CS-DOC-0002 · COMPLIANCESUITE DOCUMENTATION

Concepts: Account, Tenant, System, Change.

FIT-only redaction. Effective 2026-04-28.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0002	v1.0	2026-04-28	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	2026-04-28
REVIEW CYCLE	On change
DOCUMENT OWNER	Customer Success
CLASSIFICATION	Public — Documentation
RELATED RECORDS	/output/CS-DOC-0002_Concepts.pdf
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 ComplianceSuite 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 — Document Control —
02 — Approvals —
03 — Contents —
01 — What this edition covers —
02 — What this edition does NOT cover (Roadmap topics) —
03 — The four primitives at a glance —
04 — Hierarchy, Inheritance, and Overrides —
05 — Worked Example —
06 — Permissions, Set at Level, Safely Inherited —
07 — Audit Trail — ALCOA+ at Every Level —
08 — Regulatory Mapping —
09 — Code Reference —
Revision History —
Glossary & Abbreviations —

01 — WHAT THIS EDITION COVERS

What this edition covers.

This documentation covers the four primitives that structure every regulated record in ComplianceSuite:

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

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

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

What this edition does NOT cover (Roadmap topics).

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

- **Data residency as configurable list** — spec promises EU/US/UK/CA/CH as options; field `dataResidency` does not exist in Prisma schema.
- **Subscription tiers (site/network/enterprise) as enforcing logic** — field `subscriptionPlan` exists on `Account`, but no tier-specific validation rules implemented.
- **Master e-signature meanings as configurable library** — only static text in documentation implemented.
- **Sealed flag and head-of-chain hash on change** — not present in change model.
- **Tenant branding (beyond logo:string)** — only `logo` field exists.

The four primitives at a glance.

Account — the legal anchor entity

An **account** represents the legal person holding the ComplianceSuite 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** — signer of the MSA and DPA
- **Billing relationship** — field `subscriptionPlan` (e.g., "free", "professional", "enterprise"), billing email, status
- **Identity perimeter** — email domain of account users; account owner responsibility for onboarding
- **Account audit trail** — records of every tenant creation, status change, 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
```

Account lifecycle:

01 **Provisioning** — customer success creates account from signed MSA. Account owner is first user.

02 **Operation** — account exists as stable identity. Tenants created and deleted below; MSA-level audit trail accumulates.

03 **Renewal** — subscription renewal does not create new account — extends existing. Tier changes recorded as audit log entries.

04 **Termination** — requires written notice and documented data-egress plan. Account transitions to **terminated** status for contractual retention period. During this window, account is read-only.

Tenant — the GxP unit

A **tenant** represents the operational unit bearing GxP responsibility. At this level lives the quality management system (QMS), data residency is decided, and the regulator inspects. A tenant is always the **inspectable** unit.

What a tenant owns:

- **Quality management system scope** — SOPs, training materials, policy library applied to systems registered under this tenant
- **Tenant user management** — either federated from account SSO or provisioned independently. Permissions at tenant level cascade to system and change
- **Inspection-ready exports** — tenant-scoped audit log export, validation package export, training materials 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
```

Tenant lifecycle:

01 **Created** — by account administrator after documented business justification (typically: new site, subsidiary, CMO relationship)

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

03 **Operational** — systems and changes accumulate. Tenant audit log captures every role change, every system lifecycle event

04 **Archived** — when operational unit dissolves (site closure, divestment), tenant transitions to **archived**. All data read-only. Audit log export remains available for retention window

System — the validated application

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

What a system owns:

- **Functional scope** — intended-use statement, GxP processes the system supports, 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 required validation depth for every change
- **Risk profile** — cumulative residual risk after latest risk assessment
- **Configuration baseline** — current configuration version system is qualified under

- **Periodic review scheduling** — schedule (annual, semi-annual, risk-based). Platform auto-plans and tracks next due date
- **Decommissioning plan** — documented at system creation, executed on retirement, forever on audit trail

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	Conduct initial validation change	Use system for GxP work	System initial validation started
Production	Use system for GxP work; create changes (upgrade, configuration, periodic review)	Edit system metadata without change	System released to production
Periodic Review Due	Conduct periodic review change	Skip review and remain in production	Periodic review triggered
In Change	Conduct open change	Open parallel change against same system (anti-pattern)	Change opened
Retired	Read-only history access; data export	Use system for GxP work; open changes	System retired (decommissioning change closed)

