

Checklist

8.13 – Back-up van informatie

Thema: Technisch | ISO 27002: 8.13 | Gerelateerd: 8.6, 5.29

Doelstelling

Aantonen dat back-ups van informatie en systemen worden gemaakt, bewaard en getest conform vastgesteld beleid, zodat herstel na een incident mogelijk is.

Back-upbeleid

- Is er een vastgesteld back-upbeleid met eisen voor frequentie, retentie en opslag?
- Zijn RPO (Recovery Point Objective) en RTO (Recovery Time Objective) per systeem vastgelegd?
- Is het back-upbeleid afgestemd op de kritikaliteit en classificatie van informatie?
- Worden back-upeisen meegenomen bij aanschaf of implementatie van nieuwe systemen?

Uitvoering van back-ups

- Worden back-ups automatisch uitgevoerd conform het vastgestelde schema?
- Worden zowel volledige als incrementele back-ups gemaakt waar relevant?
- Worden back-ups opgeslagen op een locatie gescheiden van de primaire data (offsite of cloud)?
- Worden back-ups versleuteld opgeslagen?
- Worden back-ups bewaard conform de wettelijke retentietermijnen?

Testen en verificatie

- Worden back-ups periodiek getest op volledigheid en herstelbaarheid?
- Worden hersteltest uitgevoerd in een gecontroleerde omgeving?
- Worden testresultaten gedocumenteerd en afwijkingen opgevolgd?
- Is het herstelproces beschreven en getest door de beheerorganisatie?

Beheer en monitoring

- Worden back-upfouten automatisch gesignaleerd en opgevolgd?
- Is er een overzicht van welke systemen en data worden meegenomen in back-ups?
- Worden back-ups gemonitord op volledigheid en beschikbaarheid?



Worden back-upmedium en cloudopslag periodiek gecontroleerd op integriteit?

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