CS-DOC-0002 · GXP-DESK DOCUMENTATION

Concepts: Account, Tenant, System, Change.

FIT-only redaction. Effective 2026-06-04.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0002	v1.0	2026-06-04	Customer Success

Public — Documentation · Review cycle: On change

01 — DOCUMENT CONTROL

Control block and metadata anchor.

The control block identifies the document, its current revision, the regulated process it supports, and the people accountable for its lifecycle. Every value below is the source of truth for any downstream record, audit trail entry, or signature block.

DOCUMENT ID	CS-DOC-0002
TITLE	Concepts: Account, Tenant, System, Change
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-06-04
REVIEW CYCLE	On change
DOCUMENT OWNER	Customer Success
CLASSIFICATION	Public — Documentation
RELATED RECORDS	—
SUPERSEDES	— (initial release)

02 — APPROVALS

Sign-off table, ready for ink or e-signature.

The signatures below confirm review and authorisation of this document. Approvals must be recorded in chronological order. If the document is signed electronically, the e-signature record on the GxP-Desk platform supersedes any handwritten entry on this page and carries the same legal weight under 21 CFR Part 11 and EU GMP Annex 11.

Role	Name	Function	Date	Signature
Author		Validation Lead		
Reviewer		Quality Assurance		
Reviewer		Process / System Owner		
Approver		Head of Quality		
Approver		Regulatory Affairs		

03 — CONTENTS

What's in this document.

01 — WHAT THIS VERSION COVERS

What this version covers.

This documentation addresses the four primitives that structure every regulated record in GxP-Desk:

- **Account** — the legal and contractual anchor entity
- **Tenant** — the GxP-responsible operating unit within an account
- **System** — the validated computerized application
- **Change** — the controlled unit of validation work

The hierarchy, field structure, lifecycle, governance, and mapping to 21 CFR Part 11, EU GMP Annex 11, and GAMP 5 are described.

02 — WHAT THIS VERSION DOES NOT COVER (ROADMAP TOPICS)

What this version does NOT cover (roadmap topics).

The following concepts from the original spec are not implemented and are not described:

- **Data Residency UK/CA/CH** — EU/US are implemented via `Tenant.dataRegion` (physically separated regional DBs, NEW 2026-06-04); the further Enterprise options UK/Canada/Switzerland are not code-verified.
- **Subscription Tiers (Site/Network/Enterprise) as enforcing logic** — The `subscriptionPlan` field exists on `Account`, but no tier-specific validation rules are implemented.
- **Master e-signature meanings as a configurable library** — Only static texts in the documentation are implemented.
- **Sealed flag and head-of-chain hash on Change** — Not present in the Change model.
- **Tenant branding (other than logo:String)** — Only the `logo` field exists.

03 — THE FOUR PRIMITIVES AT A GLANCE

The four primitives at a glance.

Account — the legal anchor entity

An **Account** represents the legal person that holds the GxP-Desk contract. There is exactly one account per Master Services Agreement. All underlying tenants, systems, and changes operate under this single legal relationship.

What an account owns:

- **Legal entity** — the signatory of the MSA and DPA
- **Billing relationship** — the `subscriptionPlan` field (e.g., "free", "professional", "enterprise"), billing email, status
- **Identity perimeter** — the email domain of the account users; the account owner's responsibility for onboarding
- **Account audit trail** — records of every tenant creation, status change, and account-administrator action
- **Master configuration** — defaults applied to all tenants unless overridden

Account fields (Prisma):

```
id, name, slug, type, subscriptionPlan, billingEmail, status, createdAt, updatedA
t
```

Lifecycle of an account:

01 **Provisioning** — Customer Success creates the account from the signed MSA. The account owner is the first user.

02 **Operation** — The account persists as a stable identity. Tenants are created and deleted beneath it; the MSA-level audit trail accumulates.

03 **Renewal** — Subscription renewal does not create a new account — it extends the existing one. Tier changes are captured as audit-log entries.

