ComplianceSuite

FIT-CLEAN

CS-CM-0001 · COMPLIANCESUITE DOCUMENTATION

# 21 CFR Part 11 Control Matrix.

This edition contains only functions 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 | 2026-04-28 | Quality Compliance |

*Public — Compliance Matrix · 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 | 2026-04-28 |
| REVIEW CYCLE | On change |
| DOCUMENT OWNER | Quality Compliance |
| CLASSIFICATION | Public — Compliance Matrix |
| RELATED RECORDS | Complete roadmap version in /output/CS-CM-0001_21_CFR_Part_11_Control_Matrix.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 — 
03 — Control Overview — 
04 — Evidence Categories — 
05 — Code Reference — 
Revision History — 
Glossary & Abbreviations — 

01 — WHAT THIS EDITION COVERS

# What this edition covers.

This edition maps the 42 control points of 21 CFR Part 11 to the extent they are demonstrated by the ComplianceSuite codebase. It serves as compliance documentation for inspectors and audits, limited to implemented functions.

02 — WHAT THIS EDITION DOES NOT COVER

# What this edition does NOT cover.

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

- **SSO / SAML / OIDC / SCIM:** Not implemented in code. Customer responsibility for Identity Provider Management remains.
- **MFA Setup Flows & configurable second factor:** Only TOTP/Hardware Keys mentioned; no setup assistant in code for their initialization.
- **Device Fingerprinting & Conditional Access:** Code contains no Device Fingerprinting logic; only mention in audit trail structure.
- **Service Principals / B2B Authentication:** Code not present.
- **Re-Authentication Challenge on Signature:** Code has `passwordVerified: true` as default; true re-auth challenge logic not implemented.
- **Audit Trail Hash-Chain Enforcement:** Fields (`checksum`, `previousChecksum`) exist in DB, but true tamper detection in code unclear.
- **BYOK / KMS Integration:** Mentioned in code (Enterprise), but actual implementation not FIT (Roadmap Feature).
- **Audit Log Streaming:** Mentioned to Splunk/Datadog/S3, but not implemented.

03 — CONTROL OVERVIEW

# Control Overview.

ComplianceSuite implements 42 discrete control points. The following table shows FIT controls grouped by regulatory domain.

## § 11.10 Closed-System Controls (23 Controls)

| Control | Clause | Requirement | Platform Support | Customer Responsibility |
|---|---|---|---|---|
| CS-P11-001 | § 11.10(a) | System validation for accuracy, reliability, intended performance | System validated under GAMP 5 Cat 4/5; validation reports available | Perform system self-validation; conduct ComplianceSuite supplier qualification |
| CS-P11-002 | § 11.10(a) | Ability to detect invalid or altered data | Hash-bound audit trail; verification assistance; refusal to seal change with broken cross-references | Conduct periodic audit trail verification; investigate anomalies |
| CS-P11-003 | § 11.10(b) | Ability to generate accurate, complete copies in readable form | Inspection View renders all records as HTML/PDF | Export inspection pack on inspection request |
| CS-P11-004 | § 11.10(b) | Ability to generate accurate, complete copies in electronic form | JSONL export with documented schema; manifest with header hash | Distribute export per inspection or audit request |
| CS-P11-005 | § 11.10(c) | Protect records for accurate and rapid retrievability throughout retention period | Multi-zone replicated storage; daily integrity checks; archived tenants remain exportable | Define retention policy in tenant policy; verify during periodic review |
| CS-P11-006 | § 11.10(c) | Long-term retention beyond account termination | Read-only retention window after termination per MSA; audit trail export available | Negotiate retention in MSA; export if needed on termination |
| CS-P11-007 | § 11.10(d) | Restrict access to authorized persons | Tenant identity perimeter; RBAC based on tenant membership | Keep tenant user access current; conduct periodic review of access |

| Control | Clause | Requirement | Platform Support | Customer Responsibility |
|---|---|---|---|---|
| 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-generated, time-stamped audit trails | Append-only audit trail at all levels; NTP-synchronized UTC; tamper-evident hashes | Investigate audit trail anomalies identified during periodic review |
| CS-P11-010 | § 11.10(e) | Audit trail captures date and time of operator entries and actions | Server-side UTC timestamps in same transaction as every 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 not exposed via platform paths | — |
| CS-P11-012 | § 11.10(e) | Record modifications must not hide previously captured information | First-version preservation guaranteed; subsequent edits create linked new versions; original not overwritable | — |
| CS-P11-013 | § 11.10(e) | Audit trail documentation must be retained as long as electronic records | Audit trail retention horizon ≥ record retention horizon at all levels | Configure 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 export on request |
| CS-P11-015 | § 11.10(f) | Operational system checks to enforce permitted sequencing | Phase gates enforce phase order; deliverable matrix blocks out-of-sequence signing; SoD evaluated at every signature | Configure tenant-level gate criteria if needed |
| CS-P11-016 | § 11.10(g) | Authority checks: only authorized persons use system | Per-record authority check; lowest explicit grant wins; service principals follow same model | Keep role assignments current in tenant policy |

| Control | Clause | Requirement | Platform Support | Customer Responsibility |
|---|---|---|---|---|
| CS-P11-017 | § 11.10(g) | Authority checks: only authorized persons electronically sign | SoD-incompatible signers automatically filtered | Train users on signature meanings; review access during periodic review |
| CS-P11-018 | § 11.10(g) | Authority checks for record modifications | Field-level locking states; approved fields read-only; sealed records immutable | — |
| CS-P11-019 | § 11.10(h) | Device checks to determine validity of data sources | Only mentioned in spec; true device fingerprinting logic not in code | — |
| CS-P11-020 | § 11.10(i) | Training and instruction for system development, maintenance, and use | Training records linked to user profiles; platform refuses signing rights without training assignment | Keep training matrix current; record training completions in platform |
| CS-P11-021 | § 11.10(j) | Written policies for accountability under electronic signatures | Signature meanings from controlled library; manifestations always visible | Define tenant SOP for 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 in tenant library current; conduct periodic review |
| CS-P11-023 | § 11.10(k) | Change and configuration control procedures with audit trail | Change as work unit; configuration change pattern; sealed records after closure | Reference platform pattern in change control SOP |

