ISO 27001 interni audit checklist

Annex A controls po ISO/IEC 27001:2022 · 44 kontrole · za hrvatske SMB i scale-up timove

Kako koristiti ovaj checklist

Za svaku kontrolu provjeri tri stvari:

1. **Tip evidencije** — postoji li dokument, log, screenshot ili artefakt koji to dokazuje
2. **Frequent fail signal** — što external auditor obično pita kad ova kontrola padne
3. **Korektivna akcija** — što napraviti ako auditor već u Stage 1 nađe gap

Ako ne možeš odgovoriti potvrdno za sve tri, kontrola **nije spremna** za external audit.

Cilj: uloviti gap-ove tijekom internog audita u M5, ne na Stage 1 u M6.

A.5 Organizational controls (12 kontrola)

	KONTROLA	TIP EVIDENCIJE	FREQUENT FAIL SIGNAL
1	**A.5.1** Information security policies	ISMS policy s aktualnim potpisom uprave, godina pregleda	Policy iz 2021., bez review record-a
2	**A.5.7** Threat intelligence	Threat feed source list, log alert kategorija, monthly threat report	"Pretplata na newsletter" bez actionable feed-a
3	**A.5.9** Inventory of information and other assets	Asset registry s vlasnicima, classification tag-om, last-review datum	Excel iz 2022., assets bez vlasnika
4	**A.5.10** Acceptable use of information and other associated assets	AUP potpisan svake godine od zaposlenih	AUP postoji, ali zaposleni ga nisu vidjeli u 18 mjeseci
5	**A.5.12** Classification of information	Classification scheme (Public / Internal / Confidential / Restricted), primjeri po klasi	Klasifikacija u policy-ju ali nikad primijenjena u praksi
6	**A.5.15** Access control	Access matrix per role, joiner/mover/leaver procedure	"Daje IT kad zatreba", bez documented procedure

	KONTROLA	TIP EVIDENCIJE	FREQUENT FAIL SIGNAL
7	**A.5.19** Information security in supplier relationships	Supplier inventory s rizik klasom, security clauses u ugovorima	Ugovori bez security klauzula, supplier list ne postoji
8	**A.5.23** Information security for use of cloud services	Cloud vendor due diligence (SOC 2 / ISO certifikati vendor-a), data location map	"AWS je siguran", bez vendor evidence
9	**A.5.24** Information security incident management planning and preparation	Incident response plan s rolama, escalation matrix, runbook	IR plan postoji ali nije testiran u 12 mjeseci
10	**A.5.30** ICT readiness for business continuity	BCP s RTO/RPO, test report iz zadnjih 12 mjeseci	BCP iz 2022., test "planiran" ali nikad proveden
11	**A.5.32** Intellectual property rights	License inventory za sve software-e (vendor + open source)	Open source bez SBOM-a, vendor licence istekle
12	**A.5.34** Privacy and protection of PII	PII registry, GDPR DPIA za high-risk obradu, retention schedule	DPIA ne postoji za customer data flows

A.6 People controls (8 kontrola)

	KONTROLA	TIP EVIDENCIJE	FREQUENT FAIL SIGNAL
13	**A.6.1** Screening	Pre-employment background check record per hire	"Imamo intervju proces" bez formal background check-a
14	**A.6.2** Terms and conditions of employment	Ugovori sa security clauses, NDA potpisan	Generic ugovori bez security obveza
15	**A.6.3** Information security awareness, education and training	Annual training delivery s attendance log + quiz results	Email s "molim pročitajte" bez evidencije razumijevanja
16	**A.6.4** Disciplinary process	Disciplinski okvir za security violation, primjeri primjene	Policy postoji, nikad korišten — pitanje je li real
17	**A.6.5** Responsibilities after termination or change of employment	Offboarding checklist, access revocation log, asset return record	Bivši zaposleni s aktivnim VPN ili Slack pristupom
18	**A.6.6** Confidentiality or non-disclosure agreements	NDA inventory, expiry tracking, third-party NDA-ovi	NDA potpisan, ali nije u centralnoj evidenciji
19	**A.6.7** Remote working	Remote work policy, secure home setup guidance, VPN config	"Radimo from home" bez policy ili tech kontrola
20	**A.6.8** Information security event reporting	Reporting channel poznat svim zaposlenicima, response time evidencija	Zaposleni ne znaju kome prijaviti incident

A.7 Physical controls (12 kontrola)

