ISO 27001 internal audit checklist

Annex A controls per ISO/IEC 27001:2022 · 44 controls · for Croatian and US-bound SMB and scale-up teams

How to use this checklist

For each control, verify three things:

1. **Evidence type** — does a document, log, screenshot, or artifact exist that proves it
2. **Frequent fail signal** — what the external auditor usually probes when this control fails
3. **Corrective action** — what to do if the auditor finds a gap already in Stage 1

If you cannot answer yes to all three, the control **is not ready** for the external audit.

Goal: catch the gaps during the internal audit in month 5, not at Stage 1 in month 6.

A.5 Organizational controls (12 controls)

	CONTROL	EVIDENCE TYPE	FREQUENT FAIL SIGNAL
1	**A.5.1** Information security policies	ISMS policy with current management signature, year of last review	Policy from 2021, no review record
2	**A.5.7** Threat intelligence	Threat feed source list, log alert categories, monthly threat report	“We subscribe to a newsletter” without an actionable feed
3	**A.5.9** Inventory of information and other assets	Asset registry with owners, classification tag, last-review date	Excel from 2022, assets without owners
4	**A.5.10** Acceptable use of information and other associated assets	AUP signed annually by employees	AUP exists but employees have not seen it in 18 months
5	**A.5.12** Classification of information	Classification scheme (Public / Internal / Confidential / Restricted), examples per class	Classification in the policy but never applied in practice

	CONTROL	EVIDENCE TYPE	FREQUENT FAIL SIGNAL
6	**A.5.15** Access control	Access matrix per role, joiner/mover/leaver procedure	"IT grants it when needed" with no documented procedure
7	**A.5.19** Information security in supplier relationships	Supplier inventory with risk class, security clauses in contracts	Contracts without security clauses, no supplier list
8	**A.5.23** Information security for use of cloud services	Cloud vendor due diligence (vendor SOC 2 / ISO certificates), data location map	"AWS is secure" without vendor evidence
9	**A.5.24** Information security incident management planning and preparation	Incident response plan with roles, escalation matrix, runbook	IR plan exists but was not tested in 12 months
10	**A.5.30** ICT readiness for business continuity	BCP with RTO/RPO, test report from the last 12 months	BCP from 2022, test "planned" but never conducted
11	**A.5.32** Intellectual property rights	License inventory for all software (vendor + open source)	Open source without an SBOM, vendor licenses expired
12	**A.5.34** Privacy and protection of PII	PII registry, GDPR DPIA for high-risk processing, retention schedule	DPIA does not exist for customer data flows

A.6 People controls (8 controls)

	CONTROL	EVIDENCE TYPE	FREQUENT FAIL SIGNAL
13	**A.6.1** Screening	Pre-employment background check record per hire	"We have an interview process" without a formal background check
14	**A.6.2** Terms and conditions of employment	Contracts with security clauses, signed NDA	Generic contracts without security obligations
15	**A.6.3** Information security awareness, education and training	Annual training delivery with attendance log + quiz results	Email "please read" without evidence of comprehension
16	**A.6.4** Disciplinary process	Disciplinary framework for security violations, examples of application	Policy exists, never used — open question whether it is real
17	**A.6.5** Responsibilities after termination or change of employment	Offboarding checklist, access revocation log, asset return record	Former employees with active VPN or Slack access
18	**A.6.6** Confidentiality or non-disclosure agreements	NDA inventory, expiry tracking, third-party NDAs	NDA signed but not in a central registry
19	**A.6.7** Remote working	Remote work policy, secure home setup guidance, VPN config	"We work from home" without policy or technical controls

	CONTROL	EVIDENCE TYPE	FREQUENT FAIL SIGNAL
20	**A.6.8** Information security event reporting	Reporting channel known to all employees, response time evidence	Employees do not know whom to report an incident to

A.7 Physical controls (12 controls)

