



3	THEMA	EISEN Cbw (NIS2)	ARTIKEL	ISO	MAATREGEL	Status
A	GOVERNANCE EN BELEID					
A1	Goedkeuren maatregelen door bestuur	Bestuursorganen van essentiële en belangrijke entiteiten dienen de genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goed te keuren.	Artikel 20 lid 1	5.1	Beleidsregels voor informatiebeveiliging	
				5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	
				5.3	Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie	
				7.2	Competentie	
A2	Toezien op uitvoering en beoordeling maatregelen door bestuur	Bestuursorganen van essentiële en belangrijke entiteiten dienen toe te zien op de genomen maatregelen voor het beheer van cyberbeveiligingsrisico's. Indien niet (volledig) kan worden voldaan aan de implementatie van effectieve maatregelen, neemt de entiteit de noodzakelijke, passende en evenredige corrigerende maatregelen. Restrisico's worden in ogenschouw genomen en te allen tijde zichtbaar geaccepteerd.	Artikel 20 lid 1 Artikel 20 lid 4	9.1	Monitoren, meten, analyseren en evalueren	
				9.2	Interne audit	
				5.35	Onafhankelijke beoordeling van informatiebeveiliging	
				5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	
				9.3	Management review	
B	OPLEIDING EN BEWUSTWORDING					
B1	Volgen van opleiding/training voor bestuur	Leden van de bestuursorganen van essentiële en belangrijke entiteiten dienen een opleiding te volgen zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheer praktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.	Artikel 20 lid 2	6.3	Bewustwording van, opleiding en training in informatiebeveiliging	
B2	Volgen van opleiding/training door medewerkers	Leden van de bestuursorganen van essentiële en belangrijke entiteiten bieden regelmatig een opleiding aan hun werknemers aan, zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheer praktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.	Artikel 20 lid 2	6.3	Bewustwording van, opleiding en training in informatiebeveiliging	
B3	Vergroten security awareness binnen de organisatie	De entiteit heeft basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging ingericht ten aanzien van opleidingen voor hun personeel organiseren en het bewustzijn van cyberdreigingen zoals phishing of social engineering technieken.	Artikel 21 lid 2g-10a	6.3	Bewustwording van, opleiding en training in informatiebeveiliging	
				6.8	Melden van informatiebeveiligingsgebeurtenissen	
C	RISICOMANAGEMENT					
C1	Beleid en procedure risicomanagement	De entiteit heeft beleid en procedure opgesteld inzake risicoanalyse en beveiliging van informatiesystemen. Maatregelen voor het beheer van cyberbeveiligingsrisico's moeten gebaseerd zijn op een benadering die alle gevaren omvat en tot doel heeft	Artikel 21 lid 2a Overweging 77 Overweging 79 Overweging 85 Overweging 50	6.1.2	Risicobeoordeling van informatiebeveiliging	



3	THEMA	EISEN Cbw (NIS2)	ARTIKEL	ISO	MAATREGEL	Status
		<p>netwerk- en informatiesystemen en de fysieke omgeving van die systemen. Bij het risicomanagementproces is onder meer expliciet aandacht voor het aanpakken van risico's die voortvloeien uit de toeleveringsketen van een entiteit en uit haar relatie met haar leveranciers, en risico's die ontstaan door het toenemende aantal verbonden apparaten waarvan bij cyberaanvallen steeds vaker gebruik wordt gemaakt. Er moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordelingen en de uitvoering van op de risico's afgestemde maatregelen voor het beheer van cyberbeveiligingsrisico's behelst.</p>				