	KONTROLA	TIP EVIDENCIJE	FREQUENT FAIL SIGNAL
21	**A.7.1** Physical security perimeters	Floor plan s perimetrima, badge/key access log	Otvoren ulaz tijekom radnog vremena, no badge requirement
22	**A.7.2** Physical entry	Visitor log, badge access system, escort procedure	"Voditelj zna sve koji dolaze" — no log
23	**A.7.3** Securing offices, rooms and facilities	Clear desk policy, server room access list, lockable storage	Server room s "ključ na recepciji"
24	**A.7.4** Physical security monitoring	CCTV ili access monitoring, retention period, log review schedule	CCTV postoji ali se logovi nikad ne pregledavaju
25	**A.7.5** Protecting against physical and environmental threats	Fire/water/temperature monitoring, UPS test report	UPS postoji, ali test od kupnje (2 godine bez provjere)
26	**A.7.6** Working in secure areas	Secure area procedure, sign-in/sign-out, foto zabrane	Procedura postoji, nitko je ne slijedi
27	**A.7.7** Clear desk and clear screen	Spot-check report, screen-lock policy + technical enforcement	Policy postoji, lockscreen GPO ne postoji
28	**A.7.9** Security of assets off-premises	Off-premise asset register, encryption requirement, loss procedure	Laptop encryption "postoji", ne provjereno
29	**A.7.10** Storage media	Media inventory, secure disposal certificate, asset destruction log	Hard diskovi "bačeni" bez wipe ili shred dokumenta
30	**A.7.11** Supporting utilities	Power redundancy, network redundancy test, environmental controls	Single ISP bez fallback-a
31	**A.7.13** Equipment maintenance	Maintenance log per critical asset, vendor SLA, replacement schedule	Server radi od 2019., zadnji service "kad smo ga kupili"
32	**A.7.14** Secure disposal or re-use of equipment	Disposal certificate (NAID AAA ili equivalent), wipe verification	"Bacili smo na elektronički otpad" — no certifikat

A.8 Technological controls (12 kontrola)

	KONTROLA	TIP EVIDENCIJE	FREQUENT FAIL SIGNAL
33	**A.8.2** Privileged access rights	Privileged account inventory, MFA enforcement, periodic review	Admin pristupi bez review-a u 12 mjeseci
34	**A.8.5** Secure authentication	MFA enforcement evidence, password policy, breakglass procedure	"Imamo MFA" za 80% korisnika, 20% bez
35	**A.8.7** Protection against malware	EDR/AV deployment, signature updates, scan log, incident response link	EDR instaliran, log dashboard ne radi

	KONTROLA	TIP EVIDENCIJE	FREQUENT FAIL SIGNAL
36	**A.8.8** Management of technical vulnerabilities	Vulnerability scan report (monthly minimum), patch SLA, exception process	Scan postoji, findings od 6 mjeseci bez akcije
37	**A.8.9** Configuration management	Baseline configurations dokumentirani, drift detection report, change approval	"Posloženo je kako treba" bez baseline dokumenta
38	**A.8.10** Information deletion	Data retention policy, automated deletion job log, audit trail	Customer data iz 2018. još uvijek u prod DB
39	**A.8.11** Data masking	PII masking u non-prod environments, masked test dataset	Production data kopirana u staging, no masking
40	**A.8.12** Data leakage prevention	DLP policy, monitoring rules, incident handling	"Vjerujemo zaposlenima" — no DLP layer
41	**A.8.13** Information backup	Backup schedule, restore test report iz zadnjih 6 mjeseci, off-site copy	Backup-i postoje, restore "nikad nismo testirali"
42	**A.8.16** Monitoring activities	SIEM/log aggregation, alert thresholds, monthly review report	Logovi u CloudWatch, nitko ih ne gleda
43	**A.8.24** Use of cryptography	Crypto policy, key inventory, key rotation schedule, KMS audit log	TLS 1.2 minimum, ali stari servisi još na TLS 1.0
44	**A.8.28** Secure coding	Secure SDLC dokumentacija, code review evidence, SAST scan integration	"Imamo code review", PR-ovi mergani bez approval-a

Što sad?

Ako si na pola od ovih kontrola "nismo sigurni", **internom auditu trebaš 3-4 fokusirana dana**, ne 1.

Ako si na većini "ne", scope ti je preveliki za trenutni stage — vrati se na gap analizu prije nego kreneš na implementaciju.

Ako si na svemu "da, evidencija postoji", spreman si za external Stage 1.

Trebaš nezavisan interni audit prije Stage 1?

ctrlaltgrow.hr/#kontakt · 30-min razgovor, bez obveza, bez PowerPointa.