CS-DOC-0014 · COMPLIANCESUITE DOCUMENTATION

Audit Trail and Exports.

FIT-only redaction. Effective 2026-04-28.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0014	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-0014
TITLE	Audit Trail and Exports
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-04-28
REVIEW CYCLE	On change
DOCUMENT OWNER	Customer Success
CLASSIFICATION	Public — Documentation
RELATED RECORDS	/output/CS-DOC-0014_Audit_Trail_and_Exports.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 documents the Audit Trail and Export Features of ComplianceSuite that have been verified as FIT in the codebase:

- **Audit Log Model:** Append-only with sequenceNumber auto-increment per Stream
- **Fields:** id, sequenceNumber, timestamp, userId, userName, action, resourceType, resourceId, oldValue/newValue (JSON), reason, ipAddress, timezone, sessionId, accountId, tenantId, checksum, previousChecksum
- **Scoping:** Account Scope, Tenant Scope, System Scope, Change Scope via Foreign Key Filter
- **Exports:** PDF (Inspection View), manual generation via app/reporting/inspector/page.tsx
- **Tamper Evidence Fields:** checksum and previousChecksum for Hash Detection (implemented, but continuous Chain Logic not verified)
- **Components:** AuditViewer and AuditTrailViewer

02 — WHAT THIS EDITION DOES NOT COVER

What this edition does NOT cover.

- **4 parallel Streams as Data Structure:** No stream Discriminator Field; Scoping via FK Filter
- **Tamper-evident Hash Chain continuously enforced:** Fields exist; continuous Implementation unclear
- **Verify Utility as CLI Tool:** Not implemented
- **Actor Role Snapshot:** Role not frozen at Action time
- **target.version Field:** Not implemented
- **JSONL Export with stable Schema:** Not implemented
- **CSV Export Configurability:** Not implemented
- **Auto Audit Trail Digest:** Not implemented

03 — AUDIT TRAIL — OVERVIEW

Audit Trail — Overview.

The Audit Trail is the most frequently inspected artifact. Regulators in all Jurisdictions request it. ComplianceSuite treats the Audit Trail as First-Class Storage Layer with its own Integrity Guarantees.

Scope & Filtering

The Audit Trail is accessible at multiple levels:

Scope	Captures	Filter via
Account	User/Role Lifecycle, Billing, Tenant Lifecycle, Account Configuration	accountId
Tenant	User/Role Assignments in this Tenant, System Lifecycle, Tenant Configuration	tenantId
System	GAMP Category Changes, Periodic Review Events, System State Transitions	resourceId (System) + resourceType
Change	Authoring, Review, Approval, Deviation, Test Execution, Signature Events during Change Lifetime	resourceId (Change) + resourceType

The Streams are linked: a Change Event carries System and Tenant Context; a Tenant Event can reference affected Systems.

04 — AUDIT LOG FIELDS

Audit Log Fields.

Each entry in the Audit Log contains:

Field	Definition
id	Unique Identifier
sequenceNumber	Monotonically increasing within the Stream (Account, Tenant, System, or Change)
timestamp	Server-side UTC Time
timezone	Timezone of Client Request (informational)
userId	Unique User ID
userName	Resolved Name of User (Snapshot at Action time)
action	Description of Action (e.g., "deliverable.author.submit", "change.approved")
resourceType	Type of affected Record (e.g., "Document", "Change", "User")
resourceId	ID of affected Record
oldValue	JSON Snapshot of State before Action (for State Change Events)
newValue	JSON Snapshot of State after Action (for State Change Events)
reason	Why the Action was performed (if documented)
ipAddress	Source IP of Request
sessionId	Session Identifier
accountId	Account Scope for Filtering
tenantId	Tenant Scope for Filtering (if relevant)
checksum	Hash of this entry (SHA-256 over contents)
previousChecksum	Hash of previous entry in this Stream (for Hash Chain)

Hash Chain & Tamper Evidence.

