

Checklist **Risicoanalyse**

1. Scope bepalen

- ☐ Wat is de scope van de risicoanalyse?
 - ☐ Informatiesysteem/ applicatie
 - ☐ Specifiek proces
 - ☐ Afdeling/ team
 - ☐ Leverancier/ externe partij
 - ☐ Gehele organisatie
- ☐ Afbakening is duidelijk vastgelegd en gecommuniceerd
- ☐ Indien grote scope: verdeling in deelgebieden?

2. Risico's op basis van dreigingen identificeren

- ☐ Dreigingsbronnen geïnventariseerd:
 - ☐ Organisatorische dreigingen (procedures, kennisverlies)
 - ☐ Menselijke dreigingen (fouten, opzettelijke acties, social engineering)
 - ☐ Fysieke dreigingen (brand, overstroming, stroomuitval)
 - ☐ Technische dreigingen (malware, ransomware, hacking)
 - ☐ Externe dreigingen (leveranciers, natuurrampen, regelgeving)
- ☐ Gebruikte dreigingsmodellen:
 - ☐ RAVIB
 - ☐ MAPGOOD
 - ☐ OWASP Top 10
 - ☐ Eigen inventarisatie/ brainstorm

3. Inschatting risico's (kans & impact)

- ☐ Risicomatrix opgesteld met afgesproken schaal (bv. 1 t/m 5 of aangepast model)
- ☐ Eenduidige definities van kans en impact afgestemd binnen het team
- ☐ Per risico is bepaald:
 - ☐ Kans (frequentie/ waarschijnlijkheid)
 - ☐ Impact (schade/ gevolg)
- ☐ Eenduidige definities van kans en impact afgestemd binnen het team
- ☐ Resultaat: ingevulde risicomatrix met geprioriteerde risico's

4. Bestaande beveiligingsmaatregelen inventariseren

- ☐ Welke bestaande maatregelen zijn aanwezig per risico?
 - ☐ Organisatorische maatregelen (rollen & verantwoordelijkheden, beleid)
 - ☐ Menselijke maatregelen (protocol, werkinstructies, training)
 - ☐ Fysieke maatregelen (kluissloten, cameratoezicht, toegangspasjes)
 - ☐ Technische maatregelen (firewalls, monitoring)
- ☐ Zijn deze maatregelen effectief/ afdoende?

Checklist **Risicoanalyse**

5. Verantwoordelijke vastleggen

- ☐ Wie is verantwoordelijke per risico?
- ☐ Wie is de actiehouders voor het treffen van maatregelen?
- ☐ Wie monitort de voortgang en naleving?

6. Risicobeoordeling & classificatie

- ☐ Per risico bepaald:
 - ☐ Accepteren
 - ☐ Mitigeren (maatregelen treffen)
 - ☐ Overdragen (verzekering/ uitbesteding)
 - ☐ Vermijden (activiteit stoppen)
- ☐ Risico's met prioriteit voor actie gemarkeerd

7. Aanbevolen maatregelen formuleren

- ☐ Concreet plan van aanpak per risico (afhankelijk van stap 5):
 - ☐ Maatregelen om kans te verkleinen
 - ☐ Maatregelen om impact te verminderen
 - ☐ Tijdlijn en actiehouders per maatregel

8. Vervolgactie & monitoring

- ☐ Beoordeling effectiviteit van maatregelen
- ☐ Plan voor periodieke evaluatie van risicoanalyse
 - ☐ Frequentie updates (bv. jaarlijks of bij grote wijzigingen)
- ☐ Rapportage- en escalatieprocedure ingericht

Wil jij geen zorgen meer over de constante herzieningen van de normen? Wij zorgen dat onze software altijd up-to-date is.

Laat **Base27** je helpen.

Bekijk de tool