ISO 27001:2022 · STAGE 2

Stage 2 Evidence Checklist

Certification Audit under ISO 27001:2022 — 60-point check

VERSION	DATE	LICENCE
1.0	October 6, 2026	Creative Commons CC-BY-4.0

OPEN LICENCE · CC-BY-4.0

This template is licensed under Creative Commons CC-BY-4.0. Free use, sharing, and adaptation permitted, with attribution: Kopexa GmbH, kopexa.com.

How to Fill In This Checklist

This checklist structures your Stage 2 preparation (certification audit) under ISO 27001:2022. Stage 2 verifies the operational implementation of your ISMS through sampling, interviews, and technical verification. Each row represents an evidence artifact that the auditor will typically review.

Legend

1. Status: Ready = evidence is complete; Gap = evidence missing or incomplete; N/A = not applicable to our scope
2. Evidence Location: path, ticket ID, or URL to the evidence
3. Categories map to the four Annex A theme areas plus audit logistics

This template is CC-BY-4.0 licensed. Free use with attribution: Kopexa GmbH, kopexa.com. Not a substitute for legal advice. ISO 27001:2022 — Version 2026-04-18.

A.5 — Organisational Controls

û	Control	Evidence	Status	Evidence Location
☐	A.5.1	Information security policies published and acknowledgement recorded	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.2	Role matrix with ISMS responsibilities assigned	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.3	Evidence of segregation of duties (SoD matrix, recertifications)	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.4	Top management commitment statement and review cycles	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.7	Threat intelligence sources documented, reports archived	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.8	Project management guideline with security gates for projects	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.9	Asset inventory complete, with owner, classification, and review date	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.10	Acceptable-use policy signed by all employees	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.12	Information classification scheme documented and applied	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.15	Access control matrix current, recertification logs available	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.16	Identity management process with onboarding and offboarding logs	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.17	MFA enabled, exception list documented and justified	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.18	Access rights reviewed regularly, review minutes available	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.19	Supplier register complete, criticality rated	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.20	Security clauses in all supplier contracts documented	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.21	ICT supply chain risk assessment available	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.22	Supplier audits performed and minuted	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.23	Cloud security policy and list of approved cloud services	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.24	Incident response plan with escalation chain and contacts	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.26	Incident log with detection, response, and lessons learned	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.29	Disruption planning: fallback concepts for critical processes	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.30	BCM / DR test performed, protocol and lessons learned archived	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.31	Register of regulatory and contractual requirements	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.34	GDPR processes: DPIA, processor contracts, data subject rights	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.35	Evidence of independent ISMS review (internal audit)	☐ Ready ☐ Gap ☐ N/A	
☐	A.5.37	Operating procedures documented, versioned, accessible	☐ Ready ☐ Gap ☐ N/A	

A.6 — People Controls

û	Control	Evidence	Status	Evidence Location

☐	A.6.1	Background checks for new employees documented	☐ Ready	☐ Gap	☐ N/A
☐	A.6.2	Employment contracts with security obligations	☐ Ready	☐ Gap	☐ N/A
☐	A.6.3	Awareness training delivered, 100 percent participation recorded	☐ Ready	☐ Gap	☐ N/A
☐	A.6.4	Disciplinary process documented, application evidenced	☐ Ready	☐ Gap	☐ N/A
☐	A.6.5	Offboarding checklists with asset return and access revocation	☐ Ready	☐ Gap	☐ N/A
☐	A.6.6	NDA register current for all relevant people and suppliers	☐ Ready	☐ Gap	☐ N/A
☐	A.6.7	Remote work policy, technical safeguards verifiable	☐ Ready	☐ Gap	☐ N/A
☐	A.6.8	Reporting channels for security events set up and communicated	☐ Ready	☐ Gap	☐ N/A

