registered authorized report sources
Ownership rule	Nexora owns attempts/readiness; Vista presents permitted summaries.
Required checks	Actual source registration and current learner/manager data scope.
Evidence to retain	Report result traceable to owner learning records.

Contract aspect	Detail
Evidence scope	Only where source is registered

[Kernel Nexora](#) · [Kernel Vista](#)

▼ 25. Tenant Engine → Kernel Custodia · Configured evidence adapter

Contract aspect	Detail
Passed information	Identity-supporting document upload
Ownership rule	Custodia owns bytes and admission; tenant identity reviewer assesses sufficiency.
Required checks	Managed target, private-draft scope, exact evidence/version and admission.
Evidence to retain	Capture document/version/hash + identity evidence decision.
Evidence scope	Configured evidence adapter

[Tenant Engine](#) · [Kernel Custodia](#)

▼ 26. Tenant Control Plane → Kernel Custodia · Governed exit flow

Contract aspect	Detail
Passed information	Exit/retention/hold/disposition evidence references
Ownership rule	Custody and governance owners resolve obligations before lifecycle closure.
Required checks	Current holds, verified disposition receipts and accepted closure evidence.
Evidence to retain	Exit case + owner evidence + closure readback.
Evidence scope	Governed exit flow

[Tenant Control Plane](#) · [Kernel Custodia](#)

▼ 27. Kernel PGATE · specification → Kernel Nexus · specification + bounded connection capability · Specification; not full live acceptance

Contract aspect	Detail
Passed information	Admitted API/file exchange reference and correlation

Contract aspect	Detail
Ownership rule	Design: PGATE admits; Nexus orchestrates/transport.
Required checks	Design requires current gateway policy, identity, tenant, contract and permitted consumer.
Evidence to retain	Required proof: admission/rejection + exchange result with linked correlation.
Evidence scope	Specification; not full live acceptance

Kernel PGATE · specification · Kernel Nexus · specification + bounded connection capability

▼ 28. Kernel Nexus · specification + bounded connection capability → Kernel Custodia · Specification

Contract aspect	Detail
Passed information	Content reference and custody acceptance
Ownership rule	Design: Nexus can stage exchange data; Custodia remains long-term custody.
Required checks	Designed contract/classification/identity/retention rules and explicit handoff.
Evidence to retain	Required proof: transfer reference + custody acceptance/version/hash.
Evidence scope	Specification

Kernel Nexus · specification + bounded connection capability · [Kernel Custodia](#)

▼ 29. Kernel Nexus · specification + bounded connection capability → Kernel Regulix · Specification

Contract aspect	Detail
Passed information	Business workflow/policy decision reference
Ownership rule	Design: technical orchestration refers to business workflow authority.
Required checks	Current approved business definition and eligible decision/task context.
Evidence to retain	Required proof: integration execution + separate business decision.
Evidence scope	Specification

Kernel Nexus · specification + bounded connection capability · [Kernel Regulix](#)

▼ 30. Kernel Integrum · specification → Kernel Vista · Specification

Contract aspect	Detail
Passed information	Curated analytical dataset/product and semantic metric references
Ownership rule	Design: Integrum owns analytical preparation; Vista owns reports/execution/presentation.
Required checks	Published eligible data product, lineage/quality/privacy and current analytical access.
Evidence to retain	Required proof: data-product version/lineage + authorized report result.
Evidence scope	Specification

Kernel Integrum · specification · [Kernel Vista](#)

▼ 31. Kernel Nexus · specification + bounded connection capability → Kernel Integrum · specification · Specification

Contract aspect	Detail
Passed information	Governed analytical intake exchange
Ownership rule	Design: transport/admission separated from analytical ingestion and quality.
Required checks	Contract, source authority, schema, tenant, purpose and ingestion admission.
Evidence to retain	Required proof: exchange + landing/quality/curated lineage.
Evidence scope	Specification

Kernel Nexus · specification + bounded connection capability · Kernel Integrum · specification

▼ 32. Kernel Atlas → Kernel MEDES · Knowledge boundary

Contract aspect	Detail
Passed information	Versioned documentation claims and source/evidence links
Ownership rule	Atlas records knowledge; MEDES remains business/runtime authority.
Required checks	Correct module/edition, attributable source and evidence scope.