C2	Uitvoeren van een risicobeoordeling	<p>De entiteit heeft beleid en procedure opgesteld inzake risicoanalyse en beveiliging van informatiesystemen. Maatregelen voor het beheer van cyberbeveiligingsrisico's moeten gebaseerd zijn op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen. Bij het risicomanagementproces is onder meer expliciet aandacht voor het aanpakken van risico's die voortvloeien uit de toeleveringsketen van een entiteit en uit haar relatie met haar leveranciers, en risico's die ontstaan door het toenemende aantal verbonden apparaten waarvan bij cyberaanvallen steeds vaker gebruik wordt gemaakt. Er moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordelingen en de uitvoering van op de risico's afgestemde maatregelen voor het beheer van cyberbeveiligingsrisico's behelst.</p>	<p>Artikel 21 lid 2a Overweging 77 Overweging 79 Overweging 85 Overweging 50</p>	8.2	Risicobeoordeling van informatiebeveiliging	
C3	Reageren op risico's met maatregelen	<p>Er dienen passende en evenredige technische, operationele en organisatorische maatregelen te zijn genomen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken. Hierbij dient rekening te worden gehouden met het volgende:</p> <ul style="list-style-type: none"> ▪ De stand van de techniek; ▪ De desbetreffende Europese en internationale normen; ▪ De uitvoeringskosten; ▪ De mate waarin de entiteit aan risico's is blootgesteld ten aanzien van alle gevaren voor netwerk- en informatiesystemen en de fysieke 	<p>Artikel 21 lid 1 en 2 Overweging 78 Overweging 79</p>	6.1.3 8.3	Behandeling van informatiebeveiligingsrisico's Informatiebeveiligingsrisico's behandelen	



3	THEMA	EISEN Cbw (NIS2)	ARTIKEL	ISO	MAATREGEL	Status
		<p>omgeving van die systemen tegen incidenten te beschermen;</p> <ul style="list-style-type: none"> De mate waarin de entiteit aan risico's is blootgesteld ten aanzien van alle gevaren van de fysieke omgeving van netwerk- en informatiesystemen; De mate waarin de entiteit afhankelijk is van netwerk- en informatiesystemen; De omvang van de entiteit; De mate om incidenten te identificeren, te voorkomen, op te sporen, erop te reageren en ervan te herstellen en om de gevolgen ervan te beperken; De kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen. 				
C4	Beoordelen effectiviteit maatregelen en accepteren restrisico	De entiteit heeft beleid en procedures ingericht om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen. Indien niet (volledig) kan worden voldaan aan de implementatie van effectieve maatregelen, neemt de entiteit de noodzakelijke, passende en evenredige corrigerende maatregelen.	Artikel 21 lid 2f Artikel 20 lid 4	9.1 9.2 5.35 5.36	Monitoren, meten, analyseren en evalueren Interne Audit Onafhankelijke beoordeling van informatiebeveiliging Naleving van beleid, regels en normen voor informatiebeveiliging	
D1	INCIDENT EN RESPONSE					
D1	Incident en response	De entiteit heeft maatregelen ingericht voor incidentbehandeling.	Artikel 21 lid 2b	5.24 6.8 5.25 5.26 5.27 5.28 8.16	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten Melden van informatiebeveiligingsgebeurtenissen (intern in de organisatie) Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen Reageren op informatiebeveiligingsincidenten Leren van informatiebeveiligingsincidenten Verzamelen van bewijsmateriaal Monitoren van activiteiten	
D2	BEDRIJFSCONTINUÏTEIT					
