M&I/Partners/

adviseurs voor management en informatie

MAPPING: CBW NAAR ISO 27001/27002 EN BIO 2

Deze mapping laat de relatie zien tussen de maatregelen uit de Cbw (Artikel 21) en de corresponderende beheersmaatregelen uit ISO 27001/27002 en de specifieke overheidsmaatregelen uit de BIO 2 (versie 1.3):

KERNMAATREGELEN ARTIKEL 21.2

Cbw Maatregel	ISO 27001/27002 Beheersmaatregel	BIO 2 Overheidsmaatregel	Focus / Toelichting
21.2 a Risicomanagement & Beveiliging	ISO 27001: 5.2, 6.1.2, 6.1.3, 8.2, 8.3 ISO 27002: 5.1	**5.01.01**	Vaststellen van informatiebeveiligingsbeleid en risicomanagementmethodiek.
21.2 b Incidentbehandeling & Management	ISO 27002: 5.24, 5.25, 5.26, 5.27, 5.28, 6.8	**5.24.02, 5.24.04, 5.26.02, 5.27.01**	Inrichten van meldprocedures, analyse van oorzaken en rapportage.
21.2 c Bedrijfscontinuïteit	ISO 27002: 5.29, 5.30, 8.13, 8.14	**5.30.01**	Jaarlijks testen van continuïteitsplannen en focus op primaire bedrijfsvoering.
21.2 d Toeleveringsketenbeveiliging	ISO 27002: 5.19, 5.20, 5.21, 5.22, 5.23	**5.20.01 - 5.20.06, 5.21.02 - 5.21.05**	Beheer van leveranciersrelaties, inkoopvoorwaarden en ketentransparantie.
21.2 e Systeembeveiliging (Ontwikkeling & Onderhoud)	ISO 27002: 5.37, 8.8	**8.08.01 - 8.08.05**	Beheer van technische kwetsbaarheden en penetratietesten van internetfacing systemen.

Cbw Maatregel	ISO 27001/27002 Beheersmaatregel	BIO 2 Overheidsmaatregel	Focus / Toelichting
21.2 f Effectiviteit van maatregelen	ISO 27001: 9.1, 9.2, 9.3 ISO 27002: 5.35	**5.36.01**	Monitoring, interne audits en de jaarlijkse 'In Control Verklaring' (ICV).
21.2 g Cyberhygiëne & Training	ISO 27001: 7.3, 7.4 ISO 27002: 6.3	**5.04.01, 6.03.01 - 6.03.04**	Bewustwordingsprogramma's en trainingen voor medewerkers en bestuurders.
21.2 h Cryptografie & Encryptie	ISO 27002: 8.24	**8.21.01 - 8.24.05**	Beleid voor cryptografie, sleutelbeheer en gebruik van goedgekeurde middelen.
21.2 i Personeel, Toegang & Activa	ISO 27002: 6.1, 6.2, 6.4, 6.5, 6.6, 5.15, 5.16, 5.17, 5.18, 5.9, 5.10	**5.15.01, 5.16.01, 5.17.01 - 5.18.02, 5.09.01**	Screening, toegangsbeheer (MFA), identiteitsbeheer en inventarisatie van bedrijfsmiddelen.
21.2 j Configuratiebeheer & Netwerkbeveiliging	ISO 27002: 8.9, 8.20, 8.21	**7.02.01, 8.20.01 - 8.21.03**	Beveiliging van netwerkcomponenten en monitoring van dataverkeer.

NIEUWE EISEN

Deze eisen vallen buiten de standaard ISO-maatregelen maar zijn essentieel in de BIO 2 / Cbw:

Cbw Eis	BIO 2 Referentie	Toelichting
Bestuursopleiding (artikel 24)	**5.04.01 / Hoofdstuk 12**	Verplichting voor bestuurders om kennis en vaardigheden te hebben om op risico's te sturen
Bestuursverantwoordelijkheid (artikel 24)	**Hoofdstuk 11.1 / 12**	Expliciete verantwoordelijkheid voor het treffen van passende en evenredige maat-regelen
Meldplicht incidenten (artikel 25)	**5.24.07**	Strikte termijnen voor melding aan toe-zichthouder (RDI) en CSIRT
Toezicht (artikel 15)	**Hoofdstuk 10 / 11.1**	De RDI is de aangewezen toezichthouder voor de sector Overheid
Registratieplicht (artikel 44)	**Hoofdstuk 11.1**	Registratie van de organisatie als essenti-eel of belangrijk bij het NCSC