RDW

ISMS VvT

Verklaring van Toepasselijkheid

Inhoudsopgave

1. Documentbeheer 3
1.1 Herziening en goedkeuring van het management 3
1.2 Wijzigingshistorie 3
1.3 Reviewers 3
1.4 Distributie 3
2. Verklaring van toepasselijkheid 4
2.1 Inleiding 4
2.2 Gerelateerde documenten 4
2.3 Geselecteerde beheersdoelstellingen en -maatregelen 4
2.3.1 ISO 27002 4
2.3.2 Motivatie 4
2.3.3 Locatie 5
2.3.4 Operationele capaciteiten 5
2.3.5 Selectie 5
2.4 Overzicht van toepasselijkheid (‘VvT tabel’) 6

1. Documentbeheer

1.1 Herziening en goedkeuring van het management

	Versie	Datum	Paraaf
RDW directeur Bedrijfsvoering	4.0	11-2024	5.1, 2, e

1.2 Wijzigingshistorie

Datum	Auteur	Versie	Wijziging
03-10-2012	EV	1.9	Aanpassing van de versies van ISMS voorgangers.
12-10-2012	EV	2.0	Gefinaliseerd document; geen wijzigingen.
09-06-2014	EV	2.1	- Sectie 2.3.5 en laatste kolom in tabel in 'VvT tabel' (Sectie 2.4) verwijderd omdat deze niet noodzakelijk is en verwarring geeft. - In 'VvT tabel' consequent baseline genoemd als gebruik hiervan was aangegeven ('JB'). - Baseline nummering toegevoegd in de tabel in Sectie 2.2
30-10-2015	GM	2.9	Aanpassing aan ISO 27002:2015
14-12-2015	GM	3.0	Review DSO's verwerkt
15-03-2016	GM	3.1	Toelichting uitsluiten beveiligen bekabeling
15-12-2020	GM	3.2	ISMS opgenomen in de baseline omdat dit standaard ingericht is en geen extra vragen in de RBB vereist. Ook 18.1.3 toegevoegd.
12-10-2021	EW	3.2	Geen wijzigingen
06-01-2022	EW	3.3	11.2.3 Beveiliging van bekabeling niet meer uitgesloten
10-08-2024	JV	4.0	Aangepast naar ISO 27002:2022

1.3 Reviewers

Versie	Naam	Functie
1.9	GM	CSO / DSO D&S
1.9	JW	DSO R&I
1.9	JvdH	DSO VT
1.9	EA	DSO ICT Bedrijf
2.1	DSO Overleg (12 juni 2014)	
2.9	DSO overleg en 5.1, 2, e	
3.0	JW, EW, EA, GM	
3.1	DSO overleg	
3.2	DSO overleg	
3.3	DSO overleg	
4.0	DSO overleg	

1.4 Distributie

De laatste versie staat op het intranet, op de security & privacy pagina.

2. Verklaring van toepasselijkheid

2.1 Inleiding

Deze verklaring beschrijft de doelstellingen van het managementsysteem voor Informatiebeveiliging van de RDW en de geselecteerde beheersmaatregelen van de ISO/IEC 27002:2022 “Informatiebeveiliging, cybersecurity en bescherming van de privacy – Beheersmaatregelen voor informatiebeveiliging”.

De RDW maakt gebruik van een managementsysteem voor informatiebeveiliging om de vertrouwelijkheid, integriteit en beschikbaarheid te kunnen waarborgen voor de informatie toevertrouwd door klanten en om de continuïteit van haar dienstverlening te kunnen waarborgen in overeenstemming met gemaakte afspraken.

De dienstverlening wordt verleend conform relevante beheerhandboeken, ISMS Beleid, baselines en RBB procedures. Deze zijn opgesteld op basis van de ISO/IEC 27002:2022 standaard.

Een overzicht van de toepasselijkheid van de beheersmaatregelen volgt in deze verklaring. Dit document toont de relatie tussen de ISO/IEC 27002:2022 standaard en relevante documenten van de RDW. Hierin wordt verwezen naar de Generieke Baseline documenten, waar de maatregelen zijn uitgewerkt. Verder kunnen er op basis van de RBBs ook extra maatregelen genomen worden om aan de hieronder weergegeven doelstellingen te voldoen, maar deze zal hier niet worden opgenomen.

2.2 Gerelateerde documenten

Binnen dit document wordt gerefereerd naar documentatie rond informatiebeveiliging. Daarbij worden de referenties gebruikt aangegeven in de eerste kolom van onderstaande tabel.

