



Scope thema inspectie leveranciersmanagement

1. Beoordeling van derde partijen (risico's van uitbesteding)

a. Heeft de AED inzicht in de cybersecurity-risico's die zij loopt als zij onderdelen van de essentiële dienstverlening uitbesteedt (in algemene zin)?

b. Heeft de AED inzicht in de risico's die de keuze voor een specifieke leverancier met zich meebrengt voor deze uitbesteding?

2. Contractmanagement (overzicht)

Heeft de AED inzicht in de aanwezige leveranciers?

3. Contractuele overeenkomsten (inhoud)

a. Zijn de verantwoordelijkheden m.b.t. cybersecurity duidelijk gemaakt?

b. Welke security-eisen zijn overeengekomen met de leveranciers?

c. Zijn security-eisen risico-gebaseerd tot stand gekomen (oftewel, cf. risico's zoals onder punt 1 bepaald)?

d. Gelden de security-eisen ook voor onderleveranciers?

e. Wat is afgesproken over het melden van cybersecurity-incidenten die zich voordoen bij de leverancier?

f. Is er een exitstrategie (overeengekomen), om het risico van leveranciersafhankelijkheid te beperken?

4. Monitoring en auditing (naleving)

Hoe beoordeelt de AED of de cybersecurity-eisen die zijn afgesproken ook worden nageleefd?

5. Opvolging

Als de AED merkt dat cybersecurity-afspraken niet worden nagekomen of niet meer passend zijn, hoe mitigeert ze dan deze risico's?