

Checklist

5.30 – ICT-gereedheid voor bedrijfscontinuïteit

Thema: Organisatorisch | ISO 27002: 5.30 | Gerelateerd: 5.29, 8.13, 8.14

Doelstelling

Aantonen dat ICT-systemen en -infrastructuur voldoende zijn voorbereid op verstoringen zodat bedrijfscontinuïteit gewaarborgd blijft.

ICT-continuïteitsplan

- ☐ Is er een ICT-continuïteitsplan (of disaster recovery plan) beschikbaar en actueel?
- ☐ Is het ICT-continuïteitsplan afgestemd op het bedrijfscontinuïteitsplan (BCP)?
- ☐ Zijn RTO's (hersteltijden) en RPO's (herstelpunten) per kritiek systeem vastgelegd?
- ☐ Worden kritieke ICT-processen geïdentificeerd en geprioriteerd voor herstel?
- ☐ Wordt het ICT-continuïteitsplan minimaal jaarlijks herzien?

Technische continuïteitsmaatregelen

- ☐ Zijn kritieke systemen redundant uitgevoerd (hardware, connectiviteit, stroom)?
- ☐ Is er een uitwijkomgeving beschikbaar voor kritieke systemen?
- ☐ Worden back-ups bewaard op een locatie gescheiden van de primaire omgeving?
- ☐ Is automatische failover ingericht voor de meest kritieke systemen?
- ☐ Is UPS en noodstroom aanwezig voor kritieke infrastructuur?

Testen van continuïteit

- ☐ Worden herstelscenario's (disaster recovery) minimaal jaarlijks getest?
- ☐ Worden RTO's en RPO's daadwerkelijk gehaald tijdens testen?
- ☐ Worden testresultaten gedocumenteerd en verbeterpunten opgevolgd?
- ☐ Worden back-upherstel en failover-procedures aantoonbaar getest?

Leveranciers en uitbesteding

- ☐ Zijn continuïteitsverplichtingen opgenomen in contracten met ICT-leveranciers?
- ☐ Is vastgelegd hoe leveranciers de continuïteit van hun diensten waarborgen?

☐ Worden continuïteitsplannen van kritieke leveranciers periodiek beoordeeld?

☐ Is er een exitstrategie voor kritieke leveranciers bij onverwachte beëindiging?

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