04 **Termination** — Requires written notice and a documented data-egress plan. The account moves to the **Terminated** status for the contractually agreed retention period. During this window the account is read-only.

Tenant — the GxP unit

A **Tenant** represents the operating unit that bears GxP responsibility. This is the level at which the Quality Management System (QMS) lives, where data residency is decided, and where the regulator inspects. A tenant is always the **inspectable** unit.

What a tenant owns:

- **Quality Management System scope** — the SOPs, training materials, and policy library applied to the systems registered under this tenant
- **Tenant user management** — either federated from the account SSO or provisioned independently. Permissions at the tenant level cascade to System and Change
- **Inspection-ready exports** — tenant-scoped audit-log export, validation-package export, training-records export
- **Localization & compliance defaults** — language, timezone, document prefix, change prefix, retention period, e-signature requirement

Tenant fields (Prisma):

```
id, name, slug, description, logo, status, accountId, createdAt, updatedAt
```

TenantSettings fields:

```
id, tenantId, aiProvider, aiModel, language, timezone, dateFormat,
documentPrefix, changePrefix, requireESignature, retentionPeriodDays,
enableRiskManagement, enableTraining, enableSupplierMgmt
```

Lifecycle of a tenant:

01 **Created** — by an account administrator following a documented business rationale (typically: a new site, subsidiary, or CMO relationship)

02 **Configured** — with localization, SSO model, default templates, retention policy

03 **Operation** — systems and changes accumulate. The tenant audit log captures every role change and every system-lifecycle event

04 **Archived** — When the operating unit is dissolved (site closure, divestiture), the tenant moves to **Archived**. All data becomes read-only. The audit-log export remains available for the retention window

System — the validated application

A **System** is a computerized application that performs a GxP-relevant function and is therefore subject to validation. Most systems are commercial software: an EDMS, a LIMS, an ERP module, an MES. Some are in-house developments. Some are spreadsheets that the regulator classifies as computerized systems.

What a system owns:

- **Functional scope** — the intended-use statement, the GxP processes the system supports, the data it produces or transforms
- **GAMP 5 category** (Int field) — Cat 1 (infrastructure), Cat 3 (non-configured COTS), Cat 4 (configured COTS), Cat 5 (custom/bespoke). Drives the required validation depth for each change
- **Risk profile** — the cumulative residual risk after the most recent risk assessment

- **Configuration baseline** — the current configuration version under which the system is qualified
- **Periodic review schedule** — schedule (annual, semi-annual, risk-based). The platform schedules automatically and tracks the next due date
- **Decommissioning plan** — documented at system creation, executed at retirement, on the audit trail forever

System fields (Prisma):

```
id, name, description, gampCategory (Int), status (String),
customerId/tenantId, createdAt, updatedAt
```

System lifecycle states:

State	Allowed	Not allowed	Audit-trail entry
Draft	Edit metadata, attach pre-validation documents	Create changes, generate validation reports	System Created (Tenant Owner signature)
In Initial Validation	Run the initial-validation change	Use the system for GxP work	System Initial Validation Started
Production	Use the system for GxP work; create changes (upgrade, configuration, periodic review)	Edit system metadata without a change	System Released to Production
Periodic Review Due	Run the periodic-review change	Skip the review and remain in Production	Periodic Review Triggered
In Change	Run the open change	Open a parallel change against the same system (anti-pattern)	Change Opened
Retired	Read-only access to history; data export	Use the system for GxP work; open changes	System Retired (decommissioning change closed)

Change — the unit of work

Everything you actually **do** on the platform happens inside a **Change**. A change is a controlled, time-bound container for a validation activity against a system: the initial validation, an upgrade, a configuration change, a periodic review, or a retirement. It is the unit in which approvals are routed, deviations are tracked, and the validation package is sealed.

