CS-CM-0001 · GXP-DESK DOCUMENTATION

21 CFR Part 11 Control Matrix.

This version contains only features that have been verified in the codebase.
Roadmap features from the original PDF have been removed.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-CM-0001	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-0001
TITLE	21 CFR Part 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 42 control points of 21 CFR Part 11, to the extent they are evidenced by the GxP-Desk codebase. It serves as compliance documentation for inspectors and audits, kept limited to implemented features.

02 — WHAT THIS VERSION DOES NOT COVER

What this version does NOT cover.

The following control areas have been removed (included in the original but not FIT in the code):

> **NOTE**
> Updated 2026-06-04: SSO (SAML/OIDC), MFA, re-authentication at signing, the consistently enforced hash chain and BYOK are now implemented and have been moved from this list into the FIT section.

- **SCIM 2.0 provisioning/deprovisioning:** No SCIM endpoint; identity lifecycle remains a customer/IdP responsibility (P11-007/038).
- **Device fingerprinting & conditional access:** The code contains no device-fingerprinting logic; conditional access remains on the IdP side (P11-019).
- **OAuth2 service principals (client credentials):** Only hashed, scoped API keys are present; the OAuth2 client-credentials grant is still open.
- **X.509/PKCS7-signed PDF exports:** Not implemented; integrity via the audit hash chain + verification JSON (P11-025).
- **Audit log streaming to SIEM:** Mentioned for Splunk/Datadog/S3; webhooks are present, a dedicated audit sink is still open (P11-041).

03 — CONTROL OVERVIEW

Control Overview.

GxP-Desk implements 42 discrete control points. The following table shows the FIT controls grouped by regulatory area.

§ 11.10 Closed-System Controls (23 controls)

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-001	§ 11.10(a)	Validation of the system for accuracy, reliability and intended performance	System validated under GAMP 5 Cat 4/5; validation reports available	Self-validation of the system; perform supplier qualification of GxP-Desk
CS-P11-002	§ 11.10(a)	Ability to detect invalid or altered data	Hash-bound audit trail; verification aid; refusal to seal a change with broken cross-references	Perform periodic audit trail verification; investigate anomalies
CS-P11-003	§ 11.10(b)	Ability to generate accurate, complete copies in human-readable form	The Inspection View renders all records as HTML/PDF	Export the Inspection Pack upon an inspection request
CS-P11-004	§ 11.10(b)	Ability to generate accurate, complete copies in electronic form	Structured per-record JSON export in the inspection bundle (ZIP) including `audit■chain■verification.json`; JSONL stream still open	Distribute the export in accordance with an inspection or audit request
CS-P11-005	§ 11.10(c)	Protection of records for accurate and ready retrieval throughout the entire retention period	Multi-zone replicated storage; daily integrity checks; archived tenants remain exportable	Define the retention policy in the tenant policy; review at periodic review
CS-P11-006	§ 11.10(c)	Long-term retention beyond account termination	Read-only retention window after termination per the MSA; audit trail export available	Negotiate retention in the MSA; export at termination if required

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-007	§ 11.10(d)	Limit access to authorized individuals	Tenant identity perimeter; RBAC based on tenant membership; SSO (SAML/OIDC) with enforcement and domain routing; MFA. SCIM deprovisioning still open	Keep tenant user access current; periodic review of access; (in the absence of SCIM) track deprovisioning at the IdP
CS-P11-008	§ 11.10(d)	Limit physical access to systems	Cloud provider attestations (SOC 2, ISO 27001)	Enforce physical access controls on user devices
CS-P11-009	§ 11.10(e)	Secure, computer-controlled, time-stamped audit trails	Append-only audit trail at all levels; NTP-synchronized UTC; tamper-evident hashes	Investigate audit trail anomalies identified at periodic review
CS-P11-010	§ 11.10(e)	Audit trail captures the date and time of operator entries and actions	Server-side UTC timestamps in the same transaction as each action	—
CS-P11-011	§ 11.10(e)	Audit trail captures changes that create, modify or delete records	All state-change events captured with before/after fields; deletion is not available via platform paths	—
CS-P11-012	§ 11.10(e)	Record changes must not obscure previously captured information	First-version preservation guaranteed; subsequent edits create linked new versions; the original cannot be overwritten	—
CS-P11-013	§ 11.10(e)	Audit trail documentation must be retained at least as long as the electronic records	Audit trail retention horizon ≥ record retention horizon at all levels	Configure the tenant retention policy
CS-P11-014	§ 11.10(e)	Audit trail available for FDA review and copying	Tenant-scoped audit trail export; one-click Inspection Pack	Generate the export on request

