

Checklist

5.23 – Informatiebeveiliging bij gebruik van clouddiensten

Thema: Organisatorisch | ISO 27002: 5.23 | Gerelateerd: 5.19, 5.22

Doelstelling

Aantonen dat de organisatie cloudgebruik beheerst via vastgesteld beleid, risicoafweging en contractuele eisen, zodat informatie in de cloud adequaat is beveiligd.

Cloudbeleid en -strategie

- ☐ Is er beleid voor het gebruik van clouddiensten (toegestane diensten, risicocriteria)?
- ☐ Is een cloudregister bijgehouden met alle gebruikte clouddiensten (inclusief shadow IT)?
- ☐ Worden cloudleveranciers beoordeeld op beveiligingscertificeringen (ISO 27001, SOC 2)?
- ☐ Is vastgelegd welke data wel en niet in de cloud mag worden opgeslagen?
- ☐ Wordt cloudgebruik periodiek gereviewed en getoetst aan het beleid?

Contractuele en juridische eisen

- ☐ Zijn verwerkersovereenkomsten (AVG) afgesloten met alle cloudleveranciers die persoonsgegevens verwerken?
- ☐ Is de datalocatie (land/regio) contractueel vastgelegd voor gevoelige data?
- ☐ Zijn eisen voor encryptie, toegangsbeveiliging en logging opgenomen in het contract?
- ☐ Is het recht op audit of inzage in beveiligingsrapportages contractueel verankerd?

Toegang en identiteitsbeheer

- ☐ Is toegang tot cloudomgevingen beveiligd met MFA?
- ☐ Worden cloud-IAM-rechten beheerd conform het least-privilege principe?
- ☐ Worden cloud-IAM-rechten periodiek gereviewed en overbodige rechten verwijderd?
- ☐ Is er een procedure voor toegangsintrekking bij uitdiensttreding voor cloudplatforms?

Monitoring en incidenten

- ☐ Worden cloudactiviteiten gelogd en gemonitord (CloudTrail, Azure Monitor, etc.)?
- ☐ Is er een procedure voor opvolging bij beveiligingsincidenten in cloudomgevingen?
- ☐ Worden cloudbeveiligingsconfiguraties periodiek gecontroleerd (CSPM-tool of handmatig)?



Is er een exitstrategie voor het geval de cloudleverancier de dienst beëindigt?

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