Anatomy of a change:

Component	Purpose
Change Number	Tenant-unique, deterministic, never reused. Format: e.g., `EDMS■CHG■001`

Component	Purpose
Change Type	INITIAL_VALIDATION / MINOR / MAJOR / EMERGENCY. Drives the deliverable matrix
Title, Description	Free text. Required when opening the change
Regulatory Justification	Free text. Rationale. Visible in every downstream record
Status	DRAFT → SUBMITTED → APPROVED → IN_PROGRESS → COMPLETED → CLOSED (or REJECTED)
Priority	LOW / MEDIUM / HIGH / CRITICAL
Current Phase	Tracks the current validation-process state
isInitialValidation	Boolean flag marking initial-validation changes
Target Date, Implemented Date, Closed Date	Time-based milestones
Associated Documents	URS, Risk, Validation Plan, IQ/OQ/PQ, Traceability Matrix, Validation Report

Change fields (Prisma):

```
id, changeNumber, title, description, justification, type, status, priority,
systemId, requestedById, assignedToId, currentPhase, isInitialValidation,
targetDate, implementedDate, closedDate, createdAt, updatedAt
```

Change lifecycle states:

State	Description	Who can advance it
Draft	The change is being scoped. No deliverables yet. No e-signatures	Author
Plan Phase	URS, Risk, and Validation Plan are written and reviewed	Author + Reviewer; QA gates control progression
Plan Approved	All Plan-phase deliverables are QA-approved. Test execution can start	QA Approver (signs the gate)
Execute Phase	IQ/OQ/PQ are executed; deviations are raised, tracked, and closed	Test Author + Reviewer; QA gates control progression
Execute Complete	All test deliverables are approved. Outstanding deviations are closed or documented as residual risk	QA Approver (signs the gate)
Report Phase	The Validation Report is drafted; it recommends Acceptance / Conditional Acceptance / Rejection	Author + Reviewer

State	Description	Who can advance it
Closed	The VR is approved; the change is sealed; all records are locked. Audit-trail entry: "Change Closed"	Head of Quality (closes the change)
Cancelled	The change is abandoned before closure. The reason is captured. Records remain, are flagged as "Cancelled", and can never be deleted	QA Approver

04 — HIERARCHY, INHERITANCE, AND OVERRIDES

Hierarchy, inheritance, and overrides.

Configuration cascades top-down. The account sets defaults. The tenant overrides any default that the GxP unit must set independently (often: localization, retention window). The system overrides values the validated application requires (often: GAMP 5 category, periodic-review cycle). The change cannot override anything that would weaken an earlier approval — it can only strengthen.

Setting	Default on	Overridable on	Strengthen only?
Language	Tenant (de)	—	—
Timezone	Tenant (Europe/Berlin)	—	—
Document prefix	Tenant (DOC)	—	—
Change prefix	Tenant (CR)	—	—
Require E-Signature	Tenant (true)	—	—
Retention Period Days	Tenant (3650)	System	Yes (shorter only)
GAMP 5 Category	System	—	No (but a downgrade requires QA + rationale)
Risk Class	System	Change	No (but an upgrade triggers re-validation)
Periodic Review Cycle	System	System (with QA)	Yes (shorter only)

05 — WALKED EXAMPLE

Walked Example.

Acme Pharmaceuticals signs an MSA — an **Account**. They register their Boston manufacturing site as a **Tenant** with US localization and their Dublin site as a second **Tenant** with EU localization. Both inherit Acme's account-level SSO. The Boston tenant registers its **EDMS** as a system (GAMP 5 Cat 4, High Risk). The initial validation of the EDMS is the first **Change** against this system. Six months later the EDMS vendor releases version 4.2; Acme opens an upgrade **Change**. One year after go-live, the platform schedules a periodic-review **Change**. The audit trail at every level — Account, Tenant, System, Change — captures every transition. An FDA inspector visits Boston; the Boston tenant exports its complete validation history at the press of a button. Dublin's data is not touched.

