

Checklist

5.22 – Monitoring, beoordeling en wijzigingsbeheer van leveranciersdiensten

Thema: Organisatorisch | ISO 27002: 5.22 | Gerelateerd: 5.19, 5.20

Doelstelling

Aantonen dat de organisatie de prestaties en naleving van leveranciers actief monitort, beoordeelt en wijzigingen in dienstverlening beheerst.

Monitoring van leveranciersdiensten

- ☐ Worden de prestaties van leveranciers periodiek gemeten tegen afgesproken SLA's?
- ☐ Is er een proces voor het opvolgen van SLA-afwijkingen?
- ☐ Worden beveiligingsrapportages van leveranciers (incidenten, audits) periodiek beoordeeld?
- ☐ Is er een contactpersoon (service owner) aangewezen voor elke kritieke leverancier?

Periodieke beoordeling

- ☐ Worden leveranciers minimaal jaarlijks formeel beoordeeld op beveiligingsprestaties?
- ☐ Zijn beoordelingscriteria vooraf vastgesteld en gecommuniceerd aan de leverancier?
- ☐ Worden bevindingen uit beoordelingen gedocumenteerd en opgevolgd?
- ☐ Worden structurele tekortkomingen geëscaleerd naar management of inkoop?

Wijzigingsbeheer

- ☐ Is er een proces voor beoordeling van wijzigingen in leveranciersdiensten?
- ☐ Worden significante wijzigingen (infrastructuur, personeel, subcontractors) door de leverancier gemeld?
- ☐ Worden wijzigingen beoordeeld op impact voor informatiebeveiliging vóór implementatie?
- ☐ Is er change management afgesproken voor kritieke diensten?

Rapportage en escalatie

- ☐ Worden leveranciersbeoordeling gerapporteerd aan het management?
- ☐ Is er een escalatieproces bij herhaalde of ernstige tekortkomingen?
- ☐ Worden beveiligingsincidenten bij leveranciers gemeld aan de CISO?
- ☐ Is er een contractuele grondslag voor beëindiging bij structurele niet-naleving?

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