Contract aspect	Detail
Evidence to retain	Documentation trace to source; no implied runtime mutation.
Evidence scope	Knowledge boundary

[Kernel Atlas](#) · [Kernel MEDES](#)

CHAPTER 10

End-to-end MEDES crosswalk · case to reviewed communication

User stage	Owner action	Platform contribution	Evidence / failure routing
Open the member/case	MEDES resolves currently authorized business context.	IAM context; Tenant eligibility; Axis presentation.	Case/member identity and permitted read. A context denial belongs before intake/render diagnosis.
Receive documents	MEDES intake associates evidence with the case.	Custodia capture, admission, metadata and document versions.	Capture and admitted document/version/hash. Quarantine is not case acceptance.
Review evidence	Eligible independent reviewer decides the business item.	Regulix task/assignment and decision where configured.	Native review plus MEDES owner readback. Visible notification is not completion.
Create correspondence	Select current published template, recipient/channel and eligible attachments.	Pulse data binding and rendering; Custodia archival handoff.	Template/version + exact output/PDF hash + stored version.
Review generated item	Check exact PDF, recipient, channel and attachment authority.	Native independent review, current IAM and owner guards.	Decision pinned to the generated item; later correction creates new linked work.
Release and track	MEDES uses its configured delivery path.	Matching provider/channel, worker and native receipt/tracking.	Separate pending, acceptance and confirmed outcome. Parked live fax/print-mail activation remains explicit.
Respond and close work	Link replies/support activity to original item/case and require applicable confirmation.	Pulse notification/task destination and owner audit.	Response evidence and closure/reopen history. Sent communication alone is not a response.
Report and operate	Inspect authorized operational summaries and registered scheduled work.	Vista source projections; Scheduler only for supported registered operations.	Report rows trace to owner records. A general scheduler does not imply every MEDES action is schedulable.

The case is the narrative anchor. Each platform record adds a specific fact: who may act, which evidence version was used, which decision was made, what bytes were generated and what a provider actually did. Preserve these identities instead of collapsing the entire journey into one status label.

CHAPTER 11

End-to-end source → dataset → content → automation crosswalk

1. Define or pick an authorized source connection. Test the saved configuration and authentication reference, inspect fields and complete required review/publication. Refresh through the supported source operation and retain its result time.
2. Create or pick a dataset for the selected source(s). Select permitted fields and supported modeling operations. Preview types, keys, joins and row scope; save, independently review and publish under the current dataset policy.
3. Enter report/template/dashboard details before authoring. Start blank or select a meaningful template. Bind actual dataset fields, including optional/repeating cases. Inspect current saved preview rather than illustrative canvas values.
4. Submit the exact saved artifact for one independent review in the normal Pulse/Vista publication flow. The eligible checker obtains its current preview and decides. Publish only the approved version.
5. Run the published artifact manually and inspect actual report/dashboard/email/letter output. Confirm long/repeated content and pagination where relevant.
6. Create the matching Scheduler job, select Run as and exact published content, preview current inputs, independently review and publish the job. A dataset field input chooses one unique record/value; it is not implicit fan-out.
7. Run once and follow the actual producer result. Enable a reviewed schedule or start a reviewed batch only when the direct run is understood.
8. For a source-refresh batch, let content jobs depend on successful refresh. Do not assume a dependency transfers the report output into email or that a dashboard consumes the earlier report run.
9. For a content revision, publish its successor and explicitly update dashboard/job/schedule/batch dependencies through their lifecycle. Preserve earlier results and approvals.

Operation	Owner effect	Limit to explain
NEXUS_SOURCE_REFRESH_V1	Refresh published source snapshot	Bounded connection capability; not proof of every Nexus connector.
VISTA_REPORT_V1	Run published report	Current authorized data with the pinned report definition.
VISTA_DASHBOARD_V1	Run published dashboard	Every pinned tile must be available; partial is not complete success.
PULSE_EMAIL_V1	Generate published email output	Sending/delivery is separate.
PULSE_LETTER_V1	Generate published letter/PDF	Print/post/fax transport is separate.

Operation	Owner effect	Limit to explain
VISTA_RECOVERY_CLEANUP_V1 / PULSE_RECOVERY_CLEANUP_V1	Bounded expired private-recovery-copy maintenance	Not deletion of approved definitions, history or business records.

CHAPTER 12

Approval, publication, availability and temporal behavior

Concern	Rule to explain	What to inspect
Normal Vista/Pulse content	Draft → current saved preview → one independent review → publication.	Exact dataset/artifact revision, current preview and different eligible reviewer.
Dataset governance	Independent review is required by the latest user instruction.	Do not reuse earlier “save immediately available” guidance.
IAM changes	Access proposals/decisions stay attributable to their subject and origin record.	Current grant, pending change, decision and post-approval values.
Axis mapping ownership	Owner confirmation and separate independent decision can apply.	Author, responsible-role owner and reviewer identities; source/revision drift.
Business generated item	A reusable template approval may be followed by case-specific generated-item review.	Exact PDF/output, recipient and channel.
TimeVault	Decision time and effective interval are independent.	Current, future and historical values at the requested viewing date.
is_active / lifecycle	Availability does not replace review, publication, retirement or retention.	Consumer impact and eligible owner action; preserve historical decisions.
Originating grid	Use eligible contextual review actions where supplied.	A row action can be disabled for state, permission, ownership, assignment, preview or separation-of-duties reasons.

