

Checklist

5.3 – Scheiding van taken

Thema: Organisatorisch | ISO 27002: 5.3 | Gerelateerd: 5.2, 8.2

Doelstelling

Aantonen dat conflicterende taken en verantwoordelijkheden zijn gescheiden om het risico op fraude, fouten en misbruik van bevoegdheden te beperken.

Beleid voor scheiding van taken

- ☐ Is er beleid voor scheiding van taken (segregation of duties)?
- ☐ Zijn conflicterende functies geïdentificeerd en gedocumenteerd?
- ☐ Is het beleid van toepassing op zowel IT-functies als bedrijfsprocessen?
- ☐ Wordt scheiding van taken meegenomen bij het ontwerp van nieuwe processen en systemen?

Implementatie van scheiding

- ☐ Zijn autorisaties zo ingericht dat één persoon geen kritieke handeling volledig alleen kan uitvoeren?
- ☐ Is het vier-ogen-principe toegepast voor kritieke transacties en wijzigingen?
- ☐ Worden beheerdersrechten gescheiden van reguliere gebruikersrechten?
- ☐ Is ontwikkeling, testen en productie toegang gescheiden voor systemen?
- ☐ Zijn financiële autorisaties (aanvragen, goedkeuren, uitbetalen) gescheiden?

Compenserende maatregelen

- ☐ Zijn er compenserende maatregelen waar volledige scheiding niet mogelijk is (bv. kleine organisaties)?
- ☐ Worden compenserende maatregelen gedocumenteerd en periodiek beoordeeld?
- ☐ Is extra monitoring ingericht op functies waar scheiding niet volledig is doorgevoerd?

Controle en naleving

- ☐ Worden toegangsrechten periodiek gereviewed op ongewenste combinaties van rechten?
- ☐ Is er een SoD-matrix (Segregation of Duties matrix) beschikbaar en actueel?
- ☐ Worden schendingen van scheiding van taken als beveiligingsincident behandeld?
- ☐ Worden bevindingen gerapporteerd aan management of interne audit?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 20
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident	Status:	☐ Voldoet ☐ Actiepunt ☐ N.v.t.