CS-DOC-0001 · COMPLIANCESUITE DOCUMENTATION

Quickstart for Validation Managers.

This edition contains only functions that have been verified in the codebase. Onboarding functions (account verification via DNS, SSO auto-setup, SCIM activation) and provisioning flows have been removed.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0001	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-0001
TITLE	Quickstart for Validation Managers
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-04-28
REVIEW CYCLE	On change
DOCUMENT OWNER	Customer Success
CLASSIFICATION	Public — Documentation
RELATED RECORDS	Complete roadmap version in /output/CS-DOC-0001_Quickstart.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 — WHAT THIS EDITION COVERS

What this edition covers.

This edition guides a validation manager from an existing account creation through first tenant creation, system registration, and initial validation change to e-signature closure. The focus is on the actually implemented core workflow.

What this edition does NOT cover.

The following onboarding functions have been removed:

- **Account verification via DNS TXT:** Spec promises verifiable ownership, code does not implement it — only account creation and tenant provisioning.
- **SSO auto-setup flows:** Spec shows SAML/OIDC/SCIM wizard; code not implemented.
- **SCIM provisioning activation:** Not in code; identity management remains customer responsibility.
- **Customer success provisioning:** MSA/DPA pre-check, provisioning state, approval workflow — not implemented.
- **Advanced tenant configuration:** BYOK onboarding path, audit log streaming setup, multi-region choice — not FIT.
- **Inspection view demo:** Mentioned, but not demonstrable as function in quickstart.

What this edition covers.

Prerequisites

Before you start:

- **Account already exists** — ComplianceSuite customer success completed account creation.
- **First login works** — You can sign in with your credentials.
- **Designate tenant owner and QA approver** — These are needed for approval steps.
- **Choose candidate system** — A low-risk, well-understood system for validation (e.g., small EDMS, training platform, simple spreadsheet).

Step 1: Create Tenant.

1.1 Fill out tenant form

Go to **Account** → **Tenants** → **Create Tenant**:

01 Enter **Name** (e.g., "Boston Site") and **Slug** (3-letter IATA code or abbreviation).

02 Choose **Data Residency**: EU (Frankfurt), US (Virginia), or (Enterprise) UK, Canada, Switzerland.

03 Set **Retention Floor**: standard 10 years (recommended to leave).

04 Choose **Identity Model**: federated from account (standard) or tenant-local directory (CMO only).

05 **Submit** — tenant created in **Configuration** state.

1.2 Tenant owner signature

The designated tenant owner must sign the tenant configuration:

01 Notification: "Tenant configuration ready for sign-off".

02 Open tenant → click **Sign and Activate**.

03 Platform requests authentication.

04 Signature meaning: "Approved tenant configuration as tenant owner".

05 Tenant transitions to **Operational** state.

1.3 Templates (optional)

If you have custom URS/Risk/VP/IQ-OQ-PQ/VR templates, upload them under **Tenant** → **Templates** → **Upload**. Otherwise use the GAMP 5 default template library.

Step 2: Register System.

2.1 System Metadata

Go to **Tenant** → **Systems** → **Register System**:

01 Enter **Name** (human label).

02 Enter **Slug** (for change numbers, e.g., "edms-prod").

03 Enter **Vendor**.

04 Choose **GAMP 5 Category**: - Cat 4 for configured COTS (standard for first systems) - Cat 5 only for custom development

05 Choose **Risk Class**: low / medium / high (low recommended for first system).

06 **Data Classification:** GxP (for validated systems).

07 **Periodic Review Cycle:** default 12 months (high/medium) or 24 (low).

08 **Submit** — system created in **Draft** state.

2.2 Tenant validation lead signature

The tenant validation lead signs system scope:

01 Signature meaning: "Approved system scope and GAMP 5 categorisation as validation lead".

02 System transitions to **Ready**.

Step 3: Open Initial Validation Change.