# § 11.30 Open Systems (2 Controls)

| Control | Clause | Requirement | Platform Support | Customer Responsibility |
|---|---|---|---|---|
| CS-P11-024 | § 11.30 | Additional safeguards for open systems: encryption | TLS 1.3 in transit; AES-256-GCM at rest | — |

| Control | Clause | Requirement | Platform Support | Customer Responsibility |
|---|---|---|---|---|
| CS-P11-025 | § 11.30 | Additional safeguards: digital signatures | PDF exports contain X.509 signature; tampering detectable in compliant PDF readers | — |

## § 11.50 / § 11.70 Signature Manifestations & Linking (5 Controls)

| Control | Clause | Requirement | Platform Support | Customer Responsibility |
|---|---|---|---|---|
| CS-P11-026 | § 11.50(a) | Signed electronic record contains signer's printed name | Name captured at signature time; rendered in every view | — |
| CS-P11-027 | § 11.50(a) | Signed electronic record contains date and time of signature | Server-side UTC timestamps in same transaction | — |
| CS-P11-028 | § 11.50(a) | Signed electronic record contains meaning of signature | Meaning from signature meaning library; selected and visible at signature time | Keep tenant-level signature meaning library current |
| CS-P11-029 | § 11.50(b) | Signature manifestations subject to same controls as electronic records | Manifestations are part of signed record's audit trail entry; tamper-evident with rest of record | — |
| CS-P11-030 | § 11.70 | Electronic signatures must be linked to their records (cannot be cut, copied, or transferred) | Signature records reference signed payload via SHA-256 hash; signatures inseparable from 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 person | User IDs unique within account; never reissued; tombstoned on deletion | One user account per person; no shared accounts |
| CS-P11-032 | § 11.100(b) | Identity verification before establishment of electronic signature credentials | Account owner verifies identity on onboarding; signerName/signerEmail frozen from user profile at sign time | Customer SOP for identity verification of employees before user creation |
| CS-P11-033 | § 11.100(c) | Certification to FDA that electronic signatures are legally equivalent to handwritten signatures | — | Customer must submit FDA certificate (21 CFR 11.100(c)) |
| CS-P11-034 | § 11.200(a)(1) | Two distinct identification components | Username + Argon2-hashed password as components of platform authentication | Customer SOP for password requirements for users; customer-side second component outside platform |
| CS-P11-035 | § 11.200(a)(2) | Both components at first signature in session; at least one at subsequent signatures | Signature event audit captures authentication context (ipAddress, sessionId, userAgent, signedAt) | Customer SOP for session discipline; physical security in inspection office |
| CS-P11-036 | § 11.200(a)(3) | Use only by true credential holders | Per-user credentials; SoD enforcement in sign flow blocks self-approval; audit trail captures ipAddress + userAgent of every sign event | Customer SOP against credential sharing; investigate anomalies from audit trail |

# § 11.300 ID Codes / Passwords (6 Controls)

| Control | Clause | Requirement | Platform Support | Customer Responsibility |
|---|---|---|---|---|
| CS-P11-037 | § 11.300(a) | Uniqueness of identification code/password combination | User email as unique constraint in account; Argon2 password hashing per user; deleted users retain ID permanently in audit trail | Customer SOP for password complexity and non-reuse |
| CS-P11-038 | § 11.300(b) | Periodic review, recall, or recheck of identification codes and passwords | TenantUserAssignment model allows activation/deactivation; periodic review model confirms current role assignments | Customer SOP for regular access review; customer-side password rotation outside platform |
| CS-P11-039 | § 11.300(c) | Loss management procedures | failedLoginAttempts field on user; account compliance lead role exists | Customer SOP for credential loss reporting and reset workflow |
| CS-P11-040 | § 11.300(d) | Transaction safeguards to prevent unauthorized use | Permission guards (`requireAccountPermission`/`requireTenantPermission`/`requireChangePermission`); SoD enforcement in signDocument flow | Customer SOP for security incidents; customer-side offboarding processes |
| CS-P11-041 | § 11.300(d) | Detection and reporting of unauthorized use attempts | Audit trail captures all authentication and permission-denied events with ipAddress + sessionId | Customer SOP for audit trail review; incident response process |
| CS-P11-042 | § 11.300(e) | Periodic testing of devices that carry or generate identification code/password information | — | Customer obligation: periodic testing of customer-side authentication infrastructure |

04 — EVIDENCE CATEGORIES

# Evidence Categories.

Control evidence falls into the following categories:

| Category | Where it lives | Generated by |
|---|---|---|
| Audit Trail Entries | Per-record in audit log | Continuously, automatically |
| Inspection Pack | Per-change export bundle | On change closure or on-demand |
| Hash-Chain Verification | Verification utility output | On-demand against any export |
| Tenant Policy Records | Tenant configuration history (signed) | With each tenant config change |
| Customer SOPs and Policies | Customer QMS | Customer-maintained, referenced in tenant policy |
| Authentication Records | Customer-side (email provider, possibly customer IdP outside platform) | Customer-maintained; corresponds to platform user profiles via email address |

05 — CODE REFERENCE

# Code Reference.

- **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

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 —