REF	Documentnaam
Information Security Management System	
[ISMS]	Information Security Management System
Tactische documentatie	
[Organisatie]	Hoofdstuk 5, Organisatorische beheersmaatregelen
[Mens]	Hoofdstuk 6, Mensgerichte beheersmaatregelen
[Fysiek]	Hoofdstuk 7, Fysieke beheersmaatregelen
[Technologie]	Hoofdstuk 8, Technologische beheersmaatregelen
Uitwijk documentatie	
[UITW]	Uitwijkplannen: Scenario A, Scenario B en Scenario Politie uitwijk. Het betreft hier beheersboeken 51, 52 en 56 van de monitoring afdeling binnen het cluster continuïteit.

2.3 Geselecteerde beheersdoelstellingen en -maatregelen

In de tabel in Sectie 2.4 (hierna: *VvT tabel)* is aangegeven welke beheersdoelstellingen en -maatregelen zijn geadopteerd binnen het ISMS. Deze tabel bestaat uit 5 kolommen die wij onderstaand puntsgewijs bespreken.

2.3.1 *ISO 27002*

De eerste kolom is een duiding van de ISO 27002:2022 beheersdoelstellingen en –maatregelen. De beheersdoelstellingen betreft de grijs gearceerde rijen en de beheersmaatregelen betreft de ongearceerde rijen.

2.3.2 *Motivatie*

De tweede kolom in de VvT tabel genaamde ‘Motivatie’ vormt de invulling van de volgende twee ISO 27001 6.1.3 punt d: “..een verklaring van toepasselijkheid op te stellen die de benodigde beheersmaatregelen bevat (..), een rechtvaardiging voor het opnemen ervan, de informatie of ze zijn geïmplementeerd of niet..”

Hiertoe hebben wij in onderstaand overzicht de belangrijkste bedreigingen geïnventariseerd van de RDW op basis van interviews met het management en de ervaring van de Corporate Informatie Security Officer.

Ref.	Bedreiging omschrijving
[Onv-Man-Stu]	Onvoldoende management sturing. Management is niet betrokken bij informatiebeveiliging of steunt de informatiebeveiliging onvoldoende. Daarnaast wordt er onvoldoende richting aangegeven en onvoldoende doelen gesteld.

[Onv-All-Verant]	Onvoldoende allocatie verantwoordelijkheden. Het is onduidelijke wie voor welke taak verantwoordelijk is. Hierdoor worden mogelijk essentiële taken niet of in onvoldoende mate uitgevoerd.
[Onv-Naleving]	Het beveiligingsbeleid wordt niet door alle betrokken partijen in voldoende mate nageleefd.
[Non-Compliance]	De RDW handelt in strijd met geldende wet- en regelgeving.
[Contractbreuk]	Niet voldoen aan afgesloten contracten (bijvoorbeeld SLA).
[Hacking]	Hackers, die tot doel hebben de dienstverlening te verstoren dan wel ongeautoriseerde toegang te verkrijgen tot gegevens.
[Sabotage]	Moedwillige sabotage van apparatuur, bijvoorbeeld door groeperingen met terroristische motieven.
[Spionage]	Kopiëren van gevoelige gegevens door een commerciële concurrent of een buitenlandse overheid.
[Diefstal]	Diefstal van gegevens of apparatuur.
[Verlies-Gegevens]	Gegevens zijn verloren of niet tijdig beschikbaar.
[Verlies-Dienst]	Dienstverlening is niet beschikbaar of voldoet niet aan gestelde eisen.
[Ong-Toegang]	Ongeautoriseerde toegang tot gegevens, programmatuur, diensten of locaties.
[Ong-Wijziging]	Ongeautoriseerde wijziging van gegevens, programmatuur, diensten of locaties.
[Onv-Integriteit]	Medewerkers zijn onvoldoende integer, waardoor zij kwetsbaar zijn voor chantage en fraude.
[Fouten]	Onopzettelijke fouten in de ontwikkeling, gebruik of beheer van gegevens, programmatuur, diensten of apparatuur.
[Calamiteit]	Externe calamiteiten zoals stroomuitval, brand, overstroming, aardbeving, etc.

Per geselecteerde maatregel in de VvT Motivatie tabel hebben wij aangegeven de manifestatie van welke bedreigingen beperkt. In veel gevallen zal hier een ‘m op n’ relatie bestaan: een beheersmaatregel zal de manifestatie van meerdere bedreigingen beïnvloeden en vice versa. Dit overzicht stelt het management in staat vast te stellen welke bedreigingen manifest(er) kunnen worden bij het de-selecteren van een beheersmaatregel. Tot slot, in het geval dat een maatregel niet wordt geselecteerd, wordt in de VvT motivatie kolom gemotiveerd waarom dit niet het geval is.

