



Wil je aan de slag met ISO 27001 maar weet je niet waar je moet beginnen? Aan de hand van deze praktische checklist ontdek je in één oogopslag waar je organisatie staat ten opzichte van ISO 27001 en welke stappen er nog genomen moeten worden voor het implementeren van deze norm.

1

Vorbereiding & strategie

- ☐ Hebben we ISO 27001 als strategisch doel vastgelegd?
- ☐ Is er intern draagvlak bij directie en management?
- ☐ Is er een projectteam of informatiebeveiliging verantwoordelijke aangewezen?
- ☐ Zijn de doelstellingen voor informatiebeveiliging SMART geformuleerd?

2

Scope & risicoanalyse

- ☐ Is de scope van het ISMS afgebakend (systemen, afdelingen, locaties)?
- ☐ Hebben we een actuele inventarisatie van informatiemiddelen?
- ☐ Is er een risicoanalyse uitgevoerd volgens een erkende methode?
- ☐ Zijn risicobehandelingen geselecteerd en gedocumenteerd?

3

Beleidsontwikkeling & procedures

- ☐ Is security opgenomen in het beleid voor wijzigingsbeheer en projectplanning?
- ☐ Voldoet het toegangsbeleid aan eisen als *least privilege*, *zero trust*, *just-in-time*?
- ☐ Wordt er voldaan aan alle wettelijke eisen (AVG, sectorspecifiek)?
- ☐ Worden securityeisen en -impact meegenomen in het leveranciersbeleid?

4

Techniek & bewustwording

- ☐ Is de IT-infrastructuur adequaat beveiligd (firewalls, antivirus, MFA)?
- ☐ Voldoet de fysieke beveiliging aan de benodigde eisen?
- ☐ Is er een security awareness programma opgezet?
- ☐ Worden medewerkers getraind en gescreend bij onboarding?
- ☐ Is er beleid over het delen en archiveren van vertrouwelijke data?

5

Monitoring & incidentmanagement

- ☐ Wordt monitoring uitgevoerd op afwijkingen en bedreigingen?
- ☐ Is er een incidentresponsproces ingericht?
- ☐ Zijn logbestanden beveiligd en bewaard volgens beleid?
- ☐ Is 24x7 detectie en respons ingericht (SOC, SIEM)?

6

Controle & audit

- ☐ Worden er jaarlijks interne audits uitgevoerd op het ISMS?
- ☐ Is er een managementreview op basis van meetgegevens?
- ☐ Wordt het continu verbeterproces actief beheerd (PDCA)?
- ☐ Zijn auditbevindingen gedocumenteerd en verwerkt?
- ☐ Is er een verklaring voor toepasselijkheid?

7

Certificering

- ☐ Is er een gecertificeerde auditor geselecteerd voor de auditfase?
- ☐ Is het certificaat officieel verkregen en geregistreerd?
- ☐ Wordt her-certificering voorbereid en ingepland?



**Heb je hulp nodig bij het invullen van deze checklist?
Neem dan contact met ons op, we helpen je graag.**