Periodieke evaluatie van IT leveranciers

1. Beschikt uw organisatie over een formeel vastgesteld informatiebeveiligingsbeleid?

   ◯ Ja

   ◯ Nee

2. Is het informatiebeveiligingsbeleid gebaseerd op een erkend normenkader (bijv. ISO/IEC 27001, NIST, BIO)?

   ◯ Ja

   ◯ Nee

3. Hoe vaak wordt dit beleid geëvalueerd en herzien?

4. Is er een functionaris verantwoordelijk voor informatiebeveiliging (bijv. CISO) binnen uw organisatie?

5. Voert u periodiek risicoanalyses uit m.b.t. informatiebeveiliging?

   ◯ Ja

   ◯ Nee

6. Is er een systeem voor het detecteren en monitoren van beveiligingsincidenten?

   ◯ Ja

   ◯ Nee

7. Hoe snel worden incidenten gemeld aan opdrachtgevers?

8. Heeft u de afgelopen 12 maanden een ernstig beveiligingsincident gehad? Zo ja, hoe is dit opgelost?

9. Waar bevinden zich de datacenters waarin onze gegevens worden opgeslagen?

10. Is er sprake van Cloud hosting? Zo ja, welke Cloud provider wordt er gebruikt?

11. Zijn recente auditrapporten of penetratietesten beschikbaar voor inzage?

12. Vindt er periodiek interne of externe audit plaats op securitymaatregelen?

13. Hoe is uw toegangsbeheer ingericht?

14. Beschikt u over een exit-strategie met gemeente Eindhoven?

15. Leg uit hoe u wijzigingsbeheer toepast, en Eindhoven op de hoogte stelt van wijzigingen?

16. In welke mate zijn uw test- en ontwikkelingssystemen van elkaar gescheiden?

17. Bedrijfsnaam van Leverancier *