	CONTROL	EVIDENCE TYPE	FREQUENT FAIL SIGNAL
21	**A.7.1** Physical security perimeters	Floor plan with perimeters, badge/key access log	Open entrance during business hours, no badge requirement
22	**A.7.2** Physical entry	Visitor log, badge access system, escort procedure	"The manager knows everyone who comes in" — no log
23	**A.7.3** Securing offices, rooms and facilities	Clear desk policy, server room access list, lockable storage	Server room with "the key at reception"
24	**A.7.4** Physical security monitoring	CCTV or access monitoring, retention period, log review schedule	CCTV exists but logs are never reviewed
25	**A.7.5** Protecting against physical and environmental threats	Fire/water/temperature monitoring, UPS test report	UPS exists, but tested only when purchased (2 years untested)
26	**A.7.6** Working in secure areas	Secure area procedure, sign-in/sign-out, photo restrictions	Procedure exists, nobody follows it
27	**A.7.7** Clear desk and clear screen	Spot-check report, screen-lock policy + technical enforcement	Policy exists, lockscreen GPO does not
28	**A.7.9** Security of assets off-premises	Off-premise asset register, encryption requirement, loss procedure	Laptop encryption "exists" but not verified
29	**A.7.10** Storage media	Media inventory, secure disposal certificate, asset destruction log	Hard disks "thrown out" without secure wipe or shred certificate
30	**A.7.11** Supporting utilities	Power redundancy, network redundancy test, environmental controls	Single ISP without fallback
31	**A.7.13** Equipment maintenance	Maintenance log per critical asset, vendor SLA, replacement schedule	Server running since 2019, last service "when we bought it"
32	**A.7.14** Secure disposal or re-use of equipment	Disposal certificate (NAID AAA or equivalent), wipe verification	"We threw it in e-waste" — no certificate

A.8 Technological controls (12 controls)

	CONTROL	EVIDENCE TYPE	FREQUENT FAIL SIGNAL
33	**A.8.2** Privileged access rights	Privileged account inventory, MFA enforcement, periodic review	Admin access without review in 12 months
34	**A.8.5** Secure authentication	MFA enforcement evidence, password policy, breakglass procedure	"We have MFA" for 80% of users, 20% without
35	**A.8.7** Protection against malware	EDR/AV deployment, signature updates, scan log, incident response link	EDR installed, log dashboard not working
36	**A.8.8** Management of technical vulnerabilities	Vulnerability scan report (monthly minimum), patch SLA, exception process	Scan exists, findings from 6 months ago without action
37	**A.8.9** Configuration management	Baseline configurations documented, drift detection report, change approval	"It is set up correctly" without a baseline document
38	**A.8.10** Information deletion	Data retention policy, automated deletion job log, audit trail	Customer data from 2018 still in production DB
39	**A.8.11** Data masking	PII masking in non-prod environments, masked test dataset	Production data copied to staging, no masking
40	**A.8.12** Data leakage prevention	DLP policy, monitoring rules, incident handling	"We trust the employees" — no DLP layer
41	**A.8.13** Information backup	Backup schedule, restore test report from the last 6 months, off-site copy	Backups exist, restore "we never tested"
42	**A.8.16** Monitoring activities	SIEM/log aggregation, alert thresholds, monthly review report	Logs in CloudWatch, nobody looks at them
43	**A.8.24** Use of cryptography	Crypto policy, key inventory, key rotation schedule, KMS audit log	TLS 1.2 minimum, but legacy services still on TLS 1.0
44	**A.8.28** Secure coding	Secure SDLC documentation, code review evidence, SAST scan integration	"We have code review" — PRs merged without approval

What now?

If you are on "we are not sure" for half of these controls, **the internal audit needs 3-4 focused days**, not 1.

If you are on "no" for the majority, scope is too large for the current stage — go back to gap analysis before you start implementation.

If you are on "yes, evidence exists" for everything, you are ready for the external Stage 1.

Need an independent internal audit before Stage 1?

ctrlaltgrow.hr/en/#kontakt · 30-minute call, no obligations, no PowerPoint.