3.1 Open change

Go to **System** → **Changes** → **Open Change**:

01 Choose **Change Type:** "Initial Validation".

02 Platform pre-fills deliverable matrix based on system GAMP 5 category: - Cat 4: URS, risk assessment, validation plan, IQ/OQ/PQ, RTM, validation report - Cat 5: + code review record, static analysis evidence

03 Enter **Regulatory Rationale** (one line, e.g., "Initial validation of EDMS v3.2 in support of QMS document control per EU GMP Part I Chapter 4").

04 Confirm **Risk Classification** (inherited from system).

05 Confirm **Phase Gate Configuration** (plan → execute → report with QA gates).

06 **Open Change** — change receives number (e.g., "edms-prod-CHG-001"), status **Draft**.

3.2 Change layout

The change view shows three columns:

- **Deliverables:** ordered list of records that must exist before closure.
- **Phase Gates:** QA-controlled boundaries between plan, execute, report.
- **Audit Trail:** every state transition, authoring action, review, approval, live written.

Step 4: Write URS.

4.1 Use AI Composer (recommended for first URS)

Click **Compose with AI** in URS template:

01 Enter one-paragraph system description: - Example: "Document management system for controlled SOPs and validation packages, used by Quality and Validation teams across Boston site, ~150 users, GAMP 5 Cat 4."

02 Composer drafts 25–35 requirements.

03 **Review each requirement:** - ■ Accept if correct - ■ Reject if not in scope - ✒■ Edit if specific (custom workflows, integrations)

04 **Save and submit for review** — URS in **In Review**, audit trail records AI composer prompt, model version, accepted/rejected items.

4.2 Reviewer pass

Designated reviewer (senior peer) opens URS:

- ■ Approve with comments
- ■ Send back for revision

Cycle until reviewer signs. (SoD: reviewer and approver not same person.)

4.3 QA Approval

QA approves URS against tenant quality checklist (clarity, testability, regulatory completeness).

On approval: URS **locked** for edits; changes require new revision under same change.

Step 5: Risk Assessment.

5.1 Build risk register

In risk assessment template:

01 Click **Import URS-derived risks** — platform pre-populates risks from URS (regulatory, performance requirements).

02 **Add additional risks:** data integrity, security, business continuity.

03 For each risk: set **severity** (1–5), **likelihood** (1–5), **detectability** (1–5).

04 Platform calculates **RPN** automatically. Risks ≥ RPN threshold (default 25) are **High**.

05 For each high risk: add **mitigation** (control reference, test reference, or procedural control).

5.2 Reviewer + QA pass

Same SoD as URS:

01 Reviewer signs.

02 QA signs. On approval: risk assessment **locked**; validation plan inherits risk register.

Step 6: Validation Plan.

6.1 Validation plan content

The validation lead captures all sections manually (optionally with AI Composer support for section authoring). There is no automatic population from change metadata or URS.

Typical sections the validation lead maintains:

- **Scope** — system description, validation scope
- **Deliverable list** — derived from tenant's `PhaseDocumentConfig` entries
- **Risk-based test strategy** — coverage plan based on risk assessment items
- **Roles** — author, reviewer, approver per deliverable, selected from tenant personnel
- **Acceptance criteria** — derived from URS requirements

6.2 What you add

- **Schedule:** start date, phase milestones, target close date
- **Deviations handling:** standing waivers from your QMS deviation procedure
- **Out-of-scope items:** explicitly not validating in this change

6.3 Plan phase gate

QA approver signs validation plan.

This signature is also the **plan phase gate:** platform now allows execute phase entry. Until then: no test execution recording possible.

Step 7: Execute IQ / OQ / PQ.

Test execution is the longest phase, but also least complex:

7.1 Installation Qualification (IQ)

Confirms system correctly installed:

- Correct version, correct configuration baseline, expected components

IQ tests for Cat 4 are typically quickest.