06 — PERMISSIONS, SET AT A LEVEL, SAFELY INHERITED

Permissions, set at a level, safely inherited.

Permissions are evaluated at the lowest level at which a value is set. A user with **QA Approver** at the tenant level inherits that role on every system and every change beneath it. A user can be granted a **narrower** scope on a specific system (e.g., **Read-Only** on a system where they have a conflict of interest) — never a broader one.

Separation of Duties (SoD):

GxP-Desk enforces SoD at the change level:

- The person who **writes** a deliverable cannot **approve** the same deliverable
- The person who **executes** a test cannot **approve** the test result

These rules are hard-wired and cannot be relaxed at the change level — only strengthened.

SoD rule	Default	Hardwired in code?
Author ≠ Reviewer	Always enforced	Yes
Author ≠ Approver	Always enforced	Yes
Test Executor ≠ Test Approver	Always enforced	Yes

07 — AUDIT TRAIL — ALCOA+ AT EVERY LEVEL

Audit Trail — ALCOA+ at every level.

Each of the four primitives maintains its own audit-trail stream. Records on a stream are tamper-evident, append-only, and UTC-timestamped. ALCOA+ principles are applied at every level — the difference is the **retention horizon**.

Level	ALCOA+ scope	Retention horizon
Account	Identity, billing events, MSA changes, tenant lifecycle	Lifetime of the account; configurable retention floor — the Enterprise tier supports unlimited
Tenant	User & role lifecycle, system-lifecycle events, retention-policy changes	Lifetime of the tenant; bounded by the tenant retention policy
System	Configuration-baseline changes, GAMP 5 category changes, periodic-review records	Lifetime of the system; extensible per regulatory requirement
Change	Every authoring, review, and approval event, deviation, and test-result event during the change	From change opening to change closing; thereafter retained by the tenant retention policy

ALCOA+ mapping:

ALCOA+ attribute	How the platform satisfies it
Attributable	Every record carries the authenticated user, the session ID, and the IP address at the time of writing (no device fingerprinting)
Legible	Records render in human-readable HTML/PDF without platform access; exports are W3C-compliant for inspector review
Contemporaneous	A server-side UTC timestamp on write; client-supplied timestamps are recorded but never trusted as primary
Original	The first persistent version is preserved verbatim; subsequent edits create new versions linked to the original without overwriting it
Accurate	Schema validation on write; controlled-vocabulary fields prevent free-text drift

ALCOA+ attribute	How the platform satisfies it
Complete	No record exists without its required parents (no orphan records). Audit-trail entries are written in the same transaction as the record
Consistent	Cross-record references are foreign-key-controlled; the platform refuses to seal a change with broken refs
Enduring	Audit-trail storage is replicated across availability zones with daily integrity checks
Available	Tenant-scoped audit-log export is a single button press. Records remain available read-only for the full retention window, even after tenant archiving

Regulatory Mapping.

21 CFR Part 11

Part 11 clause	Primitive that satisfies it
§ 11.10(a) Validation	System (GAMP 5 cat) + Change (Validation Plan, IQ/OQ/PQ, VR)
§ 11.10(b) Accurate copies	Tenant (export tools) + Change (sealed records)
§ 11.10(c) Record retention	Account (default) + Tenant (override)
§ 11.10(d) Limit access	Account (SSO) + Tenant (roles)
§ 11.10(e) Audit trail	Streams across all four levels
§ 11.10(g) Authority checks	Tenant (roles) + Change (SoD)
§ 11.50 / 11.70 / 11.200 (e-signatures)	Account (signature meaning library) + Change (signed records)

EU GMP Annex 11

Annex 11 section	Primitive that satisfies it
1. Risk management	System (Risk Class) + Change (Risk Assessment per ICH Q9)
2. Personnel	Tenant (training records, role assignments)
3. Suppliers and service providers	Account (quality agreement); Tenant (per-site supplier qualification)
4. Validation	Change (Validation Plan, IQ/OQ/PQ, VR, Traceability Matrix)
5. Data	System (data classification) + audit-trail streams across all four levels
9. Audit trail	Streams across all four levels
10. Change and configuration management	Change (states + sealed records)
11. Periodic evaluation	System (schedule) + Change (periodic-review change)

