NIS2 maatregel	ISO27001/ISO27002 Maatregel
Artikel 21.2 a	**ISO27001:**
Beleid omtrent risicomanagement en de beveiliging van informatiesystemen	5.2 Beleid
	6.1.2 Risicobeheersing van informatiebeveiliging
	6.1.3 Behandeling van informatiebeveiligingsrisico's
	8.2 Risicobeoordeling van informatiebeveiliging
	8.3 Informatiebeveiligingsrisico's behandelen
	ISO27002
	5.1 Beleidsregels voor informatiebeveiliging
Artikel 21.2 b	**ISO27002**
Incidentbehandeling- en management	5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten
	5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen
	5.26 Reageren op informatiebeveiligingsincidenten
	5.27 Leren van informatiebeveiligingsincidenten
	5.28 Verzamelen van bewijsmateriaal
	6.8 Melden van informatiebeveiligingsgebeurtenissen
Artikel 21.2 c	**ISO27002**
Bedrijfscontinuïteit	5.29 Informatiebeveiliging bij een verstoring
	5.30 ICT-gereedheid voor bedrijfscontinuïteit
	8.13 Back-up van informatie
	8.14 Redundantie van informatieverwerkende faciliteiten.
Artikel 21.2 d	**ISO27002**
Toeleveringsketenbeveiliging	5.19 Informatiebeveiliging in leveranciersrelaties
	5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten
	5.21 Beheren van informatiebeveiliging in de ICT-toeleveringsketen
	5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten
	5.23 Informatiebeveiliging voor het gebruik van clouddiensten
Artikel 21.2 e	**ISO27002**
	5.37 Gedocumenteerde bedieningsprocedures
	8.8 Beheer van technische kwetsbaarheden

Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen	8.9 Configuratiebeheer
	8.20 Beveiliging netwerkcomponenten
	8.21 Beveiliging van netwerkdiensten
Artikel 21.2 f	**ISO27001**
Beleid en procedures omtrent het aantonen van de effectiviteit van maatregelen tegen informatieveiligheidsrisico's	9.1 Monitoren, meten, analyseren en evalueren
	9.2 interen Audit
	9.3 Management review
	ISO27002
	5.35 Onafhankelijke beoordeling van informatiebeveiliging
Artikel 21.2 g	**ISO27001**
Basis cyberhygiëne en trainingen op het gebied van informatiebeveiliging	7.3 Bewustzijn
	7.4 Communicatie
	ISO27002
	6.3 Bewustwording van, opleiding en training in informatiebeveiliging.
Artikel 21.2 h	**ISO27002**
Beleid en procedures over het gebruik van cryptografie en encryptie	8.24 Gebruik van cryptografie
Artikel 21.2 i	**ISO27002**
Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa	6.1 Screening
	6.2 Arbeidsovereenkomst
	6.4 Disciplinaire procedure
	6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband
	6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomst
	5.15 Toegangsbeveiliging
	5.16 Identiteitsbeheer
	5.17 Authenticatie-informatie
	5.18 Toegangsrechten
	5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen
	5.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen
Artikel 21.2 j	**ISO27002**
	5.16 Identiteitsbeheer

Het gebruik van multifactor-authenticatie en beveiligde (nood)communicatie	5.17 Authenticatie-informatie
	5.14 Overdragen van informatie
Artikel 21.3	**ISO27002**
Procedures voor beveiligd ontwikkelen	8.25 Beveiligen tijdens de ontwikkelcyclus
	8.26 toepassingsbeveiligingseisen
	8.27 Veilige systeemarchitectuur en technische uitgangspunten
	8.28 Veilig coderen
	8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie
	8.30 Uitbestede systeemontwikkeling
	8.31 Scheiding van ontwikkel-, test en productieomgevingen
	8.32 Wijzigingsbeheer
	8.33 Testgegevens
Artikel 21.4	**ISO27001**
Passende en proportionele corrigerende maatregelen	10.2 Afwijkingen en corrigerende maatregelen

NIS2 maatregel	Nieuwe maatregelen t.o.v. ISO27001/ISO27002
Registratieplicht	
	Bepaal of de organisatie essentieel of belangrijk is
	Registreer de organisatie bij het NCSC
Governance	
	Alle bestuursleden moeten periodiek trainingen over informatieveiligheid volgen
	Alle bestuursleden moeten aantoonbaar kennis en ervaring hebben op het gebied van informatieveiligheid
	Het bestuur moet actief toezien op de informatieveiligheid in de organisatie (impliciet onderdeel in de ISO27001)
Meldplicht	
	Richt een proces in voor medewerkers om informatieveiligheidsincidenten te melden (zowel cyberincidenten als datalekken)
	Informeer medewerkers binnen de organisatie over het proces om meldingen te maken
	Richt een proces in om meldingen te maken bij de toezichthouder (en de CSIRT)
CSIRT	
	Meld de organisatie aan bij de aangewezen CSIRT voor de sector
	Regel een procedure in om relevante informatie vanuit het CSIRT te internaliseren in de organisatie
	Regel een procedure in om relevante informatie met het CSIRT te delen