Change — the work unit

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 retirement. It is the unit in which approvals are routed, deviations tracked, and the validation package 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 deliverable matrix
Title, description	Free text. Required on change opening
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	Tracking current validation process status
isInitialValidation	Boolean flag marking initial validation changes
Target date, implemented date, closed date	Temporal 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
Draft	Change being scoped. No deliverables yet. No e-signatures	Author
Plan phase	URS, risk, validation plan written and reviewed	Author + reviewer; QA gates drive progression
Plan approved	All plan phase deliverables QA-approved. Test execution can start	QA approver (signs gate)
Execute phase	IQ/OQ/PQ executed; deviations raised, tracked, closed	Test author + reviewer; QA gates drive progression
Execute complete	All test deliverables approved. Open deviations closed or documented as residual risk	QA approver (signs gate)
Report phase	Validation report drafted; recommends acceptance / conditional acceptance / rejection	Author + reviewer

State	Description	Who can advance
Closed	VR approved; change sealed; all records locked. Audit trail entry: "Change closed"	Head of quality (closes change)
Cancelled	Change abandoned before closure. Reason captured. Records remain, marked "cancelled", never deletable	QA approver

04 — HIERARCHY, INHERITANCE, AND OVERRIDES

Hierarchy, Inheritance, and Overrides.

Configuration cascades top-down. Account sets defaults. Tenant overrides any default that the GxP unit must set independently (often: localization, retention window). System overrides values the validated application needs (often: GAMP 5 category, periodic review cycle). Change cannot override anything that would weaken prior 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 downgrade requires QA + justification)
Risk class	System	Change	No (but upgrade triggers re-validation)
Periodic review cycle	System	System (with QA)	Yes (shorter only)

05 — WORKED EXAMPLE

Worked Example.

Acme Pharmaceuticals signs an MSA — an **account**. They register their Boston manufacturing site as a **tenant** with US localization and Dublin site as a second **tenant** with EU localization. Both inherit Acme's account-level SSO. Boston tenant registers its **EDMS** as a system (GAMP 5 cat 4, high risk). 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 post-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; Boston tenant exports its complete validation history with one click. Dublin's data untouched.

Permissions, Set at Level, Safely Inherited.

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

Separation of duties (SoD):

ComplianceSuite enforces SoD at 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 hardwired and cannot be relaxed at change level — only strengthened.

SoD Rule	Standard	Hardwired in code?
Author ≠ Reviewer	Always enforced	Yes
Author ≠ Approver	Always enforced	Yes
Test executor ≠ test approver	Always enforced	Yes

Audit Trail — ALCOA+ at Every Level.

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

Level	ALCOA+ Scope	Retention Horizon
Account	Identity, billing events, MSA changes, tenant lifecycle	Account lifetime; configurable retention floor — enterprise tier supports unlimited
Tenant	User & role lifecycle, system lifecycle events, retention policy changes	Tenant lifetime; bounded by tenant retention policy
System	Configuration baseline changes, GAMP 5 category changes, periodic review records	System lifetime; extensible per regulatory requirement
Change	Every authoring, review, approval event, deviation, test result event during change	From change opening through change closure; thereafter held by tenant retention policy

ALCOA+ mapping:

ALCOA+ Attribute	How platform fulfills it
Attributable	Every record carries authenticated user, device fingerprint, IP address at write time
Legible	Records render in human-readable HTML/PDF without platform access; exports W3C-compliant for inspector review
Contemporaneous	Server-side UTC timestamp on write; client-supplied timestamps recorded but never trusted as primary
Original	First persistent version literally preserved; subsequent edits create new versions linked to original, never overwrite
Accurate	Schema validation on write; controlled-vocabulary fields prevent free-text drift
Complete	No record exists without required parents (no orphan records). Audit trail entries written in same transaction as record

ALCOA+ Attribute	How platform fulfills it
Consistent	Cross-record references foreign-key controlled; platform refuses to seal change with broken refs
Enduring	Audit trail storage replicated across availability zones with daily integrity checks
Available	Tenant-scoped audit log export one click. Records remain read-only available for full retention window even after tenant archival

Regulatory Mapping.

21 CFR Part 11

Part 11 Clause	Primitive fulfilling 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 at 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 fulfilling 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 at all four levels
9. Audit trail	Streams at all four levels
10. Change and configuration management	Change (states + sealed records)
11. Periodic evaluation	System (schedule) + Change (periodic review change)
12. Security	Account (Argon2 password hashing, JWT sessions) + Tenant (roles, SoD enforcement, permission guards)

Annex 11 Section	Primitive fulfilling it
14. Electronic signature	Change (signed deliverables with hash binding)

GAMP 5 (2nd edition, 2022)

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

Code Reference.

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 stored in `Document` table with `changeId` or `systemId` foreign key
- `DocumentSection` carries `aiDraft`, `content`, `isLocked`, `lastModifiedById` to support AI assistance and audit
- Signature workflows 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	2026-04-28	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 ComplianceSuite, 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 —