2.3.3 *Locatie*

De Locatie kolom geeft aan waar de relevante tactische informatie kan worden gevonden (zie Sectie 2.2.).

2.3.4 *Operationele capaciteiten*

De kolom Operationele capaciteiten is overgenomen uit de ISO 27002:2022 norm en is een attribuut om beheersmaatregelen te bekijken vanuit het perspectief van beroepsbeoefenaren op informatiebeveiligingscapaciteiten.

2.3.5 *Selectie*

Zoals uitgebreid beschreven in het ISMS handboek, maakt de RDW gebruik van de zogenaamde ‘*combined approach*’ voor informatiebeveiliging. Hierbij wordt:

- een selectie van beheersmaatregelen als baseline van toepassing gesteld voor alle toepasselijke objecten (informatiesystemen, mensen etc.)
- middels een Business Impact Scan (BIS) vastgesteld of een informatiesysteem essentieel is voor de RDW of niet.
- Voor essentiële informatiesystemen wordt een Risicobeoordeling en –behandeling (RBB) toegepast waarbij wordt vastgesteld of beheersmaatregelen additioneel aan de baseline noodzakelijk is.

In de VvT Tabel staat in de Selectie kolom:

- een ‘J’ als de beheersdoelstelling of –maatregel feitelijk is geselecteerd en een ‘N’ als dat niet het geval is (mogelijk dat feitelijke selectie op een later moment wel plaatsvindt),
- een ‘B’ als de beheersmaatregel onderdeel van de baseline is en geen ‘B’ als dat niet geval is.

Uit de VvT tabel blijkt dat de RDW alle ISO 27002 beheersdoelstellingen heeft geselecteerd.

2.4 Overzicht van toepasselijkheid (‘VvT tabel’)

ISO 27002:2022	Motivatie	Locatie/Toelichting	Operationele capaciteiten	Selectie (N, J, B)
5 Organisatorische beheersmaatregelen				
5.1 Beleidsregels voor informatiebeveiliging	[Onv-Man-Stu], [Onv-Naleving]	[ISMS]	#Governance	JB
5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging	[Onv-Man-Stu]	[ISMS]	#Governance	JB
5.3 Functiescheiding	[Fouten], [Onv-Integriteit] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Organisatie]	#Governance #Identiteits-_en_toegangsbeheer	JB
5.4 Managementverantwoordelijkheden	[Onv-All-Verant]	[ISMS], [Organisatie]	#Governance	JB
5.5 Contact met overheidsinstanties	[Hacking], [Sabotage]	[Organisatie]	#Governance	JB
5.6 Contact met speciale belangengroepen	[Hacking], [Sabotage]	[Organisatie]	#Governance	JB
5.7 Informatie en analyses over dreigingen	[Hacking], [Spionage]	[Organisatie]	#Beheer_van_dreigingen_en_kwetsbaarheden	JB
5.8 Informatiebeveiliging in projectmanagement	[Hacking], [Diefstal], [Verlies-Gegevens], [Verlies-Dienst], [Onv-Man-Stu], [Onv-All-Verant]	[Organisatie]	#Governance	JB
5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	[Diefstal], [Ong-Toegang], [Onv-All-Verant]	[Organisatie]	#Beheer_van_bedrijfsmiddelen	JB
5.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	[Diefstal], [Ong-Toegang], [Onv-All-Verant], [Onv-Naleving]	[Organisatie]	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	JB
5.11 Retourneren van bedrijfsmiddelen	[Ong-Toegang], [Onv-All-Verant]	[Organisatie]		JB
5.12 Classificeren van informatie	[Onv-All-Verant]	[Organisatie]	#Informatiebescherming	JB
5.13 Labelen van informatie	[Onv-All-Verant], [Onv-Naleving], [Non-compliance]	[Organisatie]	#Informatiebescherming	JB

