CS-DOC-0001 · GXP-DESK DOCUMENTATION

Quickstart for Validation Managers.

This version contains exclusively functions that have been verified in the codebase. Onboarding functions that are still missing (account verification via DNS TXT, SCIM activation, customer-success provisioning) have...

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0001	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-0001
TITLE	Quickstart for Validation Managers
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 version takes a validation manager from an existing account creation through the first tenant creation, system registration, and initial validation change to e-signature closure. The focus is on the actually implemented core workflow.

02 — WHAT THIS VERSION DOES NOT COVER

What this version does NOT cover.

The following onboarding functions have been removed:

- **Account Verification via DNS TXT:** The spec promises verifiable ownership, but the code does not implement it — only account creation and tenant setup.
- **SSO Self-Service Setup Wizard:** SSO via SAML 2.0 / OpenID Connect is implemented (including enforcement and domain routing); only the guided self-service setup wizard and SCIM remain open. SSO providers are currently configured administratively.
- **SCIM Provisioning Activation:** Not present in the code; the identity lifecycle remains a customer/IdP responsibility.
- **Customer-Success Provisioning:** MSA/DPA pre-check, provisioning state, approval workflow — not implemented.
- **Advanced Tenant Configuration (out of Quickstart scope):** BYOK and multi-region data residency (EU/US) have been implemented since 2026-06-04 but are not walked through in this Quickstart; audit-log streaming setup (SIEM sinks) remains open.
- **Inspection View Demo:** Mentioned, but not demonstrable as a function within the Quickstart.

What this version covers.

Prerequisites

Before you begin:

- **Account already exists** — GxP-Desk Customer Success has completed the account creation.
- **First login works** — you can sign in with your credentials.
- **Provide a Tenant Owner and QA Approver** — these are needed for the approval steps.
- **Choose a candidate system** — a low-risk, well-understood system for validation (e.g., a small EDMS, a trained platform, a simple spreadsheet).

Step 1: Create a tenant.

1.1 Complete the tenant form

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

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

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

03 Set the **Retention Floor**: default 10 years (recommended; leave as is).

04 Choose the **Identity Model**: Federated from Account (default) or Tenant-Local Directory (for CMOs only).

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

1.2 Tenant Owner signature

The designated Tenant Owner must sign the tenant configuration:

01 Receives the notification: "Tenant configuration ready for sign-off".

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

03 The platform requests authentication.

04 Signature meaning: "Approved Tenant configuration as Tenant Owner".

05 The tenant transitions to the **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 a system.

2.1 System metadata

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

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

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

03 Enter the **Vendor**.

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

05 Choose the **Risk Class**: Low / Medium / High (Low recommended for the first system).

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

07 **Periodic Review Cycle:** default 12 months (High/Medium) or 24 (Low).

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

2.2 Tenant Validation Lead signature

The Tenant Validation Lead signs the system scope:

01 Signature meaning: "Approved System scope and GAMP 5 categorisation as Validation Lead".

02 The system transitions to **Ready**.

Step 3: Open the Initial Validation Change.

3.1 Open the change

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

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

02 The platform pre-fills the deliverable matrix based on the system's 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 the **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 the **Risk Classification** (inherited from the system).

05 Confirm the **Phase Gate Configuration** (Plan → Execute → Report with QA gates).

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

3.2 Change layout

The change view shows three columns:

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

Step 4: Write the URS.

4.1 Use the AI Composer (recommended for the first URS)

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

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

02 The composer drafts 25–35 requirements.

03 **Review each requirement:** - Accept those that are correct - Reject those that do not fit the scope - Edit those that are specific (custom workflows, integrations)

04 **Save and Submit for Review** — the URS moves to **In Review**; the audit trail records the AI composer prompt, model version, and accepted/rejected items.

4.2 Reviewer pass

The designated reviewer (a senior peer) opens the URS:

- Approve with comments
- Send back for revision

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

4.3 QA approval

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

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

Step 5: Risk Assessment.

5.1 Build the risk register

In the Risk Assessment template:

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

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

03 For each risk, set the **Severity** (1–5), **Likelihood** (1–5), and **Detectability** (1–5).

04 The platform calculates the **RPN** automatically. Risks ≥ the RPN threshold (default 25) are **High**.

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

5.2 Reviewer + QA pass

The same SoD as the URS:

01 The reviewer signs.

02 QA signs. On approval: the Risk Assessment is **locked**; the Validation Plan inherits the risk register.

Step 6: Validation Plan.

6.1 Contents of the Validation Plan

The Validation Lead captures all sections manually (optionally assisted by the AI Composer during section authoring). There is no automatic population from change metadata or the URS.

Typical sections the Validation Lead maintains:

- **Scope** — description of the system, the validation's scope of applicability
- **Deliverable list** — derived from the tenant's `PhaseDocumentConfig` entries
- **Risk-based test strategy** — coverage plan based on the risk-assessment items
- **Roles** — Author, Reviewer, Approver per deliverable, selected from the tenant personnel
- **Acceptance criteria** — derived from the 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 validated in this change

6.3 Plan-phase gate

The **QA Approver** signs the Validation Plan.

This signature is also the **Plan-phase gate:** the platform now permits entry into the Execute phase. Until then, no test-execution recording is possible.

Step 7: Execute IQ / OQ / PQ.

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

7.1 Installation Qualification (IQ)

Confirms the system is correctly installed:

- Correct version, correct configuration baseline, expected components

IQ tests for Cat 4 are typically the fastest.

7.2 Operational Qualification (OQ)

Confirms the system functions correctly under controlled conditions:

- Each functional requirement from the URS is tested against an acceptance criterion
- The platform pre-generates an OQ test for each URS requirement above Low Risk

7.3 Performance Qualification (PQ)

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

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

7.4 Deviations

A test failed or behaved unexpectedly?

Click **Raise Deviation** directly from the test record. The deviation lives within the change and follows your QMS procedure:

- Investigation, root-cause analysis, CAPA, closure
- A change cannot close with an open **Critical** or **Major** severity

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

7.5 Execute-phase gate

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

QA signs the Execute-phase gate → the change transitions to the **Report phase**.

Step 8: Validation Report.

8.1 The platform writes

- **Executive Summary:** scope, schedule, test counts, deviation counts
- **Deliverable Status Table:** all deliverables, versions, approver, 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 one paragraph of reasoning
- **Residual Risk Statement:** what is accepted, and why
- **Operational Handover Notes:** what the system owner needs to know post-go-live

Step 9: Close the change.

9.1 Closure checklist

The platform shows the closure checklist:

- All deliverables signed?
- All tests concluded?
- All deviations closed?
- Validation Report approved?

9.2 Closure initiation

01 Click **Initiate Closure** → the Head of Quality is notified.

02 The closer reviews the Validation Report acceptance recommendation.

03 The closer signs the closure. Signature meaning: "Accepted Validation and authorised release of the System for GxP use as Head of Quality".

9.3 Seal & transition

The platform **seals** the change:

- A final audit-log entry with the SHA-256 of every record in the change
- The system transitions to the **Production** state

13 — WHAT COMES NEXT

What comes next.

This week

- Onboard the rest of the validation team
- Upload your own URS/Risk/VP/IQ-OQ-PQ/VR templates (the tenant template library)
- Run an internal-audit dry-run inspection (using the Inspection View)

This month

- Register the rest of the in-scope systems
- Configure the 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)

14 — TROUBLESHOOTING

Troubleshooting.

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

Code references.

- **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/`

As of: 2026-06-04 | **Version:** 1.0 | **Classification:** Public — 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 —