CS-CM-0002 · GXP-DESK DOCUMENTATION

EU GMP Annex 11 Control Matrix.

This version contains only features that have been verified in the codebase.
Roadmap features have been removed or reduced.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-CM-0002	v1.0	2026-06-04	Quality Compliance

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-CM-0002
TITLE	EU GMP Annex 11 Control Matrix
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-06-04
REVIEW CYCLE	On change
DOCUMENT OWNER	Quality Compliance
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 maps the 40 control points of EU GMP Annex 11, to the extent they are evidenced by the GxP-Desk codebase. It structures the supplier's deliverable (GxP-Desk) separately from the responsibility of the regulated operation.

02 — WHAT THIS VERSION DOES NOT COVER

What this version does NOT cover.

The following areas have been removed or reduced:

> **NOTE**
> Updated 2026-06-04: SSO (SAML/OIDC), change-level RTM auto-generation and multi-region data residency (EU/US) are now implemented and have been moved into the FIT section.

- **Citation-graph RTM / system-level union:** Change-level RTM including gap detection is FIT; auto-generation from a citation graph and the system-wide union as a sealed PDF remain open.
- **Validation report auto-population:** The code can provide the structure and audit data, but not auto-population of narrative elements.
- **Periodic-review auto-digest:** No auto-compiled audit trail digest as reviewer input (the scheduler opens reviews, but the digest artifact is missing).
- **Audit log streaming to SIEM:** Splunk/Datadog/S3 not implemented; webhooks (HMAC) are present, a dedicated audit sink is still open.
- **SCIM 2.0:** No SCIM provisioning/deprovisioning; conditional access remains on the IdP side.
- **Sandbox provisioning for qualification:** No multi-environment sandbox feature.
- **Two-person entry / nightly reconciliation:** Four-eyes entry of critical fields and nightly reconciliation reports are not implemented.
- **X.509/PKCS7-signed PDF exports:** Not implemented; integrity via the audit hash chain + verification JSON.

03 — § 1 RISK MANAGEMENT

§ 1 Risk Management.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-001	§ 1	Risk management across the entire lifecycle, taking patient safety, data integrity and product quality into account	ICH Q9-aligned Risk Assessment template; FMEA scoring; risk class drives test depth in the Validation Plan; risk re-evaluation in every change	Risk policy in the QMS; define risk-acceptance authority; set risk-class thresholds
CS-A11-002	§ 1	Extent of validation and data-integrity controls based on the risk assessment	Coverage rules block under-tested URS items; risk class drives test depth at VP generation	Risk-coverage policy; deviation handling for residual risk

§ 2 Personnel.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-003	§ 2	Close cooperation between key personnel (process owner, system owner, qualified persons, IT)	Roles per system and tenant; cross-tenant account compliance lead; named ownership at every level	Job descriptions; clear ownership in the QMS
CS-A11-004	§ 2	Personnel qualified with appropriate training and access rights	Training records linked to user profiles; the platform denies signing rights without a training assignment	Training matrix; qualification records; training verification at periodic review

§ 3 Suppliers and Service Providers.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-005	§ 3.1	Quality agreement with the supplier when using a third party	Quality agreement template available; signed at the account level	Negotiate and execute the quality agreement; periodic review
CS-A11-006	§ 3.2	Supplier competence and reliability; supplier audits where necessary	ISO 27001 / SOC 2 evidence available; platform validation reports on request	Supplier-qualification SOP; periodic review of supplier evidence
CS-A11-007	§ 3.3	COTS documentation reviewed for compliance with user requirements	Platform documentation set (CS-DOC-0001 to 0018) covers compliance; release notes signed	Document review at supplier qualification
CS-A11-008	§ 3.4	Quality system and audit information for vendors of critical systems	Internal QMS documentation summary available; SOC 2 Type II on request; ISO 27001 alignment statement	Audit information request; review against qualification standards

