ISO 27001 Audit-Ready Checklist 2026

Door Secrotec B.V. — ISO 27001 Lead Auditor & informatiebeveiliging

Deze checklist helpt u systematisch te beoordelen of uw Information Security Management System (ISMS) klaar is voor een ISO/IEC 27001-audit. Of u nu toewerkt naar een eerste certificering of een hercertificering: gebruik deze lijst om de belangrijkste bewijslast op orde te krijgen, hiaten vroegtijdig te signaleren en verrassingen tijdens de audit te voorkomen.

Werk de items per thema af. Vink af wat aantoonbaar geregeld én gedocumenteerd is — een maatregel die u niet kunt onderbouwen met bewijs telt tijdens de audit niet mee. Twijfelt u bij een onderdeel? Markeer het en plan een verbeteractie.

> **Tip:** Een auditor toetst niet alleen óf iets bestaat, maar of het werkt, wordt bijgehouden en past bij uw risico's. Denk bij elk item dus aan: beleid, uitvoering én bewijs.

---

1. Scope & context (clausules 4–5)

- ☐ **Scope van het ISMS** is formeel vastgesteld en beschreven: welke organisatieonderdelen, locaties, processen en assets vallen erbinnen — en wat er bewust buiten valt (met onderbouwing).
- ☐ **Context van de organisatie** is in kaart: relevante interne en externe issues die de informatiebeveiliging beïnvloeden (clausule 4.1).
- ☐ **Belanghebbenden** (klanten, leveranciers, toezichthouders, medewerkers) en hun eisen/verwachtingen zijn geïnventariseerd (clausule 4.2).
- ☐ **Wettelijke, contractuele en regelgevende eisen** zijn vastgelegd (denk aan AVG/GDPR, NIS2, sectorspecifieke normen).
- ☐ **Informatiebeveiligingsbeleid** is opgesteld, door de directie goedgekeurd, gedateerd en intern gecommuniceerd.
- ☐ **Rollen, verantwoordelijkheden en bevoegdheden** zijn toegewezen (bijv. CISO/security officer) en aantoonbaar belegd.

- ☐ **Betrokkenheid van de directie (leadership)** is aantoonbaar: besluiten, budget, middelen en zichtbare steun voor het ISMS.

2. Risicoanalyse & risicobehandeling (clausule 6)

- ☐ **Risicobeoordelingsmethodiek** is gedocumenteerd: criteria voor het accepteren van risico's en de schaal voor kans × impact.
- ☐ **Assets, dreigingen en kwetsbaarheden** zijn geïdentificeerd en gekoppeld aan eigenaren.
- ☐ **Risico's zijn beoordeeld** (kans en impact) en geprioriteerd in een actueel risicoregister.
- ☐ **Risicobehandelplan (RTP)** beschrijft per risico de keuze: verminderen, accepteren, vermijden of overdragen.
- ☐ **Geselecteerde beheersmaatregelen** zijn gekoppeld aan de risico's die ze afdekken.
- ☐ **Risico-eigenaren** hebben de restrisico's formeel geaccepteerd.
- ☐ **Informatiebeveiligingsdoelstellingen** zijn meetbaar (SMART), met verantwoordelijke, middelen en deadline.
- ☐ Het risicoregister is **recent geactualiseerd** (minimaal jaarlijks of bij significante wijzigingen).

3. Statement of Applicability (SoA)

- ☐ **SoA is opgesteld** en bevat alle beheersmaatregelen uit Annex A (ISO 27001:2022 — 93 maatregelen).
- ☐ Per maatregel is aangegeven of deze **van toepassing** is (ja/nee) met een **onderbouwing**.
- ☐ Per toepasselijke maatregel is de **implementatiestatus** vastgelegd (geïmplementeerd / in uitvoering / gepland).
- ☐ **Uitsluitingen** zijn expliciet beargumenteerd (waarom een maatregel niet van toepassing is).
- ☐ De SoA is **consistent** met het risicobehandelplan en het risicoregister.
- ☐ De SoA heeft een **versienummer en datum** en is door de juiste rol goedgekeurd.

4. Beheersmaatregelen (ISO 27001:2022 Annex A)

4.1 ORGANISATORISCHE MAATREGELEN (A.5)

- ☐ **Beleid voor informatiebeveiliging** en onderwerp-specifieke beleidsstukken zijn vastgesteld en periodiek herzien.
- ☐ **Toegangsbeleid** en het beheer van toegangsrechten zijn gedocumenteerd (need-to-know / least privilege).
- ☐ **Leveranciers- en ketenbeheer**: beveiligingsafspraken met leveranciers, verwerkers en cloud-diensten zijn contractueel vastgelegd.
- ☐ **Incidentmanagement**: proces voor melden, beoordelen en afhandelen van beveiligingsincidenten is operationeel.
- ☐ **Bedrijfscontinuïteit (ICT-continuïteit)** en herstelplannen zijn gedocumenteerd en getest.
- ☐ **Classificatie van informatie** is ingevoerd (bijv. publiek / intern / vertrouwelijk / geheim) met bijbehorende behandeling.
- ☐ **Threat intelligence** wordt verzameld en benut voor het bijsturen van maatregelen.

