

Checklist

8.14 – Redundantie van informatieverwerkingsfaciliteiten

Thema: Technisch | ISO 27002: 8.14 | Gerelateerd: 8.6, 8.13

Doelstelling

Aantonen dat kritieke informatieverwerkingsfaciliteiten redundant zijn uitgevoerd zodat beschikbaarheid gewaarborgd blijft bij storingen.

Redundantiebeleid en -strategie

- ☐ Zijn kritieke systemen en infrastructuurcomponenten geïdentificeerd die redundantie vereisen?
- ☐ Zijn beschikbaarheidseisen (SLA's, uptime) per systeem vastgelegd?
- ☐ Is de redundantiestrategie (actief-actief, actief-passief, failover) per systeem beschreven?
- ☐ Wordt redundantie meegenomen bij ontwerp van nieuwe systemen en infrastructuur?

Technische redundantie

- ☐ Zijn kritieke servers geconfigureerd met redundante componenten (voeding, opslag, netwerk)?
- ☐ Is er een redundante internetverbinding via een andere provider of route?
- ☐ Zijn kritieke applicaties ingericht op meerdere servers of in een cluster?
- ☐ Wordt gebruik gemaakt van load balancing voor kritieke webdiensten?
- ☐ Is cloudinfrastructuur ingericht over meerdere beschikbaarheidszones?

Uitwijklocatie en disaster recovery

- ☐ Is er een uitwijklocatie of clouduitwijkoplossing voor kritieke systemen?
- ☐ Is de uitwijklocatie voldoende geografisch gescheiden van de primaire locatie?
- ☐ Worden uitwijkprocedures periodiek getest?
- ☐ Is het RTO (hersteltijd) voor kritieke systemen haalbaar met de huidige redundantie?

Monitoring en testen

- ☐ Worden redundante componenten actief gemonitord op beschikbaarheid en gezondheid?
- ☐ Worden failover-mechanismen periodiek getest (geplande switchover)?
- ☐ Worden testresultaten gedocumenteerd en verbeterpunten opgevolgd?



Is er een procedure voor herstel naar de primaire omgeving na een failover?

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