Bijlage 10 Casus DigiD-Beveiligingsassessment – Overheidsorganisatie X

1. Aanleiding

Overheidsorganisatie X beschikt over een DigiD-aansluiting en is verplicht jaarlijks een DigiD-beveiligingsassessment te laten uitvoeren conform de eisen van Logius. Voor het komende jaar wenst Overheidsorganisatie X een opdrachtnemer te contracteren die het volledige assessment uitvoert, inclusief alle verificaties, het onderzoek naar onderliggende processen en systemen, het opstellen van het auditrapport en het begeleiden van eventuele herstelacties.

De organisatie werkt sinds kort volgens een **multi-vendor strategie**, wat betekent dat verantwoordelijkheden voor beheer, beveiliging en dienstverlening verdeeld zijn over meerdere externe leveranciers én interne organisatieonderdelen.

---

2. Situatieschets

2.1 DigiD-aansluiting en keten

De DigiD-aansluiting van Overheidsorganisatie X maakt gebruik van meerdere schakels en leveranciers:

- **Serviceorganisatie [1]**
  Levert en beheert de **hybride cloudinfrastructuur**, inclusief hosting en platformcomponenten waarop onderdelen van de DigiD-keten draaien.

- **Serviceorganisatie [2]**
  Verzorgt de **connectiviteitsdiensten** en aanvullende **security-diensten**, zoals netwerkverbindingen, firewalls en eventuele security-componenten die ondersteunend zijn aan DigiD.

- **Serviceorganisatie [3]**
  Ondersteunt Overheidsorganisatie X bij **Security Operations**, waaronder:
  • SOC-monitoring
  • Incident response
  • Vulnerability management
  • Coördinatie bij security-meldingen

- **Identity broker**
  Wordt gebruikt voor de verificatie van de identiteit van de gebruiker. De broker levert jaarlijks een **Third Party Mededeling (TPM)** die onderdeel is van de DigiD-ketenverantwoordelijkheid.

- **Platform Y (Liferay)**
  Primaire beheertool voor webapplicaties. Formulieren die via de DigiD-koppeling ontsloten worden, worden hierbinnen beheerd.

- **Platform Z (Layer7 API Gateway)**
  Interface voor veilige toegang tot diverse omgevingen. Biedt overheidsstandaardkoppelingen zoals DigiD, eIDAS en eHerkenning.

---

3. Organisatiekenmerken

De opdrachtnemer moet rekening houden met de volgende kenmerken van Overheidsorganisatie X:

1. **Informatieaanlevering kost tijd.**
   Informatie die nodig is voor het assessment moet tijdig en duidelijk worden uitgevraagd. Afstemming en het vooraf duidelijk scheppen van verwachtingen zijn essentieel.

2. **Versnipperde verantwoordelijkheden.**
   Beveiligingsrichtlijnen en eigenaarschap van componenten liggen bij verschillende afdelingen en personen, wat impact heeft op planning en afstemming.

3. **Multi-vendor strategie.**
   Contactmomenten met externe partijen (serviceorganisaties) zijn noodzakelijk om het assessment volledig te kunnen uitvoeren. De organisatie maakt gebruik van het SIAM-model om de verschillende leveranciers aan te sturen.