06 — § 4 VALIDATION

§ 4 Validation.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-009	§ 4.1	Documented validation lifecycle	Phase-gated change pattern; URS → Risk → VP → IQ/OQ/PQ → VR; sealed records	Validation Master Plan; lifecycle policy
CS-A11-010	§ 4.2	Validation evidence available for inspection	Inspection View; Inspection Pack; tenant-scoped audit trail export	Generate the Inspection Pack on an inspection request; archival
CS-A11-011	§ 4.3	Specifications approved before development	URS, FRS templates; field-level locking; SoD; QA approval before the next phase	Authoring SOP; subject-matter expert engagement
CS-A11-012	§ 4.4	Configuration management across the lifecycle	System metadata as a configuration baseline; configuration change pattern; periodic review of configuration	Configuration management SOP; baseline ownership
CS-A11-013	§ 4.5	Up-to-date list of all relevant systems and their GxP function	Tenant-scoped system inventory; GAMP 5 category and GxP scope on every system	Keep the inventory current; review at periodic review
CS-A11-014	§ 4.6	Quality risk management and traceability documentation	Auto-generated change-level RTM (`getTraceabilityMatrix`) including gap detection (`identifyTraceabilityGaps`); coverage warnings at the gate; sealed RTM at change closure	Sign-off on the RTM; risk-traceability policy

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-015	§ 4.7	User requirements traceable across the lifecycle	URS → FRS → test cases → risks via DocumentRelation links; change-level RTM auto-generated (system-level union as a sealed PDF: Roadmap)	Sign-off on traceability at change closure
CS-A11-016	§ 4.8	For Cat 5: source-code review and structured testing	Custom-code review record; static-analysis evidence attachment; reviewer signature; test-coverage evidence	Source-code review SOP; secure-development training

07 — § 5 DATA

§ 5 Data.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-017	§ 5	Data integrity safeguarded across the data lifecycle	ALCOA+ aligned data model; schema validation (Zod); foreign-key integrity. (Standalone reconciliation reports: Roadmap)	Data lifecycle policy; periodic data review
CS-A11-018	§ 5	Critical data manual entry subject to an additional check	Roadmap: No dedicated two-person-entry mode; the four-eyes principle is currently provided via SoD signatures at the deliverable level	Map four-eyes control of critical fields via SOP; training

08 — § 6 ACCURACY CHECKS

§ 6 Accuracy Checks.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-019	§ 6	Built-in checks for correct and secure data entry and processing	OQ tests on critical data fields; foreign-key integrity at write; schema validation. (Nightly reconciliation reports: Roadmap)	Test design for accuracy; acceptance criteria

09 — § 7 DATA STORAGE

§ 7 Data Storage.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-020	§ 7.1	Data secured by physical and electronic means against damage	Multi-zone replicated storage; AES-256-GCM at rest (optional BYOK via AWS/Azure/GCP KMS); backup integrity tests	Backup verification; restoration tests as a DR procedure
CS-A11-021	§ 7.2	Regular backups; integrity and accuracy checked	Daily integrity checks; backup snapshots replicated across zones; tested DR	Periodic verification of restoration capability

§ 8 Printouts.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-022	§ 8.1	Clear printed copies of electronically stored data	PDF rendering of every record; integrity via the audit hash chain + `audit■chain■verification.json` (no X.509 PDF signature)	Printout SOP where required by the customer process
CS-A11-023	§ 8.2	Records for batch release should reflect changes; the printout must show the audit trail	PDF exports contain the Inspection View with audit trail context; revisions linked to originals	Batch-release SOP referencing the platform records

11 — § 9 AUDIT TRAILS

§ 9 Audit Trails.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-024	§ 9	Audit trail of all GxP-relevant changes and deletions built into the system	Audit trail at every level (account, tenant, system, change); deletion not exposed	Audit trail review SOP; trigger criteria
CS-A11-025	§ 9	Reasons for changes documented	Free-text justification field on every controlled action; rationale required for retention-affecting actions	User training on rationale capture; review
CS-A11-026	§ 9	Audit trails available, convertible to an intelligible form, regularly reviewed	One-button Inspection Pack; hash-chain verification (Verify-Report). (Auto-compiled audit trail digest: Roadmap)	Conduct audit trail review per cadence; document findings

§ 10 Change and Configuration Management.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-027	§ 10	Changes to a computerized system only in a controlled manner in accordance with a procedure	Change as a unit of work; configuration change pattern; phase gates; sealed records	Change-control SOP; impact-assessment policy

