BESTUURLIJKE NIS2-CHECKLIST

Deze handreiking ondersteunt bestuurders bij het invullen van hun rol onder de NIS2 richtlijn en de aankomende Cyberbeveiligingswet. De checklist is bedoeld als stuurinstrument aan de bestuurstafel en kan periodiek worden gebruikt.

1. BESTUURLIJKE VERANTWOORDELIJKHEID

- Valt onze organisatie onder de Cyberbeveligingswet en wat betekent dit concreet voor bestuur en toezicht?
- Is cybersecurity expliciet belegd als bestuurlijke verantwoordelijkheid (inclusief eigenaarschap van het cyberrisico)?
- Is helder wie (CISO/CIO) mandaat heeft voor uitvoering en escalatie?

2. INZICHT IN KRITIEKE ZORG- EN CYBERRISICO'S

- Hebben wij een actueel overzicht van de grootste cyberrisico's voor onze zorgprocessen (EPD, medicatie, planning)?
- Begrijpen wij welke kwetsbaarheden onze continuïteit van zorg direct kunnen raken?
- Hebben wij zicht op onze meest kritieke leveranciers en ketenafhankelijkheden?

3. STURING, GOVERNANCE EN INFORMATIEVOORZIENING

- Krijgt het bestuur periodiek begrijpelijke stuurinformatie (risico's, KPI's, incidenten)?
- Zijn escalatiecriteria voor cyberincitenten bestuurlijk vastgesteld?
- Worden cybersecurity en risico's structureel besproken in de bestuursagenda?
- Is vastgelegd dat de Raad van Bestuur de Raad van Toezicht periodiek en transparant informeert over cyberrisico's, voortgang en knelpunten?
- Is geborgd dat de Raad van Toezicht bij grote cyberrisico's of incidenten tijdig wordt betrokken bij escalatie, besluitvorming en verantwoording om effectief toezicht te kunnen houden?

4. MAATREGELEN EN AANTOONBARE WEERBAARHEID

- Zijn onze maatregelen aantoonbaar passend en in verhouding tot de risico's?
- Sluiten beleid en maatregelen aan op strategie en zorgcontinuïteit?
- Wordt effectief getoetst of maatregelen werken (audits, testen, evaluaties)?

5. INCIDENTEN, CRISIS EN CONTINUÏTEIT

- Is er een getest incident response plan met duidelijke rolverdeling voor bestuur?
- Weten wij wat onze rol is bij uitval van kritieke systemen of cyberincitenten?
- Is business continuity getest, inclusief scenario's met leveranciersuitval?

6. KETENAFHANKELIJKHEID EN EXTERNE WEERBAARHEID

- Zijn afspraken met kritieke leveranciers vastgelegd (inclusief security-eisen en continuïteit)?
- Hebben wij fallbackscenario's bij uitval van essenciële ICT-diensten?
- Is er samenwerking met toezichthouders en relevante ketenpartners georganiseerd?

7. BESTUURLIJKE CYBERCOMPETENTIE EN CULTUUR

- Heeft het bestuur voldoende kennis om cyberrisico's te kunnen beoordelen en bevragen?

- Is cybersecurity zichtbaar onderdeel van leiderschap en voorbeeldgedrag?
- Wordt bewustworing en training structureel geborgd in de organisatie?

BESTUURLIJK UITGANGSPUNT

Het bestuur is in control onder de NIS2-richtlijn wanneer het:

- De grootste cyberrisico's kent
- Actief stuurt op continuïteit van zorg
- Voorbereid is op verstoring en crisis

Deze checklist is opgesteld door Aon