The Beginner's Guide to ISO/IEC 27001 Compliance with Kitecyber

Discover how Kitecyber helps organisations align with ISO/IEC 27001 (ISMS) by protecting information assets across endpoints, cloud infrastructure, SaaS and network channels, enabling risk-based controls, audit evidence, and continuous monitoring.

What is ISO/IEC 27001?

ISO/IEC 27001 is the international standard that defines requirements for an Information Security Management System (ISMS). Organisations implement an ISMS to identify risks, select controls from Annex A, and demonstrate continual improvement of information security.

Why DLP and Endpoint Controls matter now

ISO 27001:2022 introduced or emphasized controls that make a formal Data Loss Prevention (DLP) strategy and endpoint controls central to meeting technological controls in Annex A — DLP is explicitly called out as an important control for preventing sensitive data exfiltration. Effective ISO compliance therefore blends policy, process, and technical tooling (DLP + UEM + UEBA + classification + SWG + ZTNA).

How Kitecyber helps companies enable endpoints and DLP controls for ISO 27001 Compliance

Kitecyber is an AI security copilot that helps organization unifies:

- Data Loss Prevention (DLP) - discovery, content & context inspection, blocking/exceptions, incident workflows.
- Data Classification – automated & custom classifiers (PII, IP, IP-type files, source tagging).
- Unified Endpoint Management (UEM)– encryption, patch enforcement, device posture, remote wipe.
- User & Entity Behaviour Analytics (UEBA) - anomaly detection, prioritised alerts, insider risk scoring.
- Secure Web Gateway (SWG) – safe web/SaaS access, TLS enforcement, blocking of unsafe upload destinations.
- Zero-Trust Network Access (ZTNA)– least-privilege microsegmentation, identity + device posture checks.

Together these tools provide technical controls, logging and evidence required by an ISMS and Annex A controls.

ISO 27001 (Annex A) → Kitecyber mapping table

The table maps key Annex A / ISMS control themes to Kitecyber modules and explains how each feature of Kitecyber AI security copilot helps satisfy ISO requirements and produce audit-ready evidence.

ISO/Annex A Control Theme / Example Controls	Mapped Kitecyber Product(s)	How Kitecyber Helps (audit / evidence focus)
A. 5 / Organizational (ISMS policies & governance) — policies, risk assessment, roles	DLP (policy enforcement), Compliance workflows (Kitecyber), Audit logs	Enforce technical policy settings across endpoints; exportable policy attestation logs and risk treatment evidence for ISMS records.
A.6 / People (awareness, training, access responsibilities)	DLP, UEBA, Compliance workflows	DLP incident reports feed training; UEBA shows user risk trends; workflows record staff attestations and role assignments.
A.7 / Physical controls (assets off-site)	UEM, DLP	UEM enforces disk encryption & remote wipe for off-site assets; DLP prevents writing sensitive files to removable media.
A.8 / Asset management & information classification	Data Classification, DLP	Auto discovery and tagging of sensitive assets; classification metadata propagates to DLP policies and ISMS asset register.
A.9 / Access control	ZTNA, UEM, DLP	ZTNA + identity integration enforce least-privilege; UEM ensures device trust; DLP enforces context-based access rules for sensitive data.
A.10 / Cryptography	UEM, SWG	UEM enforces disk and TLS cert posture; SWG ensures encrypted transport for sensitive flows; logs show crypto enforcement.
A.11 / Physical & operational environment (media handling)	DLP, UEM	Prevents storage of classified data on removable media; UEM enforces USB policy and logs attempts.
A.12 / Operations security (logging, monitoring, malware, backups)	UEBA, DLP, UEM, SWG	Centralised logging for all data events; UEBA correlates anomalies; UEM enforces AV/patch posture; SWG blocks risky web traffic.
A.13 / Communications & operations management (network segregation, transfer protection)	SWG, ZTNA, DLP	ZTNA microsegments CDEs; SWG protects and inspects web/SaaS transfers; DLP prevents policy-violating transfers and logs evidence.
A.14 / System acquisition, development & maintenance (secure SDLC)	DLP, UEBA, UEM	DLP protects test and production data; UEBA detects abnormal app behaviour post-deploy; UEM enforces secure baseline configurations.
A.15 / Supplier relationships (third-party risk)	DLP, ZTNA, SWG, UEBA	DLP monitors data flows to vendors; ZTNA limits vendor access scope; SWG and UEBA monitor third-party behaviour and generate audit logs.
A.16 / Information security incident management	DLP, UEBA, Audit Logs, Compliance workflows	DLP detects exfil attempts; UEBA correlates events; combined logs + workflows provide incident timelines, containment actions, and post-incident evidence for ISO requirements.
A.17 / Business continuity	UEM, DLP, ZTNA	UEM ensures device resilience/patching; DLP reduces data loss during incidents; ZTNA supports controlled access during disaster recovery.
A.18 / Compliance (legal, regulatory & contractual)	DLP, Data Classification, Audit Logs	Classification and DLP create evidence for legal/ contractual requirements; exportable logs and retention/erasure workflows support compliance audits.

(Notes: ISO/IEC 27001:2022 groups controls into organizational, people, physical and technological domains — many Annex A controls are satisfied by combining process + Kitecyber technical controls).)

Practical outcomes — what auditors & ISMS owners get

Clear asset inventory & classification	Technical enforcement of policy	Detection + containment of data exfiltration
(records for Statement of Applicability).	(policy-to-enforcement traceability).	(DLP + UEBA correlation + automatic containment actions).

Vendor control evidence	Incident timelines & forensic evidence
(monitored, logged third-party access and transfers).	(exportable audit reports for corrective actions and continual improvement).

Quick ISO-aligned implementation checklist (recommended first 30–90 days)

1. **Run discovery & classification** —inventory sensitive information and map to ISMS asset register (Data Classification + DLP).
2. **Define policy → enforce policies —** translate Annex A controls into DLP/UEM/ ZTNA policies and baseline configurations.
3. **Deploy UEM baseline** — full-disk encryption, AV posture, patching, USB controls, device inventory.
4. **Protect data in motion & at rest** — SWG for web/SaaS, ZTNA for app access, DLP for at-rest and in-flight controls.
5. **Enable UEBA & centralized logging —** tune alerts, connect to SIEM/incident workflows, retain evidence per retention policies.
6. **Create IR & evidence playbook —** map DLP/UEBA playbooks to ISMS incident handling and corrective action records.
7. **Third-party oversight —** enforce vendor access via ZTNA, monitor transfers with DLP, record SLA/KPI evidence.

KITE CYBER

Kitecyber, 691 S Milpitas Blvd, Ste 217, Milpitas, CA 95035
Email: info@kitecyber.com
Website: www.kitecyber.com

LinkedIn Twitter YouTube