D2	Bedrijfscontinuïteit	De entiteit heeft maatregelen ingericht ten aanzien van de bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningsplannen, en crisisbeheer.	Artikel 21 lid 2c Artikel 21 lid 2g-5	5.30 8.13 8.14 Nvt	ICT-gereedheid voor bedrijfscontinuïteit Back-up van informatie Redundantie van informatieverwerkende faciliteiten Crisisbeheer	
D3	MAATREGELN KRITIEKE TOELEVERINGSKETTEN EN LEVERANCIERS					
D3			Artikel 21 lid 2d	5.19	Informatiebeveiliging in leveranciersrelaties	



3	THEMA	EISEN Cbw (NIS2)	ARTIKEL	ISO	MAATREGEL	Status
	Maatregelen kritieke toeleveringsketen en leveranciers	De entiteit heeft maatregelen ingericht rondom de beveiliging van de kritieke toeleveringsketen, met inbegrip van beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners. Hierbij is rekening gehouden met: <ul style="list-style-type: none"> De uitgevoerde beveiligingsrisicobeoordelingen; De specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener; De algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners; Veilige ontwikkelingsprocedures bij leveranciers. 	Artikel lid 3 Overweging 75	5.20 5.21 5.22 5.23 8.30	Adresseren van informatiebeveiliging in leveranciersovereenkomsten Beheren van informatiebeveiliging in de ICT-keten Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten Informatiebeveiliging voor het gebruik van clouddiensten Uitbestede systeemontwikkeling entiteiten	
D4	BEVEILIGING VAN NETWERKEN EN INFORMATIESYSTEMEN					
D4	Beveiliging van netwerk- en informatiesystemen	De entiteit heeft maatregelen ingericht rondom de beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen (incl. netwerksegmentatie).	Artikel 21 lid 2e Artikel 21 lid 2g-8 Overweging 58	5.20 8.20 8.21 8.22 8.30	Adresseren van informatiebeveiliging in leveranciersovereenkomsten Beveiliging netwerkcomponenten Beveiliging van netwerkdiensten Netwerksegmentatie Uitbestede systeemontwikkeling entiteiten	
D5	KWETSBAARHEDEN MANAGEMENT (INCL. PATCH MANAGEMENT EN PENTESTING)					
D5	Kwetsbaarhedenmanagement (incl. patch management en pentesting).	De entiteit heeft maatregelen ingericht de respons op en bekendmaking van kwetsbaarheden.	Artikel 21 lid 2e Overweging 58	8.7 5.7 8.8	Bescherming tegen malware Informatie en analyses over dreigingen Beheer van technische kwetsbaarheden	
D6	SOFTWARE EN HARDWARE-UPDATES					
D6	Software en hardware updates	De entiteit heeft basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging ingericht ten aanzien van software- en hardware-updates.	Artikel 21 lid 2g-1	8.1 8.32	Installeren van software op operationele systemen Wijzigingen-beheer	
D7	BEHEER VAN NIEUWE INSTALLATIES					
D7	Beheer van nieuwe installaties	De entiteit heeft basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging ingericht ten aanzien van het beheer van nieuwe installaties en de configuratie van apparaten.	Artikel 21 lid 2g-3 Artikel 21 lid 2g-7	8.9 8.19 8.32	Configuratiebeheer Installeren van software op operationele systemen Wijzigingen-beheer	
D8	WACHTWOORDBEHEER EN AUTHENTICATIE					
D8	Wachtwoordenbeheer en authenticatie	De entiteit heeft basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging ingericht ten aanzien van wijzigingen van wachtwoorden. De entiteit heeft maatregelen ingericht, wanneer gepast, voor het gebruik van multi-factor-authenticatie- of continue-authenticatieoplossingen,	Artikel 21 lid 2g-2	5.17 8.5	Beheren authenticatie-informatie Beveiligde authenticatie	



3	THEMA	EISEN Cbw (NIS2)	ARTIKEL	ISO	MAATREGEL	Status
		beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.				
