

Checklist

5.36 – Naleving van beleid, regels en normen voor informatiebeveiliging

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

Doelstelling

Aantonen dat de naleving van het informatiebeveiligingsbeleid en geldende normen periodiek wordt beoordeeld en dat afwijkingen worden gecorrigeerd.

Compliancebeoordeling

- ☐ Worden beveiligingsbeleid en -procedures periodiek getoetst op naleving?
- ☐ Is er een intern controleproces voor naleving van het informatiebeveiligingsbeleid?
- ☐ Zijn verantwoordelijkheden voor compliancebewaking belegd bij een eigenaar?
- ☐ Wordt naleving beoordeeld op zowel technisch als organisatorisch niveau?
- ☐ Worden systeemeigenaren betrokken bij de compliancebeoordeling van hun systemen?

Technische compliancecontroles

- ☐ Worden technische configuraties periodiek gecontroleerd op naleving van baselines?
- ☐ Worden vulnerability scans ingezet om technische afwijkingen te detecteren?
- ☐ Worden penetratietests uitgevoerd om de effectiviteit van technische maatregelen te toetsen?
- ☐ Worden cloudconfiguraties gecontroleerd op naleving via CSPM-tools?

Afwijkingen en correcties

- ☐ Worden geconstateerde afwijkingen van beleid gedocumenteerd?
- ☐ Is er een proces voor het corrigeren van afwijkingen met prioritering op ernst?
- ☐ Worden afwijkingen gerapporteerd aan de proceseigenaar en CISO?
- ☐ Worden herhaalde afwijkingen geëscaleerd naar management?
- ☐ Is er een uitzondering- of dispensatieproces voor gemotiveerde afwijkingen?

Rapportage en verbetering

- ☐ Worden complianceresultaten periodiek gerapporteerd aan het management?
- ☐ Is er een compliancedashboard of overzicht van de beveiligingsstatus?

- ☐ Worden trends in niet-naleving geanalyseerd op structurele oorzaken?
- ☐ Worden complianceresultaten gebruikt als input voor beleidsverbetering?

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