A.7 — Physical Controls

û	Control	Evidence	Status			Evidence Location
☐	A.7.1	Perimeter protection documented, entry points defined	☐ Ready	☐ Gap	☐ N/A	
☐	A.7.2	Entry control with logging, visitor register in place	☐ Ready	☐ Gap	☐ N/A	
☐	A.7.3	Protection of rooms with critical infrastructure	☐ Ready	☐ Gap	☐ N/A	
☐	A.7.4	Physical monitoring (cameras, alarms) operational	☐ Ready	☐ Gap	☐ N/A	
☐	A.7.5	Protection against fire, water, environment documented and tested	☐ Ready	☐ Gap	☐ N/A	
☐	A.7.7	Clear-desk and clear-screen policy implemented	☐ Ready	☐ Gap	☐ N/A	
☐	A.7.9	Protection concept for off-premises assets	☐ Ready	☐ Gap	☐ N/A	
☐	A.7.10	Handling of removable media, encryption policy	☐ Ready	☐ Gap	☐ N/A	
☐	A.7.14	Secure disposal evidence for hardware and media	☐ Ready	☐ Gap	☐ N/A	

A.8 — Technological Controls

û	Control	Evidence	Status			Evidence Location
☐	A.8.1	Endpoint management: MDM, encryption, antivirus active	☐ Ready	☐ Gap	☐ N/A	
☐	A.8.2	Privileged accounts with dedicated admin IDs and MFA	☐ Ready	☐ Gap	☐ N/A	
☐	A.8.5	Secure authentication (MFA, password policy) enforced everywhere	☐ Ready	☐ Gap	☐ N/A	
☐	A.8.7	Malware protection centrally managed, alert logs available	☐ Ready	☐ Gap	☐ N/A	
☐	A.8.8	Vulnerability scans over at least 6 months, remediation tracking	☐ Ready	☐ Gap	☐ N/A	
☐	A.8.9	Configuration baselines for servers and endpoints	☐ Ready	☐ Gap	☐ N/A	
☐	A.8.10	Secure deletion procedures for sensitive data documented	☐ Ready	☐ Gap	☐ N/A	
☐	A.8.12	Data leakage prevention controls active and monitored	☐ Ready	☐ Gap	☐ N/A	

CC-BY-4.0 — Kopexa GmbH — Free-use template with attribution

☐	**A.8.13**	Backup concept active, restore tests with protocol	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.15**	Central logging with retention policy and access protection	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.16**	Monitoring and SIEM alerts with documented use cases	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.20**	Network segmentation and firewall policies documented	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.22**	Separation of production, test, development technically enforced	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.24**	Cryptography policy with approved algorithms	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.25**	Secure SDLC with security gates in the development process	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.28**	Secure coding guidelines, code review evidence	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.29**	Security testing (SAST, DAST) as part of the pipeline	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.31**	Separation of dev / test / prod enforced and verifiable	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.32**	Change management history complete, with risk assessment	☐ Ready	☐ Gap	☐ N/A
☐	**A.8.34**	Protection of information systems during internal audits	☐ Ready	☐ Gap	☐ N/A

Audit Interviews and Walk-Through

û	Control	Evidence	Status			Evidence Location
☐	**Host**	Audit host designated (usually CISO or ISMS manager)	☐ Ready	☐ Gap	☐ N/A	
☐	**CISO**	CISO available for questions on clauses 5, 6, 9, and 10	☐ Ready	☐ Gap	☐ N/A	
☐	**IT-Admin**	IT administrator prepared for access and network topics	☐ Ready	☐ Gap	☐ N/A	
☐	**Dev**	Engineering lead available for A.8.25 to A.8.28	☐ Ready	☐ Gap	☐ N/A	
☐	**HR**	HR representative available for A.6 and background checks	☐ Ready	☐ Gap	☐ N/A	
☐	**Proc.**	Procurement available for A.5.19 to A.5.22	☐ Ready	☐ Gap	☐ N/A	
☐	**Walk**	Pre-audit walk-through 1 week in advance with all interviewees	☐ Ready	☐ Gap	☐ N/A	

CC-BY-4.0 — Kopexa GmbH — Free-use template with attribution