D9	BEPERKING VAN TOEGANGSRECHTEN OP BEHEERNIVEAU					
D9	Beperking van toegangssaccounts op beheerniveau	De entiteit heeft basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging ingericht ten aanzien van de beperking van toegangssaccounts op beheerniveau	Artikel 21 lid 2g-4	8.2 8.3	Speciale toegangsrechten Beperking toegang tot informatie	
D10	IDENTITEITS- EN TOEGANGSBEHEER					
D10	Identiteits- en toegangsbeheer	De entiteit heeft basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging ingericht ten aanzien van toegangsbeleid, identiteits- en toegangsbeheer en gebruikersbewustzijn.	Artikel 21 lid 2g-9 Artikel 21 lid 2i-2	5.15 5.16 5.17 5.18	Toegangsbeveiliging Identiteitsbeheer Beheren van authenticatie-informatie Toegangsrechten	
D11	CRYPTOGRAFIE EN ENCRYPTIE					
D11	Cryptografie en encryptie	De entiteit heeft beleid en procedures inzake het gebruik van cryptografie.	Artikel 21 lid 2h Overweging 98	8.24	Gebruik van cryptografie	
D12	VEILIG PERSONEEL					
D12	Veilig personeel	De entiteit heeft maatregelen ingericht ten aanzien van beveiligingsaspecten voor personeel.	Artikel 21 lid 2i-1	6.1 6.2 6.4 6.5 6.6 5.10	Screening Arbeidsovereenkomst Disciplinaire procedure Verantwoordelijkheden na beëindiging of wijziging van het dienstverband Vertrouwelijkheids- of geheimhoudingsovereenkomsten Aanvaard gebruik van informatie en andere gerelateerde bedrijfsmiddelen	
D13	ASSET MANAGEMENT					
D13	Asset management	De entiteit heeft maatregelen ingericht ten aanzien van het beheer van activa.	Artikel 21 lid 2i-3	5.9 5.10 5.11	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen Aanvaard gebruik van informatie en andere gerelateerde bedrijfsmiddelen Retourneren van bedrijfsmiddelen	
E	MELDP LICHT					
E1	Afgeven waarschuwing binnen 24 uur bij CSIRT	Entiteiten melden elk significant incident dat aanzienlijke gevolgen heeft bij het CSIRT of, indien van toepassing, zijn bevoegde autoriteit. Een incident wordt als significant beschouwd als het: <ul style="list-style-type: none"> Een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; 	Artikel 23 lid 1 en 4 Overweging 102	6.8 5.14	Melden van informatiebeveiligingsgebeurtenissen (extern aan autoriteiten en belanghebbenden) Overdragen van informatie	



3	THEMA	EISEN Cbw (NIS2)	ARTIKEL	ISO	MAATREGEL	Status
		<ul style="list-style-type: none"> Andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. <p>Entiteiten melden significante incidenten binnen 24 uur nadat zij kennis hebben gekregen van het significante incident, waarbij wordt aangegeven of het incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben.</p>				
E2	Indienen verslaglegging binnen 72 uur bij CSIRT	<p>Entiteiten melden significante incidenten binnen 72 uur nadat zij kennis hebben gekregen van het significante incident met de volgende informatie:</p> <ul style="list-style-type: none"> Omschrijving incident; Update van het incident; Initiële beoordeling incident (ernst en de gevolgen); Indicatoren voor aantasting. 	<p>Artikel 23 lid 1 en 4</p> <p>Overweging 102</p>	<p>6.8</p> <p>5.14</p>	<p>Melden van informatiebeveiligingsgebeurtenissen (extern aan autoriteiten en belanghebbenden)</p> <p>Overdragen van informatie</p>	
E3	Indienen eindrapport binnen één maand bij CSIRT	<p>Entiteiten dienen uiterlijk één maand na de indiening van de incidentmelding, een eindverslag in waarin het volgende is opgenomen:</p> <ul style="list-style-type: none"> Een gedetailleerde beschrijving van het incident; Definitieve beoordeling incident (incl. ernst en de gevolgen); Het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid; Toegepaste en lopende risicobeperkende maatregelen; Grensoverschrijdende gevolgen van het incident (indien van toepassing). <p>Indien het incident nog aan de gang is op het moment dat het eindverslag wordt ingediend, dienen de entiteiten een voortgangsverslag in en binnen één maand nadat zij het incident hebben afgehandeld, het definitieve eindverslag.</p>	<p>Artikel 23 lid 1 en 4</p> <p>Overweging 102</p>	<p>6.8</p> <p>5.14</p>	<p>Melden van informatiebeveiligingsgebeurtenissen (extern aan autoriteiten en belanghebbenden)</p> <p>Overdragen van informatie</p>	
E4	Informeren belanghebbenden bij incident	<p>Entiteiten stellen de ontvangers van hun diensten in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten. Er wordt aangegeven welke maatregelen zijn genomen en welke maatregelen ontvangers kunnen nemen in reactie op die dreiging.</p>	<p>Artikel 23 lid 1 en 2</p> <p>Overweging 103</p>	<p>6.8</p> <p>5.14</p>	<p>Melden van informatiebeveiligingsgebeurtenissen (extern aan autoriteiten en belanghebbenden)</p> <p>Overdragen van informatie</p>	