ISO 27002:2022	Motivatie	Locatie/Toelichting	Operationele capaciteiten	Selectie (N, J, B)
5.14 Overdragen van informatie	[Onv-Man-Stu], [Onv-All-Verant], [Niet-Naleving], [Fouten], [Ong-Wijziging] *Alleen voor essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Organisatie]	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	JB
5.15 Toegangsbeveiliging	[Onv-Man-Stu], [Onv-All-Verant], [Onv-Naleving], [Hacking], [Spionage]	[Organisatie]	#Identiteits-_en_toegangsbeheer	JB
5.16 Identiteitsbeheer	[Onv-Toegang], [Onv-Wijziging]	[Organisatie]	#Identiteits-_en_toegangsbeheer	JB
5.17 Beheren van authenticatie-informatie	[Onv-Toegang], [Onv-Wijziging], [Hacking], [Spionage], [Onv-All-Verant], [Onv-Naleving], [Ong-Toegang], [Ong-Wijziging]	[Organisatie]	#Identiteits-_en_toegangsbeheer	JB
5.18 Toegangsrechten	[Onv-Toegang], [Onv-Wijziging], [Onv-Naleving]	[Organisatie]	#Identiteits-_en_toegangsbeheer	JB
5.19 Informatiebeveiliging in leveranciersrelaties	[Onv-Man-Stu], [Onv-All-Verant]	[Organisatie]	#Beveiliging_in_leveranciersrelaties	JB
5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten	[Fouten], [Verlies-Dienst]	[Organisatie]	#Beveiliging_in_leveranciersrelaties	JB
5.21 Beheren van informatiebeveiliging in de ICT-keten	[Fouten], [Verlies-Dienst]	[Organisatie]	#Beveiliging_in_leveranciersrelaties	JB
5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	[Onv-Naleving], [Fouten], [Verlies-Dienst]	[Organisatie]	#Beveiliging_in_leveranciersrelaties #Borging_van_informatiebeveiliging	JB
5.23 Informatiebeveiliging voor het gebruik van clouddiensten	[Onv-Naleving], [Non-Compliance]	[Organisatie]	#Beveiliging_in_leveranciersrelaties	JB
5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	[Onv-All-Verant]	[Organisatie]	#Governance #Beheer_van_informatiebeveiligingsgebeurtenissen	JB
5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen		[Organisatie]	#Beheer_van_informatiebeveiligingsgebeurtenissen	JB
5.26 Reageren op informatiebeveiligingsincidenten	[Fouten]	[Organisatie]	#Beheer_van_informatiebeveiligingsgebeurtenissen	JB
5.27 Leren van informatiebeveiligingsincidenten	[Fouten]	[Organisatie]	#Beheer_van_informatiebeveiligingsgebeurtenissen	JB
5.28 Verzamelen van bewijsmateriaal	[Non-Compliance]	[Organisatie]	#Beheer_van_informatiebeveiligingsgebeurtenissen	JB

ISO 27002:2022	Motivatie	Locatie/Toelichting	Operationele capaciteiten	Selectie (N, J, B)
5.29 Informatiebeveiliging tijdens een verstoring	[Onv-Man-Stu], [Onv-All-Verant], [Verlies-Gegevens], [Verlies-Dienst], [Calamiteit] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Organisatie]	#Continuïteit	J
5.30 ICT-gereedheid voor bedrijfscontinuïteit	[Verlies-Gegevens], [Verlies-Dienst], [Calamiteit]	[Organisatie]	#Continuïteit	JB
5.31 Wettelijke, statutaire, regelgevende en contractuele eisen	[Onv-Man-Stu], [Onv-All-Verant], [Non-Compliance] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Organisatie], [ISMS]	#Juridisch_en_compliance	JB
5.32 Intellectuele-eigendomsrechten	[Non-Compliance], [Contractbreuk]	[Organisatie]	#Juridisch_en_compliance	JB
5.33 Beschermen van registraties	[Spionage], [Verlies-Gegevens] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Organisatie]	#Juridisch_en_compliance #Beheer_van_bedrijfsmiddelen #Informatiebescherming	JB
5.34 Privacy en bescherming van persoonsgegevens	[Non-Compliance]	[Organisatie]	#Informatiebescherming #Juridisch_en_compliance	JB
5.35 Onafhankelijke beoordeling van informatiebeveiliging	[Onv-Man-Stu], [Onv-Naleving]	[Organisatie]	#Borging_van_informatiebeveiliging	JB
5.36 Naleving van beleid, regels en normen voor informatiebeveiliging	[Onv-Naleving]	[Organisatie]	#Juridisch_en_compliance #Borging_van_informatiebeveiliging	JB
5.37 Gedocumenteerde bedieningsprocedures	[Fouten], [Verlies-Dienst]	[Organisatie]	#Beheer_van_bedrijfs_middelen #Fysieke_beveiliging #Systeem-_en_netwerkbeveiliging #Toepassingsbeveiliging #Veilige_configuratie #Identiteits-_en_toegangsbeheer #Beheer_van_dreigingen_en_kwetsbaarheden #Continuïteit #Beheer_van_informatiebeveiligingsgebeurtenissen	JB