7.2 Operational Qualification (OQ)

Confirms system functions correctly under controlled conditions:

- Every functional requirement from URS tested against acceptance criterion
- Platform pre-generates OQ test for every URS requirement over low risk

7.3 Performance Qualification (PQ)

Confirms system performs in intended use environment with intended users and data:

- Typically end-to-end workflows
- Platform supports human-executed (with evidence) and automated (API call-out) PQ tests

7.4 Deviations

Test failed or unexpected?

Click **Raise Deviation** directly from test record. Deviation lives in change and follows your QMS procedure:

- Investigation, root-cause analysis, CAPA, closure
- Change cannot close with open **critical** or **major** severity

Evidence capture: every executed test step accepts evidence (screenshot, file upload, command output). Platform timestamps and hashes evidence on upload; hash is part of audit trail record. Tampering after upload forever detectable.

7.5 Execute phase gate

When all tests have final result and all deviations closed (or documented as residual risk carried):

QA signs execute phase gate → change transitions to **report phase**.

Step 8: Validation Report.

8.1 Platform writes

- **Executive summary:** scope, schedule, test counts, deviation counts
- **Deliverable status table:** all deliverables, versions, approvers, timestamp
- **Test summary table:** IQ/OQ/PQ counts, pass/fail ratio, average time-to-close
- **Deviation summary:** all deviations, severity, resolution
- **Risk re-evaluation:** pre- vs. post-mitigation RPN distribution
- **Traceability summary:** URS coverage via tests; coverage gaps

8.2 You write

- **Acceptance recommendation:** accept / conditionally accept / reject — with 1 paragraph reasoning
- **Residual risk statement:** what accepted, why
- **Operational handover notes:** what system owner needs to know post-go-live

Step 9: Close Change.

9.1 Closure checklist

Platform shows closure checklist:

- ■ All deliverables signed?
- ■ All tests concluded?
- ■ All deviations closed?
- ■ Validation report approved?

9.2 Closure initiation

01 Click **Initiate Closure** → head of quality notified.

02 Closer reviews validation report acceptance recommendation.

03 Closer signs closure. Signature meaning: "Accepted validation and authorised release of the system for GxP use as head of quality".

9.3 Seal & transition

Platform **seals** the change:

- Final audit log entry with SHA-256 of every record in change
- System transitions to **Production** state

13 — WHAT COMES NEXT

What comes next.

This week

- Onboard rest of validation team
- Upload own URS/Risk/VP/IQ-OQ-PQ/VR templates (tenant template library)
- Run internal audit dry-run inspection (use inspection view)

This month

- Register rest of in-scope systems
- Configure periodic review schedule for each system

This quarter

- Migrate legacy validation packages (from SharePoint/network drives)
- Define tenant-level SOPs (deviation handling, access reviews, periodic role reviews)

Troubleshooting.

Symptom	Likely Cause	Resolution
Tenant owner sign-off button grayed out	User created in account, but not assigned tenant owner role	Account administrator: open tenant → assign role → user refresh
AI Composer returns generic content	System description prompt too short	Provide vendor name, version, GAMP category, ~150 user count, 1–2 specific use cases. 2 paragraphs ideal
Risk assessment shows "0 risks imported from URS"	URS requirements all tagged functional, no risk attributes	Tag at least regulatory and performance requirements. Platform imports these as candidate risks
QA cannot sign gate	Open deliverable below gate (check closure checklist)	Resolve open deliverable first; gate signature unlocks automatically
Change cannot close: "Open critical deviation"	By design — critical deviations block	Close deviation, or downgrade severity with QA approval + justification, or cancel change

Code Reference.

- **Prisma Models:**
  `/Users/christophseydel/Sites/ComplianceSuite/prisma/schema.prisma`
- `Account`, `Tenant`, `System`, `Change`, `Document`, `AuditLog`, `ElectronicSignature`
- **Server Actions (Tenant, system, change, document management):**
  `/Users/christophseydel/Sites/ComplianceSuite/app/actions/`
- **Components (Change lifecycle, approval UI):**
  `/Users/christophseydel/Sites/ComplianceSuite/components/`

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 —