CS-DOC-0014 · GXP-DESK DOCUMENTATION

Audit Trail and Exports.

FIT-only redaction. Effective 2026-06-04.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0014	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-0014
TITLE	Audit Trail and Exports
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 documents the audit trail and export features of GxP-Desk 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 filters
- **Tamper-evident hash chain v2 (NEW 2026-06-04):** canonical JSON + scope key (`computeChainChecksumV2`); a Postgres **immutability trigger** blocks UPDATE/DELETE; a gap-free sequence via advisory lock/serializable transaction
- **Verification (NEW 2026-06-04):** integrity/verification report + startup check (`lib/audit/integrity-report.ts`, `startup-check.ts`) and a reconstruction utility (`scripts/audit-reconstruction/reconstruct.ts`)
- **Exports:** PDF (Inspection View); **REST audit export** (`app/api/v1/audit-logs`); **inspection bundle** (ZIP with `audit-chain-verification.json`) via `app/actions/tenant/export-validation-history.ts`
- **Webhooks (NEW 2026-06-04):** HMAC-SHA256-signed event delivery with retry/backoff (`lib/api/webhooks/*`, `Webhook`, `WebhookDelivery`)
- **Components:** AuditViewer and AuditTrailViewer

02 — WHAT THIS VERSION DOES NOT COVER

What this version does NOT cover.

> **NOTE**
> Updated 2026-06-04: Hash-chain enforcement and the verify utility are now implemented (see above) and have therefore been removed from this list.

- **4 parallel streams as a data structure:** No stream discriminator field; scoping via FK filters
- **Actor role snapshot:** The role is not frozen at the time of the action
- **target.version field:** Not implemented
- **JSONL export with a stable schema:** Not implemented (the export delivers per-record JSON, not a JSONL stream)
- **CSV export configurability:** Not implemented
- **Automatic audit trail digest:** Not implemented
- **X.509/PKCS7-signed PDF exports:** Not implemented (integrity via the hash chain + verification JSON)
- **Audit log streaming to SIEM (Splunk/Datadog/S3):** Not implemented (webhooks deliver business events, not a dedicated audit sink)

03 — AUDIT TRAIL — OVERVIEW

Audit Trail — Overview.

The audit trail is the most frequently inspected artifact. Regulators in every jurisdiction request it. GxP-Desk treats the audit trail as a 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 the 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 the client request (informational)
userId	Unique user ID
userName	Resolved name of the user (snapshot at the time of the action)
action	Description of the action (e.g. "deliverable.author.submit", "change.approved")
resourceType	Type of the affected record (e.g. "Document", "Change", "User")
resourceId	ID of the affected record
oldValue	JSON snapshot of the state before the action (for state-change events)
newValue	JSON snapshot of the state after the action (for state-change events)
reason	Why the action was performed (where documented)
ipAddress	Source IP of the request
sessionId	Session identifier
accountId	Account scope for filtering
tenantId	Tenant scope for filtering (where relevant)
checksum	Hash of this entry (SHA-256 over its contents)
previousChecksum	Hash of the previous entry in this stream (for the hash chain)

Hash Chain & Tamper Evidence.

The audit log has **checksum** and **previousChecksum** fields:

```
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 changed, the chain breaks.

As of 2026-06-04: The hash chain is implemented as **v2** (canonical JSON, scope key; `computeChainChecksumV2`). A Postgres **immutability trigger** prevents UPDATE/DELETE on the audit table, and an advisory lock secures the gap-free sequence. Verification is performed via a startup check and an integrity/reconstruction report (`lib/audit/integrity-report.ts`, `scripts/audit-reconstruction/reconstruct.ts`); the inspection bundle contains an `audit-chain-verification.json`.

06 — EXPORTS

Exports.

Audits can be exported manually via the Inspection View.

Export Generation

01 **From the Inspection View:** Click **Export** (reporting interface)

02 **Select scope:** Account, tenant, system, or a specific change

03 **Time range:** The default is "since inception"; alternatives are "since the last periodic review" or "during the inspection window"

04 **Format:** The platform supports PDF rendering (Inspection PDF)

05 **Processing:** Interactive for small scopes; with a notification on completion for large scopes

06 **Download:** The export is downloadable from the tenant's **Inspection Pack** for a configurable retention period

PDF Export (Inspection PDF)

- **Audience:** Regulators, internal audit, executive review
- **Content:** Human-readable rendering of the audit trail with entries inline next to the records they affected
- **Integrity:** PDF exports carry **no** X.509/PKCS7 signature; integrity is evidenced through the audit hash chain and the accompanying `audit-chain-verification.json`
- **Best practice:** Always pair with a machine-readable export for completeness

Export Manifest

Each export contains a manifest with:

- Head-of-chain hash (or the last available checksum)
- Scope and applied filters
- Generation timestamp
- Result of the hash-chain verification (`audit-chain-verification.json`)

07 — OPERATIONAL CONSIDERATIONS

Operational Considerations.

Audit Trail Review SOP

The tenant policy specifies the 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 that spans user actions over time:

01 **Start in the tenant audit trail:** Filter by actor, time window

02 **Narrow to the change audit trail:** Focus on the affected records

03 **Platform filter controls:** Support both directions

04 **Saved views:** Saved investigation views can be re-run as the investigation evolves

Storage & Cost

GxP-Desk stores audit trail entries natively — there is no separate cost line. The platform bears the storage cost from the account-level retention floor.

08 — ARCHIVING & LONG-TERM RETENTION

Archiving & Long-Term Retention.

When a tenant is archived:

01 **Read-only freeze:** The tenant is made read-only

02 **Full audit trail export:** At the point in time when archiving occurs

03 **Remaining access:** Archived tenants remain inspectable and exportable

04 **Retention:** Retention policy according to the regulatory floor (e.g. 3–5 years for pharma)

09 — DATA INTEGRITY — SUMMARY

Data Integrity — Summary.

The audit trail system addresses the requirements of 21 CFR Part 11 § 11.10(e) and EU GMP Annex 11 § 9:

- **Append-only design:** No deletion; additions only
- **Timestamps:** Captured server-side in UTC
- **Actor resolution:** User name captured at the time of the action
- **State tracking:** oldValue / newValue snapshots for audit trails
- **Scoping:** Account, tenant, system, change — hierarchical filtering possible
- **Export integrity:** Manifest and timestamp at export; an end-to-end hash chain v2 (immutability trigger + Verify-Report) to detect tampering

Customers are responsible for:

- Defining an audit trail review cadence
- Documenting and implementing investigation processes
- The archiving SOP and the retention-horizon definition
- Periodic review for anomalies or unauthenticated changes

As of: 2026-06-04 **Source:** Codebase snapshot with FIT verification (GAP/FIT re-analysis 2026-06-04) **Contact:** Compliance Office, GxP-Desk

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 —