

Checklist

5.31 – Wettelijke, statutaire, regelgevende en contractuele eisen

Thema: Organisatorisch | ISO 27002: 5.31 | Gerelateerd: 5.32, 5.33

Doelstelling

Aantonen dat de organisatie alle relevante wettelijke, regelgevende en contractuele verplichtingen op het gebied van informatiebeveiliging identificeert en naleeft.

Identificatie van verplichtingen

- ☐ Is er een actueel overzicht van alle relevante wet- en regelgeving op het gebied van informatiebeveiliging?
- ☐ Zijn verplichtingen uit NIS2, AVG, BIO2, Archiefwet en sectorale regelgeving geïdentificeerd?
- ☐ Worden wijzigingen in wet- en regelgeving actief gemonitord en vertaald naar maatregelen?
- ☐ Is vastgelegd wie verantwoordelijk is voor het bijhouden van compliance-verplichtingen?

Naleving van wet- en regelgeving

- ☐ Is de organisatie aantoonbaar compliant met de AVG (verwerkersregister, DPIA's, meldplicht)?
- ☐ Voldoet de organisatie aan de NIS2-verplichtingen (risicomaatregelen, meldplicht, governance)?
- ☐ Wordt voldaan aan de BIO2-verplichtingen als overheidsorganisatie?
- ☐ Worden wettelijke bewaartermijnen voor informatie nageleefd?
- ☐ Is er een functionaris gegevensbescherming (FG/DPO) aangesteld waar vereist?

Contractuele verplichtingen

- ☐ Zijn contractuele beveiligingseisen van klanten en opdrachtgevers geïdentificeerd?
- ☐ Worden contractuele beveiligingsverplichtingen nagekomen en gemonitord?
- ☐ Worden beveiligingseisen in contracten periodiek herzien op actualiteit?
- ☐ Is er een proces voor het signaleren van contractuele verplichtingen die niet kunnen worden nagekomen?

Rapportage en audit

- ☐ Wordt compliance met wet- en regelgeving periodiek intern geauditeerd?
- ☐ Worden compliancebevindingen gerapporteerd aan management en bestuur?
- ☐ Is er een proces voor het opvolgen van bevindingen uit audits en toezichthoudersinspecties?



Worden externe certificeringen of audits (ISO 27001, DigiD-audit) ingezet als compliancebewijs?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 21
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.