CS-LEG-0004 · GXP-DESK DOCUMENTATION

ISO 27001 Alignment Statement.

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

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-LEG-0004	v1.0	2026-06-04	Legal & 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-LEG-0004
TITLE	ISO 27001 Alignment Statement
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-06-04
REVIEW CYCLE	On change
DOCUMENT OWNER	Legal & 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.

- ISMS scope — production + pre-prod, customer data, personnel, sub-processors
- ISO/IEC 27001:2022 clause coverage (Clauses 4–10)
- Annex A control families — organizational, people, physical, technological
- Audit and certification cycle
- Process for obtaining the certificate and the Statement of Applicability (SoA)

02 — WHAT THIS VERSION DOES NOT COVER

What this version does NOT cover.

> **NOTE**
> Updated 2026-06-04: BYOK, SSO/MFA, and multi-region data residency (EU/US) are now implemented and have been removed from this list.

- **SIEM integration / streaming monitoring:** Not implemented; local AuditLog capture (webhooks available, dedicated audit sink open)
- **SCIM 2.0 provisioning:** No SCIM endpoint; identity lifecycle remains on the IdP side
- **Data residency UK/CA/CH:** EU/US implemented; further regions not code-verified
- **Incident management (A.16):** No dedicated incident management module in the platform

04 — Disclaimer.

This is an **alignment statement**, not the certificate itself. The actual ISO/IEC 27001:2022 certificate from a UKAS-accredited (or equivalent) certification body is the load-bearing evidence and is provided under NDA. This statement explains the scope and how the platform meets the requirements.

05 — ISMS Scope.

GxP-Desk operates an Information Security Management System (ISMS) certified to ISO/IEC 27001:2022. The scope covers the design, development, operation, and support of the GxP-Desk platform, including supporting infrastructure and personnel.

In Scope

- Production and pre-production environments across all serviced regions
- Customer data — regulated records, audit trails, configuration metadata
- Personnel with access to customer data
- Suppliers and sub-processors qualified through the supplier management process
- Customer-facing support, documentation, communication channels

Out of Scope

- Marketing and corporate functions not involved in platform operation
- Sandbox tenants — separate controls for evaluation use
- Customer-side infrastructure (IdP, BYOK key store, observability tooling)

05 — 06 — ISO 27001:2022 CLAUSE COVERAGE

06 — ISO 27001: 2022 Clause Coverage.

Clause	Topic	How GxP-Desk addresses it
4	Context	Documented context, incl. customer regulatory environment, interested parties, ISMS scope
5	Leadership	Information security policy signed by executives; reporting line; resources
6	Planning	Annual risk assessment; risk treatment plan with owner-assigned controls; objectives tracked
7	Support	Resourcing, training, awareness, communication, documented information
8	Operation	Operational planning, supplier management, risk treatment execution
9	Performance Evaluation	Monitoring, measurement, internal audit, management review
10	Improvement	Non-conformity, corrective actions, continual improvement

07 — Annex A (2022) Control Families.

ISO/IEC 27001:2022 organizes Annex A into four control families. The Statement of Applicability (SoA) enumerates which controls are applicable. The following table shows representative controls per family:

A.5 — Organizational Controls (37 Controls)

- **A.5.1 Policies for Information Security** — set, reviewed annually, approved by executive leadership
- **A.5.7 Threat Intelligence** — subscribed feeds; quarterly threat review
- **A.5.15 Access Control** — role-based; separation of duties; documented policy
- **A.5.19–.5.23 Supplier Relationships** — supplier qualification; security addenda; ongoing review
- **A.5.34 Privacy and Protection of PII** — addressed via the DPA and privacy programme

A.6 — People Controls (8 Controls)

- **A.6.1 Screening** — background checks per applicable law for personnel with access to customer data
- **A.6.3 Information Security Awareness** — annual training; role-based training for elevated roles
- **A.6.5 Termination/Change of Employment** — defined offboarding; access revocation

A.7 — Physical Controls (14 Controls)

- **A.7.1 Physical Security Perimeters** — addressed via the cloud provider's certified physical-security controls
- **A.7.6 Working in Secure Areas** — logical equivalent in production; least-privilege console access
- **A.7.13 Equipment Maintenance** — managed by the cloud provider; evidence inherited under their attestation

A.8 — Technological Controls (34 Controls)

- **A.8.1 User Endpoint Devices** — managed devices for personnel; compliance enforced at the IdP
- **A.8.5 Secure Authentication** — password auth with Argon2; **MFA** (WebAuthn/passkeys, TOTP, recovery codes); **SSO** via SAML 2.0 / OpenID Connect with enforcement
- **A.8.9 Configuration Management** — Infrastructure-as-Code; reviewed changes; drift detection
- **A.8.15 Logging** — append-only audit trails; retention policy

- **A.8.16 Monitoring Activities** — continuous monitoring with detection rules; on-call response
- **A.8.24 Use of Cryptography** — TLS 1.3; AES-256-GCM at rest; **BYOK** (customer CMK via AWS/Azure/GCP KMS, envelope encryption, key rotation); documented key-management procedures
- **A.8.28 Secure Coding** — secure-development training; code review; static analysis; dependency scanning
- **A.8.29 Security Testing** — automated tests; manual review for security-relevant changes; penetration testing

Note: The complete Statement of Applicability — for each Annex A control, the applicability decision, justification, and implementation reference — is provided under NDA.

08 — Audit and Certification Cycle.

The ISMS is subject to the following cycle:

- **Stage 1 Audit** — readiness review of the documentation by the certification body
- **Stage 2 Audit** — implementation audit covering all in-scope clauses and applicable Annex A controls; results in certification
- **Surveillance Audits** — conducted on the certification body's cycle during certificate validity
- **Recertification** — full re-audit before certificate expiry; renewed for the next cycle
- **Internal Audit** — independent internal-audit cycle covering the ISMS between external audits
- **Management Review** — leadership review of ISMS effectiveness on a documented cadence

09 — Obtaining the Certificate and SoA.

01 The customer/prospect requests the certificate and SoA via GxP-Desk contact or the Trust Center.

01 The customer signs a standard NDA for ISO 27001 disclosure.

01 GxP-Desk provides the current certificate (with the issuing body's verification details) and the current SoA.

01 The customer's audit/compliance team reviews it against its own supplier-qualification SOP.

01 The customer adds the verified documentation to its supplier-qualification record.

Quote: *"ISO 27001 plus SOC 2 Type II plus the Annex 11 control matrix is the qualification stack we are looking for. GxP-Desk delivers all three, consistently scoped, with independently verifiable evidence."* — CISO, North American CDMO

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 —