4.2 MAATREGELEN VOOR MENSEN (A.6)

- ☐ **Screening** van medewerkers vóór indiensttreding vindt plaats, passend bij rol en risico.
- ☐ **Arbeidsvoorwaarden** bevatten verantwoordelijkheden voor informatiebeveiliging.
- ☐ **Bewustwording, opleiding en training** worden structureel uitgevoerd en geregistreerd (incl. deelnamebewijs).
- ☐ **Disciplinair proces** bij overtredingen is vastgelegd.
- ☐ **Uit-/doorstroomproces**: intrekken van toegang en retourneren van assets bij vertrek of functiewijziging.
- ☐ **Vertrouwelijkheids-/geheimhoudingsverklaringen (NDA’s)** zijn ondertekend en gearchiveerd.

4.3 FYSIEKE MAATREGELEN (A.7)

- ☐ **Fysieke toegangsbeveiliging** tot kantoren, serverruimtes en gevoelige zones is geregeld en geregistreerd.
- ☐ **Beveiligde zones** en een clear desk / clear screen-beleid zijn ingevoerd.
- ☐ **Bescherming van apparatuur**: tegen stroomuitval, brand, water en diefstal.
- ☐ **Veilige verwijdering en hergebruik** van media en apparatuur (datawissen / vernietiging) is geborgd.
- ☐ **Bekabeling en nutsvoorzieningen** zijn beschermd tegen onderschepping en uitval.

4.4 TECHNOLOGISCHE MAATREGELEN (A.8)

- ☐ **Endpointbeveiliging** (antimalware, hardening) is uitgerold op alle apparaten binnen de scope.
- ☐ **Patch- en kwetsbaarhedenbeheer**: tijdige updates en periodieke vulnerability scans.
- ☐ **Logging en monitoring** zijn ingericht; logs worden bewaard en periodiek beoordeeld.
- ☐ **Back-ups** worden gemaakt, beveiligd opgeslagen én aantoonbaar getest op herstelbaarheid.
- ☐ **Versleuteling / cryptografie** wordt toegepast op gevoelige data (in rust en in transit), met sleutelbeheer.
- ☐ **Netwerkbeveiliging**: segmentatie, firewallregels en beveiliging van netwerkdiensten.
- ☐ **Identiteits- en toegangsbeheer (IAM)**: sterke authenticatie (MFA), beheer van bevoorrechte accounts.
- ☐ **Veilige softwareontwikkeling**: secure coding, scheiding van omgevingen (OTAP) en wijzigingsbeheer.

5. Interne audit (clausule 9.2)

- ☐ **Intern auditprogramma** is opgesteld met frequentie, scope en methode.
- ☐ **Auditors zijn onafhankelijk** van het geauditeerde proces en aantoonbaar competent.

- ☐ **Alle ISMS-onderdelen** zijn binnen de auditcyclus gedekt.
- ☐ **Auditbevindingen** zijn vastgelegd in rapportages, inclusief afwijkingen en observaties.
- ☐ **Opvolging van bevindingen** is geborgd en de status wordt bewaakt.

6. Management review (clausule 9.3)

- ☐ **Directiebeoordeling** vindt minimaal jaarlijks plaats en is genotuleerd.
- ☐ De input bevat alle verplichte onderwerpen: auditresultaten, incidenten, doelstellingen, risico's, feedback en verbetermogelijkheden.
- ☐ **Besluiten en acties** uit de review zijn vastgelegd met eigenaar en termijn.
- ☐ **Prestatie-indicatoren (KPI's/metingen)** van het ISMS zijn beoordeeld (clausule 9.1).
- ☐ **Wijzigingen in context of risico's** sinds de vorige review zijn meegenomen.

7. Verbeteracties (clausule 10)

- ☐ **Afwijkingen (non-conformiteiten)** worden geregistreerd met root-cause-analyse.
- ☐ **Correctieve maatregelen** zijn gedefinieerd, uitgevoerd en op effectiviteit beoordeeld.
- ☐ **Register van verbeteracties** is actueel en de doorlooptijden worden bewaakt.
- ☐ **Continue verbetering** is aantoonbaar: het ISMS wordt structureel bijgesteld op basis van leerpunten.

8. Documentatie & bewijs

- ☐ **Documentbeheer** is op orde: versiebeheer, eigenaar, goedkeuring en review-datum per document.
- ☐ **Verplichte gedocumenteerde informatie** is aanwezig (scope, beleid, risicobeoordeling, RTP, SoA, doelstellingen, auditresultaten, management review, correctieve acties).
- ☐ **Registraties (records)** zijn vindbaar en herleidbaar: trainingen, incidenten, back-uptests, toegangsreviews.

- ☐ **Bewaartermijnen** voor documenten en logs zijn vastgesteld en worden nageleefd.
- ☐ **Toegang tot documentatie** is gecontroleerd; verouderde versies zijn uit roulatie.
- ☐ **Eén centrale bron van waarheid** (ISMS-omgeving of -map) is ingericht en bekend bij betrokkenen.

Klaar om audit-ready te worden?

U heeft de checklist doorlopen — maar een paar open vinkjes of twijfels kunnen het verschil maken tussen een soepele audit en een afwijking. Secrotec voert als onafhankelijk **ISO 27001 Lead Auditor** een vrijblijvende audit-scan uit: we beoordelen uw ISMS, brengen de hiaten in kaart en geven u een concreet stappenplan richting certificering.

Vraag een vrijblijvende audit-scan aan:

- Web: **secrotec.nl/contact/**
- E-mail: **info@secrotec.nl**
- Telefoon: **+31 6 19529370**
