

Checklist

5.35 – Onafhankelijke beoordeling van informatiebeveiliging

Thema: Organisatorisch | ISO 27002: 5.35 | Gerelateerd: 5.36, 5.31

Doelstelling

Aantonen dat het informatiebeveiligingsbeleid en de implementatie daarvan periodiek onafhankelijk worden beoordeeld om de effectiviteit en naleving te waarborgen.

Auditbeleid en -planning

- ☐ Is er een auditbeleid of -programma voor informatiebeveiliging vastgesteld?
- ☐ Worden audits uitgevoerd door onafhankelijke partijen (intern of extern)?
- ☐ Is de auditfrequentie afgestemd op het risiconiveau van de organisatie?
- ☐ Worden auditplannen tijdig gecommuniceerd aan betrokkenen?
- ☐ Zijn de scope en criteria van audits vooraf vastgesteld en gedocumenteerd?

Uitvoering van audits

- ☐ Hebben auditors toegang tot alle benodigde systemen, documenten en medewerkers?
- ☐ Worden audits uitgevoerd conform een vastgestelde methodologie (ISO 27001, BIO2, etc.)?
- ☐ Worden auditbevindingen gedocumenteerd inclusief bewijs?
- ☐ Worden geconstateerde tekortkomingen geclassificeerd naar ernst?
- ☐ Is er aandacht voor zowel technische als organisatorische beveiligingsaspecten?

Opvolging van bevindingen

- ☐ Worden auditbevindingen gerapporteerd aan het management?
- ☐ Worden verbeteracties gedefinieerd voor elke bevinding?
- ☐ Worden verbeteracties toegewezen aan verantwoordelijken met een deadline?
- ☐ Worden verbeteracties gemonitord op implementatie en effectiviteit?
- ☐ Worden herhaalde bevindingen geëscaleerd naar hoger management?

Externe certificering

- ☐ Wordt externe certificering (ISO 27001, BIO2-audit) overwogen of uitgevoerd?

- ☐ Worden DigiD-audits, ISAE 3000/3402-rapporten of vergelijkbare audits uitgevoerd waar vereist?
- ☐ Worden certificeringsresultaten gebruikt als bewijs van compliance richting opdrachtgevers?
- ☐ Worden bevindingen uit externe audits behandeld als interne auditbevindingen?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 22
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.