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-015	§ 11.10(f)	Operational system checks to enforce permitted sequencing	Phase gates enforce phase order; the deliverable matrix blocks out-of-order signing; SoD evaluated on every signature	Configure tenant-level gate criteria if required
CS-P11-016	§ 11.10(g)	Authority checks: only authorized individuals use the system	Per-record authority check; the lowest explicit grant wins; service principals follow the same model	Keep role assignments current per the tenant policy
CS-P11-017	§ 11.10(g)	Authority checks: only authorized individuals sign electronically	SoD-incompatible signers are filtered out automatically	Train users on signature meanings; review access at periodic review
CS-P11-018	§ 11.10(g)	Authority checks for record changes	Field-level locking states; approved fields read-only; sealed records immutable	—
CS-P11-019	§ 11.10(h)	Device checks to determine the validity of data sources	Only mentioned in the spec; real device-fingerprinting logic is not in the code	—
CS-P11-020	§ 11.10(i)	Education and training for system development, maintenance and use	Training records bound to user profiles; the platform denies signing rights without a training assignment	Keep the training matrix current; capture training completions in the platform
CS-P11-021	§ 11.10(j)	Written policies for accountability under electronic signatures	Signature meanings from a controlled library; manifestations always visible	Tenant SOP defines accountability; cross-reference to signature meanings
CS-P11-022	§ 11.10(k)	Control over system documentation (distribution and access)	Tenant document library; controlled SOP versioning; field-level locking; sealed-record discipline	Keep SOPs current in the tenant library; perform periodic review
CS-P11-023	§ 11.10(k)	Revision and change-control procedures with an audit trail	Change as a unit of work; configuration change pattern; sealed records after closure	Reference the platform pattern in the change-control SOP

§ 11.30 Open Systems (2 controls)

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-024	§ 11.30	Additional measures for open systems: encryption	TLS 1.3 in transit; AES-256-GCM at rest; optional BYOK (customer CMK via AWS/Azure/GCP KMS, envelope encryption, key rotation)	—
CS-P11-025	§ 11.30	Additional measures: digital signatures	Roadmap: No X.509/PKCS7 signature in PDF exports; integrity instead via the tamper-evident audit hash chain and `audit■chain■verification.json`	—

§ 11.50 / § 11.70 Signature Manifestations & Linking (5 controls)

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-026	§ 11.50(a)	A signed electronic record contains the printed name of the signer	Name captured at the time of signing; rendered in every view	—
CS-P11-027	§ 11.50(a)	A signed electronic record contains the date and time of the signature	Server-side UTC timestamps in the same transaction	—
CS-P11-028	§ 11.50(a)	A signed electronic record contains the meaning of the signature	Meaning from the signature meaning library; selected and visible at the time of signing	Keep the tenant-level signature meaning library current
CS-P11-029	§ 11.50(b)	Signature manifestations are subject to the same controls as electronic records	Manifestations are part of the audit trail entry of the signed record; tamper-evident with the rest of the record	—

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-030	§ 11.70	Electronic signatures must be linked to their records (cannot be cut, copied or transferred)	Signature records reference the signed payload via a SHA-256 hash; signatures are inseparable from the record	—

§ 11.100 / § 11.200 Electronic Signature Components (6 controls)

