Is je organisatie klaar voor NIS2 en ISO 27001?

Tien vragen om in tien minuten te zien waar je staat. Beantwoord elke vraag met ja, nee of weet ik niet.

		Ja	Nee	?
1	Weet je of je organisatie onder NIS2 en de Cyberbeveiligingswet valt? Dat hangt af van je sector en je omvang, meestal vanaf 50 medewerkers of € 10 miljoen jaaromzet. NIS2 art. 2 en 3, bijlage I en II	☐	☐	☐
2	Heeft de directie de beveiligingsmaatregelen goedgekeurd, en hebben de bestuurders een cybersecuritytraining gevolgd? NIS2 art. 20	☐	☐	☐
3	Is er een actuele risicoanalyse van je informatiesystemen, met een eigenaar per risico? NIS2 art. 21 lid 2(a) · ISO 27001 6.1.2	☐	☐	☐
4	Heeft de directie een informatiebeveiligingsbeleid vastgesteld dat medewerkers kennen? NIS2 art. 21 lid 2(a) · ISO 27001 5.2	☐	☐	☐
5	Kun je een ernstig incident binnen 24 uur vroegtijdig melden en binnen 72 uur een volledige melding doen? NIS2 art. 23 lid 4	☐	☐	☐
6	Heb je back-ups die je regelmatig test, en een plan om na een storing of aanval weer op te starten? NIS2 art. 21 lid 2(c)	☐	☐	☐
7	Heb je beveiligingseisen vastgelegd voor je belangrijkste IT-leveranciers, en controleer je die? NIS2 art. 21 lid 2(d)	☐	☐	☐
8	Gebruik je meerfactorauthenticatie (MFA) voor toegang op afstand en voor beheeraccounts? NIS2 art. 21 lid 2(j)	☐	☐	☐
9	Krijgen alle medewerkers minstens één keer per jaar een security-awarenesstraining? NIS2 art. 21 lid 2(g)	☐	☐	☐
10	Toets je periodiek of je maatregelen werken, met een interne audit en een directiebeoordeling? NIS2 art. 21 lid 2(f) · ISO 27001 9.2 en 9.3	☐	☐	☐

Drie keer of vaker 'nee' of '?'

Dan is een scan de snelste manier om je risico's en NIS2-plichten in kaart te brengen. Plan een gratis kennismaking van 30 minuten: **calendly.com/menno-verheij/30min**

Deze checklist is een hulpmiddel, geen juridisch advies. Bronnen: Richtlijn (EU) 2022/2555 (NIS2) en ISO/IEC 27001:2022. De Cyberbeveiligingswet is de Nederlandse invulling van NIS2.

Luméro · KvK 99056011 · lumero.nl · +31 6 11 80 48 10