a. **Zijn de genoemde maatregelen een minimale set of moeten wij aantonen dat wij volledige NIS2-compliance behalen?**

Voor kleine organisaties wordt proportionele compliance verwacht. Dit betekent:

- Aantoonbare basismaatregelen conform NIS2
- Focus op beleid, processen en praktische uitvoering

Aantonen gebeurt door:

- Vastgelegde procedures en beleidsdocumenten
- Overzicht van technische maatregelen
- Bewijs van bewustwording en incidentafhandeling

"Volledige compliance" betekent in de praktijk: aantoonbaar en passend bij omvang en risico's van de organisatie.

b. **Welke bewijslast verwacht OG om aan te tonen dat wij voldoen aan de NIS2-maatregelen (beleid, logbestanden, auditrapporten, trainingsregistraties, risicoregisters)?**

Gebruikelijk verwacht OG (selectief en risico gebaseerd):

- Beleid & procedures
  Informatiebeveiligingsbeleid
  Incidentmanagementprocedure
  Back-up- en continuïteitsafspraken
- Operationele bewijzen
  Overzicht gebruikte beveiligingsmaatregelen (MFA, antivirus, firewall)
  Patch- en updatebeleid (beschrijvend, geen detail-logs
- Awareness & training
  Trainingsregistratie, e-learning of toolbox-bijeenkomsten
  Bewijs van periodieke communicatie (bijv. phishing-awareness)
- Risicobeheer
  Eenvoudig risicoregister of risico-overzicht
  Leveranciersbeoordeling (hoog-over niveau)
- Incidentregistratie
  Basislog met datum, type incident en opvolging

Continue logbestanden of externe auditrapporten zijn niet vereist voor kleine opdrachtnemers, tenzij expliciet benoemd.

c. **Moet de onderbouwing vooraf bij inschrijving of na gunning worden aangeleverd?**

- Na gunning

Detailonderbouwing en documentatie
Eventuele aanvullende bewijslast op verzoek

d. **Moeten leveranciers en subcontractors van opdrachtnemer aantoonbaar voldoen aan dezelfde NIS2-maatregelen?**

Ja, voor zover relevant en proportioneel:

- Kritieke leveranciers (IT, cloud, hosting, beheer) moeten:
  Passende beveiligingsmaatregelen aantoonbaar hebben
  Contractueel vastgelegde beveiligingsafspraken kennen
- Niet-kritieke leveranciers:
  Basisbeoordeling volstaat

Volledige NIS2-compliance bij álle subcontractors is niet vereist.

e. Hoe monitort OG de naleving van NIS2: jaarlijkse audit, externe audits, steekproeven?

Gebruikelijke vormen van toezicht:

- Periodieke zelfverklaring of update
- Steekproeven of documentreview
- Gesprekken tijdens contract- of evaluatiemomenten
- Alleen bij verhoogd risico: externe audit

Jaarlijkse externe audits zijn niet verplicht voor kleine opdrachtnemers.

f. Is het niet voldoen aan NIS2 een grond voor sancties of ontbinding van de overeenkomst?

Incidentele onvolkomenheden leiden niet direct tot sancties.

Er geldt een getrapt model:

1. Signalering van tekortkoming
2. Hersteltermijn/ verbeterplan
3. Escalatie bij structurele of ernstige tekortkomingen

Ontbinding of sancties:

- Alleen bij ernstige nalatigheid
- Of bij beveiligingsincidenten met aantoonbare impact

g. **Is OG bereid een overgangsperiode te hanteren voor opdrachtnemers om volledige NIS2-compliance te realiseren?**

Ja, met een overgangsperiode van 12 maanden.

- Mits:
    - Er een concreet verbeterplan ligt
    - Basismaatregelen al zijn getroffen
    - Transparantie richting OG bestaat