Do not apply one universal workflow length to every record type. The guide explains why a distinct business review may follow a template publication, while avoiding unnecessary repetition of the same content approval. The current owner flow and exact submitted object determine which decision is required.

CHAPTER 13

Recovery ownership and failure decision tree

Observed symptom	First boundary to inspect	Next action / evidence
401 / expired session	IAM authentication/session	Sign in through the intended environment; inspect saved record before retrying a prior submission.

Observed symptom	First boundary to inspect	Next action / evidence
Menu missing / 403	IAM effective context, mappings and ABAC	Record selected profile and target screen/action; distinguish missing navigation from denied read.
DB_EXEC_ERROR / 500	Failing owner operation and database/runtime trace	Capture request route, timestamp and correlation. Broad grants and repeated refreshes are not repairs.
Tenant registered but blocked	Tenant owner evidence and TCP readiness	Identify stale/missing identity/commercial/configuration/placement/grant fact.
Preview has wrong values	Source snapshot, dataset model/bindings and record key	Compare refresh time, source rows, key multiplicity and saved artifact revision.
PDF queued / unavailable	Render request, worker and producer result	Follow existing request; inspect processing/failure before resubmitting.
Review action missing	IAM action plus owner state/assignment/subject separation	Check exact pending request, current revision and eligible independent identity.
Job queued	Queue policy, worker heartbeat, overlap and capacity	Inspect admissions and leases; do not spawn duplicate runs.
Waiting external / uncertain effect	Producer/provider result and reconciliation	Preserve attempts and reconcile before retry/resend.
Document present but business incomplete	Custodia admission plus MEDES/owner review	Trace the actual document version and separate business decision.
Unexpected future/current value	TimeVault interval and viewing date	Compare boundary convention and actual approved timeline.
External connector not in selector	Registered operation/capability and environment activation	A design catalog entry does not make a transport executable.

The recovery record should identify the first failing boundary, not merely the page where the failure became visible. Keep original attempts, errors and receipts. If the outcome is uncertain, determine whether a side effect already occurred before repeating it. Use a controlled fixture to verify failure handling; avoid interrupting shared services.

CHAPTER 14

Change-impact and version adoption checklist

Changed owner record	Potential consumers	Required check
Tenant commercial/configuration evidence	TCP readiness, entitlements and signed truth	Refresh current evidence and review exact new bindings.

Changed owner record	Potential consumers	Required check
IAM assignment/role/permission/menu bridge	Navigation, screen read, controls and producer execution	Re-evaluate selected context and both permitted/denied behavior; do not add static fallback menus.
Axis source inventory or label/mapping	Pending reviews, experience and delivery	Resolve invalidation and publish/activate eligible successor.
Rule/process/assignment	New governed consumers and instances	Bind exact approved successor; inspect existing instance pin behavior.
Country/State interval	Date-sensitive master consumers	Preview every affected interval and parent association.
Source/dataset contract	Report/template bindings and scheduled inputs	Inspect field/type/key/authorization changes and obtain affected reviews.
Report version	Dashboard tiles and report jobs	Explicitly adopt the intended published version.
Template version	Generation jobs and business correspondence selection	Rebind jobs/consumers through governance; do not alter existing generated bytes.
Calendar/job version	Schedules and batches	Review timezone/version/dependency impact and upcoming dates.
Document version/classification/access	Business review, attachments, shares and exports	Recheck exact content authority; preserve old decision evidence.
Provider credential/reference	Source refresh, transport or registered operation	Test the actual configured integration without exposing secrets; inspect uncertain prior effects.

CHAPTER 15

Current governance and documentation handoffs

Owner	Handoff / expected evidence
IAM → Axis	Approved menu/page/control permissions and selected role/profile; screen publication does not create grants.
Axis → business screen	Approved screen title/help and owning control labels/formats; pending proposals leave current presentation effective.
IAM → domain/profile assignment	A new domain starts empty; explicit reviewed domain-profile mapping precedes the user assignment.
Pulse → originating record	Recipient-checked notification opens the current record/outcome; read state is separate from the business decision.
Administrator → audit	Named same-person exception is recorded, scoped and effective only for the selected authorized administrator profile.

Owner	Handoff / expected evidence
MEDES → release owner	Technical installation requires activation; role grants, APIs, workflow and provider dependencies are separate entry gates.
Documentation → UAT	The manual explains operation; the demo supplies the presentation sequence; the UAT pack holds executable cases and actual evidence. Documentation browser checks do not certify application business journeys.