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-031	§ 11.100(a)	Each electronic signature is unique to one individual	User IDs unique within the account; never reissued; tombstoned on deletion	One user account per person; no shared accounts
CS-P11-032	§ 11.100(b)	Identity verification before establishing electronic signature credentials	The account owner verifies identity at onboarding; signerName/signerEmail are frozen from the user profile at the time of signing	Customer SOP for identity verification of employees before user creation
CS-P11-033	§ 11.100(c)	Certification to the FDA that electronic signatures are legally binding equivalent to handwritten ones	—	The customer must submit the FDA certificate (21 CFR 11.100(c))
CS-P11-034	§ 11.200(a)(1)	Two distinct identification components	Username + Argon2-hashed password as the components of platform authentication	Customer SOP for password requirements for users; customer-side second component outside the platform
CS-P11-035	§ 11.200(a)(2)	Both components at the first signature in a session; at least one for subsequent signatures	Re-authentication on every signature via MFAGrant (single-use, 5-minute window); the signature event audit captures the authentication context (ipAddress, sessionId, userAgent, signedAt)	Customer SOP for session discipline; physical security in the inspection office

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-036	§ 11.200(a)(3)	Use only by the genuine credential owner	Per-user credentials; SoD enforcement in the sign flow blocks self-approval; the audit trail captures ipAddress + userAgent of every sign event	Customer SOP against credential sharing; investigate anomalies from the audit trail

§ 11.300 ID Codes / Passwords (6 controls)

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-037	§ 11.300(a)	Uniqueness of the identification code/password combination	User email as a unique constraint within the account; Argon2 password hashing per user; deleted users retain their ID permanently in the audit trail	Customer SOP for password complexity and non-reuse
CS-P11-038	§ 11.300(b)	Periodic checking, recall or revision of identification codes and passwords	The TenantUserAssignment model allows activation/deactivation; the periodic-review model confirms current role assignments	Customer SOP for regular access review; customer-side password rotation outside the platform
CS-P11-039	§ 11.300(c)	Loss-management procedures	failedLoginAttempts field on the user; an account compliance-lead role exists	Customer SOP for credential-loss reporting and the reset workflow
CS-P11-040	§ 11.300(d)	Transaction safeguards to prevent unauthorized use	Permission guards (`requireAccountPermission`/`requireTenantPermission`/`requireChangePermission`); SoD enforcement in the signDocument flow	Customer SOP for security incidents; customer-side offboarding processes
CS-P11-041	§ 11.300(d)	Detection and reporting of unauthorized-use attempts	The audit trail captures all authentication and permission-denied events with ipAddress + sessionId	Customer SOP for audit trail review; incident-response process

Control	Clause	Requirement	Platform support	Customer responsibility
CS-P11-042	§ 11.300(e)	Periodic testing of devices that bear or generate identification code/password information	—	Customer obligation: periodic testing of the customer-side authentication infrastructure

04 — EVIDENCE CATEGORIES

Evidence Categories.

The control evidence falls into the following categories:

Category	Where it lives	Generated by
Audit trail entries	Per-record in the audit log	Continuously, automatically
Inspection Pack	Per-change export bundle	At change closure or on demand
Hash-chain verification	Verification utility output	On demand against any export
Tenant policy records	Tenant configuration history (signed)	With every tenant config change
Customer SOPs and policies	The customer's QMS	Customer-maintained, referenced in the tenant policy
Authentication records	On the customer side (email provider, possibly a customer IdP outside the platform)	Customer-maintained; corresponds to platform user profiles via the email address

05 — CODE REFERENCES

Code references.

- **Prisma models:** `/Users/christophseydel/Sites/ComplianceSuite/prisma/schema.prisma` (AuditLog, ElectronicSignature, DocumentVersion, ValidationPhase, User, Role)
- **Server Actions (audit, change, approval):** `/Users/christophseydel/Sites/ComplianceSuite/app/actions/`
- **Components (approval, signature UI):** `/Users/christophseydel/Sites/ComplianceSuite/components/`
- **Encryption / hashing:** Codebase standard AES-256-GCM, SHA-256 for hashes; BYOK (`lib/byok/*`, `TenantEncryption`); SSO (`lib/sso/*`); audit hash chain v2 (`lib/audit/chain-algorithm.ts`)

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 —