Annex 11 section	Primitive that satisfies it
12. Security	Account (Argon2 password hashing, JWT sessions) + Tenant (roles, SoD enforcement, permission guards)
14. Electronic signature	Change (signed deliverables with hash binding)

GAMP 5 (2nd edition, 2022)

GAMP 5 is a lifecycle framework, not a clause-by-clause rule. The four primitives map its lifecycle as follows: **System** defines the validation depth (via the GAMP 5 category); **Change** executes one pass of the V-model; **Tenant** holds the supplier-qualification artifacts; **Account** holds the quality agreement with the platform vendor.

09 — CODE REFERENCES

Code references.

Prisma models

- `Account` — top-level entity with `name`, `slug`, `type`, `subscriptionPlan`, `billingEmail`, `status`
- `AccountSettings` — ai-configuration per account (aiProvider, aiModel, openai/anthropic/gemini API keys, aiTemperature, aiMaxTokens)
- `Tenant` — operational unit with `name`, `slug`, `accountId`, `status`, `logo`
- `TenantSettings` — tenant-level defaults (language, timezone, dateFormat, documentPrefix, changePrefix, requireESignature, retentionPeriodDays, feature flags)
- `TenantUserAssignment` — M2M between User and Tenant with roleId
- `System` — validated application with `name`, `gampCategory` (Int), `status`, `tenantId/customerId`
- `Change` — unit of work with `changeNumber`, `title`, `description`, `type`, `status`, `systemId`, `requestedById`, `assignedToId`, `currentPhase`, `isInitialValidation`, `targetDate`, `closedDate`

Server actions

- `app/actions/account/*` — account creation, settings, audit-trail retrieval
- `app/actions/tenant/*` — tenant lifecycle, settings, user assignments
- `app/actions/system/*` — system registration, metadata, status transitions
- `app/actions/change/*` — change opening, phase transitions, closures

Documentation

- All documents are stored in the `Document` table with a `changeId` or `systemId` foreign key
- `DocumentSection` carries `aiDraft`, `content`, `isLocked`, `lastModifiedById` to support AI assistance and audit
- Signature workflows are modeled in `SignatureWorkflow` and `SignatureStep`

End of documentation

REVISION HISTORY

Every change, tracked and signed.

Add one row for every controlled revision. Minor changes (typos, formatting) increment the patch version; substantive edits trigger a fresh review cycle and a new approver round.

Version	Date	Author	Summary of Change	Approver
1.0	2026-06-04	Documentation Team	FIT-only redaction limited to codebase-verified functionality.	Head of Documentation
—	—	—	Reserved for next revision. Do not delete this row.	—

GLOSSARY

Shared language, no ambiguity.

Definitions used throughout this document. Where a term has a specific meaning inside GxP-Desk, the platform-specific definition takes precedence over the generic regulatory term.

CSV	Computerized Systems Validation
GAMP 5	Good Automated Manufacturing Practice, Edition 5 (2nd edition, 2022)
GxP	Good 'x' Practice — covers GMP, GLP, GCP, GDP, GVP
IQ / OQ / PQ	Installation / Operational / Performance Qualification
Part 11	21 CFR Part 11 — US FDA rule on electronic records and electronic signatures
Annex 11	EU GMP Annex 11 — EU rule on computerised systems
URS	User Requirements Specification
FRS	Functional Requirements Specification
RTM	Requirements Traceability Matrix
SOP	Standard Operating Procedure
ALCOA+	Attributable, Legible, Contemporaneous, Original, Accurate (+ Complete, Consistent, Enduring, Available)
ICH Q9	International Council for Harmonisation Quality Risk Management guideline

— End of document —