The Audit Log has Fields **checksum** and **previousChecksum**:

```
Entry N:   checksum = SHA-256(Entry N content + previousChecksum)
           previousChecksum = SHA-256(Entry N-1 content + Entry N-2 checksum)
```

If a historical entry is altered, the Chain breaks.

Important: The Design supports Tamper Detection; continuous Verification of all entries at each Export is conceptually defined, but Implementation of a CLI Verify Utility and continuous Chain Validation in code is not verified.

06 — EXPORTS

Exports.

Audits can be exported manually via Inspection View.

Export Generation

01 **From Inspection View:** Click **Export** (Reporting Interface)

02 **Choose Scope:** Account, Tenant, System, or specific Change

03 **Time Range:** Standard is "since Inception"; Alternatives are "since last Periodic Review" or "during Inspection Window"

04 **Format:** Platform supports PDF Rendering (Inspection PDF)

05 **Processing:** For small Scopes interactive; for large Scopes with Notification at Completion

06 **Download:** Export is in Tenant's **Inspection Pack** for configurable Retention Duration

PDF Export (Inspection PDF)

- **Audience:** Regulators, Internal Audit, Executive Review
- **Content:** Human-readable Rendering of Audit Trail with Entries inline beside the Records they affected
- **Signature:** PDF can be signed by Platform (X.509 Signature)
- **Best Practice:** Always pair with machine-readable Export for Completeness

Export Manifest

Each Export contains a Manifest with:

- Head of Chain Hash (or last available checksum)
- Scope and applied Filters
- Generation Timestamp
- Platform Signature (if available)

07 — OPERATIONAL CONSIDERATIONS

Operational Considerations.

Audit Trail Review SOP

Tenant Policy specifies Cadence for Audit Trail Review:

- **High-Risk Systems:** Monthly
- **Medium-Risk Systems:** Quarterly
- **Low-Risk Systems:** At Periodic Review

Investigation Pattern

When a Deviation raises a question spanning User Actions over time:

01 **Start in Tenant Audit Trail:** Filter by Actor, Time Window

02 **Narrow to Change Audit Trail:** Focus on affected Records

03 **Platform Filter Controls:** Support both directions

04 **Saved Views:** Saved Investigation Views can be re-executed when Investigation evolves

Storage & Costs

ComplianceSuite stores Audit Trail Entries natively — there is no separate Cost Line. The Platform absorbs Storage Costs from Account-level Retention Floor.

08 — ARCHIVING & LONG-TERM RETENTION

Archiving & Long-Term Retention.

When a Tenant is archived:

01 **Read-Only Freeze:** The Tenant becomes write-protected

02 **Complete Audit Trail Export:** At the time Archive occurs

03 **Remaining Access:** Archived Tenants remain inspectable and exportable

04 **Retention:** Retention Policy per Regulatory Floor (e.g., 3–5 years for Pharma)

09 — DATA INTEGRITY — SUMMARY

Data Integrity — Summary.

The Audit Trail System addresses Requirements from 21 CFR Part 11 § 11.10(e) and EU GMP Annex 11 § 9:

- **Append-only Design:** No Deletion; Append only
- **Time Stamp:** Server-side captured in UTC
- **Actor Resolution:** User Name at Action time captured
- **State Tracking:** oldValue / newValue Snapshots for Audit Trails
- **Scoping:** Account, Tenant, System, Change — hierarchical Filtering possible
- **Export Integrity:** Manifest and Timestamp at Export; Hash Fields for Manipulation Detection

Customers are responsible for:

- Definition of Audit Trail Review Cadence
- Documentation and implementation of Investigation Processes
- Archiving SOP and Retention Horizon Definition
- Periodic review for Anomalies or unauthorized Changes

Effective: 2026-04-28 **Source:** Codebase Snapshot with FIT Verification **Contact:** Compliance Office, ComplianceSuite

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 —