13 — § 11 PERIODIC EVALUATION

§ 11 Periodic Evaluation.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-028	§ 11	Computerized systems regularly evaluated to remain in the validated state	Periodic-review change pattern; automated scheduling and reminders (scheduler sweep). (Auto-digest: Roadmap)	Periodic-review SOP; cadence policy
CS-A11-029	§ 11	Periodic evaluation should cover current functionality, deviations, incidents, upgrade history, performance, reliability, security and validation status	The Periodic Review Report template structures the review; the audit trail is retrievable manually (auto-compiled digest: Roadmap)	Conduct the review; follow-up changes where warranted

§ 12 Security.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-030	§ 12.1	Physical and/or logical controls restrict access to authorized individuals	Tenant-level RBAC with permission guards (`requireAccountPermission`/`requireTenantPermission`/`requireChangePermission`); SSO (SAML/OIDC) with enforcement and domain routing	Customer SOP for access review at periodic review
CS-A11-031	§ 12.2	Suitable methods to prevent unauthorized entry (keys, pass cards, personal codes, passwords, biometrics)	Argon2 password hashing; MFA (WebAuthn/passkeys, TOTP, recovery codes); failedLoginAttempts tracking; encryption at rest and in transit	Customer SOP for password strength; physical-access control to user devices
CS-A11-032	§ 12.3	Creation, change and cancellation of access authorizations recorded	The audit trail captures every TenantUserAssignment creation, role change and deactivation	Customer SOP for role-lifecycle management; review at periodic review
CS-A11-033	§ 12.4	Management systems for data and documents designed to record the operator, operations, change details, time and date	Every audit trail entry contains actor, action, target, before/after and timestamp	—

15 — § 13 INCIDENT MANAGEMENT

§ 13 Incident Management.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-034	§ 13	All incidents (not only system failures and data errors) reported and assessed; root cause identified	Deviation lifecycle in every change; CAPA integration; platform-side incident notifications for security and availability	Incident-management SOP; communication plan; CAPA tracking

16 — § 14 ELECTRONIC SIGNATURE

§ 14 Electronic Signature.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-035	§ 14	Electronic records electronically signable; electronic signatures have the same effect as handwritten ones	21 CFR Part 11 / Annex 11 compliant e-signature; manifestations always shown; bound to the record hash	E-signature policy; signature meanings tenant-owned; hand-signature SOP where applicable
CS-A11-036	§ 14	Electronic signatures permanently linked to their record	The signature record references the signed payload via a hash; inseparable from the record	—
CS-A11-037	§ 14	Electronic signatures contain the time and date of application	Server-side UTC timestamp in the same transaction	—

17 — § 15 BATCH RELEASE

§ 15 Batch Release.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-038	§ 15	At batch release, only Qualified Persons may certify batch release	Out of scope for the platform; the batch-release system is registered as a separate system with its own validation evidence	Batch-release SOP; QP responsibilities; interface validation

18 — § 16 BUSINESS CONTINUITY

§ 16 Business Continuity.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-039	§ 16	For the availability of critical systems, provisions for continuity of support	Multi-region replication; documented DR/backup; RTO/RPO published in the security whitepaper	Business-continuity policy; tested fallback procedures; communication chain

19 — § 17 ARCHIVING

§ 17 Archiving.

Control	Section	Requirement	Platform support	Customer responsibility
CS-A11-040	§ 17	Data can be archived; archived data should be checked for accessibility, readability and integrity	Tenant archival path; read-only frozen tenants; audit trail export at archival; periodic accessibility test on archived tenants	Archiving SOP; retention horizon aligned with the regulatory floor

20 — CODE REFERENCES

Code references.

- **Prisma models:** `/Users/christophseydel/Sites/ComplianceSuite/prisma/schema.prisma` (RiskAssessment, ValidationPhase, AuditLog, ElectronicSignature, PeriodicReview, TrainingRecord)
- **Server Actions (change, risk, periodic review):** `/Users/christophseydel/Sites/ComplianceSuite/app/actions/`
- **Components (approval workflow, signature UI):** `/Users/christophseydel/Sites/ComplianceSuite/components/`
- **Security & encryption:** Codebase standard TLS 1.3, AES-256-GCM

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

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 —