Checklist ISO 27001

1. Beleid vaststellen

- [ ] Context van de organisatie is bepaald.
- [ ] Toepassingsgebied van de informatiebeveiliging is in kaart gebracht.
- [ ] Belanghebbenden zijn in kaart gebracht.
- [ ] Doelstellingen zijn bepaald in termen van:
  - [ ] Beschikbaarheid van informatie
  - [ ] Integriteit van informatie
  - [ ] Vertrouwelijkheid van informatie
- [ ] Rollen, verantwoordelijkheden en bevoegdheden zijn vastgesteld.

2. Analyse van processen, systemen en leveranciers

- [ ] Informatieclassificatie in termen van:
  - [ ] Beschikbaarheid
  - [ ] Integriteit
  - [ ] Vertrouwelijkheid
- [ ] Inventarisatie en business impact vaststellen o.b.v. informatieclassificatie:
  - [ ] Processen
  - [ ] Systemen
  - [ ] Leveranciers
- [ ] Eventueel zijn ook losse bedrijfsmiddelen (laptops, telefoons) in kaart gebracht.

3. Risicobeheersing starten

- [ ] Risicoacceptatie is vastgesteld.
- [ ] Potentiële dreigingen en risico's zijn in kaart gebracht.
- [ ] Eerder plaatsgevonden incidenten zijn bekeken.

4. Implementeren van maatregelen

- [ ] Risico's uit de risicoanalyse zijn volledig uitgewerkt en de aanpak per risico is bepaald:
  - [ ] Beheersen
  - [ ] Overdragen
  - [ ] Ontwijken
  - [ ] Accepteren
- [ ] Maatregelen zijn bepaald.
- [ ] De maatregelen zijn geïmplementeerd.

Checklist ISO 27001

5. Resterende risico evalueren

- [ ] Het restrisico is bepaald.
- [ ] Extra maatregelen zijn geïmplementeerd bij onvoldoende teruggebrachte risico's.

6.Invulling van de AVG

- [ ] Welke persoonsgegevens worden verwerkt door de organisatie (en/of haar toeleveranciers)?
- [ ] DPIA uitgevoerd voor risicovolle verwerking van gevoelige of bijzondere persoonsgegevens.
- [ ] Verwerkersovereenkomst is vastgesteld/geïnventariseerd.
- [ ] Er is een procedure opgesteld voor het melden van datalekken.
  - [ ] Medewerkers zijn hierover geïnstrueerd.

7. Bewustwording onder medewerkers vergroten

- [ ] Medewerkers zijn geïnformeerd over het beleid.
- [ ] Trainingen rondom informatiebeveiliging zijn aangeboden.

8. Interne controle en audits

- [ ] Periodieke controles zijn ingericht.
  - [ ] Autorisatiecontroles door eigenaren van informatiesystemen.
  - [ ] Leveranciersbeoordelingen
  - [ ] Organisatorische/proces controles
  - [ ] Technische controles
- [ ] Interne audits zijn uitgevoerd.
  - [ ] Er is een auditprogramma opgesteld.
  - [ ] Rapportage en opvolging

Checklist ISO 27001

9. Voorbereiding op de certificering

- [ ] Verklaring van toepasselijkheid controleren en vaststellen.
- [ ] Managementrapportage over informatiebeveiliging opgesteld en ondertekend.
- [ ] Proefaudit uitgevoerd.
- [ ] Herstelacties toegepast.

10. Externe audit en certificering

- [ ] Geaccrediteerde auditor is bepaald.
- [ ] Verschillende audits ingepland.
- [ ] Plan van aanpak voor de opvolging van de audit.