ISO 27002:2022	Motivatie	Locatie/Toelichting	Operationele capaciteiten	Selectie (N, J, B)
6 Mensgerichte beheersmaatregelen				
6.1 Screening	[Onv-Intregriteit]	[Mens]	#Personeelsbeveiliging	JB
6.2 Arbeidsovereenkomst	[Onv-All-Verant]	[Mens]	#Personeelsbeveiliging	JB
6.3 Bewustwording van, opleiding en training in informatiebeveiliging	[Onv-Integriteit], [Fouten]	[Mens]	#Personeelsbeveiliging	JB
6.4 Disciplinaire procedure	[Onv-Naleging], [Onv-Integriteit]	[Mens]	#Personeelsbeveiliging	JB
6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	[Onv-All-Verant], [Onv-Naleving]	[Mens]	#Personeelsbeveiliging #Beheer_van_bedrijfsmiddelen	JB
6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten	[Onv-All-Verant], [Onv-Naleving]	[Mens]	#Personeelsbeveiliging #Informatiebescherming #Leveranciersrelaties	JB
6.7 Werken op afstand	[Ong-Toegang], [Hacking], [Spionage]	[Mens]	Beheer_van_bedrijfsmiddelen #Informatiebescherming #Fysieke_beveiliging #Systeem-_en_netwerkbeveiliging	JB
6.8 Melden van informatiebeveiligingsgebeurtenissen	[Onv-Man-Stu], [Onv-All-Verant], [Onv-Naleving]	[Mens]	#Beheer_van_informatiebeveiligingsgebeurtenissen	JB
7 Fysieke beheersmaatregelen				
7.1 Fysieke beveiligingszones	[Onv-All-Verant], [Ong-Toegang], [Hacking], [Spionage]	[Fysiek]	#Fysieke_beveiliging	JB
7.2 Fysieke toegangsbeveiliging	[Sabotage], [Diefstal], [Spionage], [Non-Compliance]	[Fysiek]	#Fysieke_beveiliging #Identiteits-_en_toegangsbeheer	JB
7.3 Beveiligen van kantoren, ruimten en faciliteiten	[Sabotage], [Diefstal], [Spionage], [Ong-Toegang], [Ong-Wijziging]	[Fysiek]	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	JB
7.4 Monitoren van de fysieke beveiliging	[Sabotage], [Diefstal], [Spionage], [Ong-Toegang], [Ong-Wijziging]	[Fysiek]	#Fysieke_beveiliging	JB
7.5 Beschermen tegen fysieke en omgevingsdreigingen	[Diefstal], [Spionage]	[Fysiek]	#Fysieke_beveiliging	JB
7.6 Werken in beveiligde zones	[Sabotage], [Diefstal], [Hacking]	[Fysiek]	#Fysieke_beveiliging	JB
7.7 ‘Clear desk’ en ‘clear screen’	[Onv-Naleving], [Verlies-Gegevens], [Spionage]	[Fysiek]	#Fysieke_beveiliging	JB

ISO 27002:2022	Motivatie	Locatie/Toelichting	Operationele capaciteiten	Selectie (N, J, B)
7.8 Plaatsen en beschermen van apparatuur	[Sabotage], [Diefstal], [Spionage]	[Fysiek]	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	JB
7.9 Beveiligen van bedrijfsmiddelen buiten het terrein	[Diefstal], [Spionage], [Verlies-Gegevens]	[Fysiek]	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	JB
7.10 Opslagmedia	[Verlies-Gegevens], [Diefstal], [Spionage], [Hacking], [Onv-All-Verant], [Fouten]	[Fysiek]	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	JB
7.11 Nutsvoorzieningen	[Calamiteit], [Verlies-Dienst], [Contractbreuk]	[Fysiek]	#Fysieke_beveiliging	JB
7.12 Beveiligen van bekabeling	[Sabotage], [Spionage]	[Fysiek]	#Fysieke_beveiliging	JB
7.13 Onderhoud van apparatuur	[Fouten], [Verlies-Dienst], [Contractbreuk]	[Fysiek]	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	JB
7.14 Veilig verwijderen of hergebruiken van apparatuur	[Spionage]	[Fysiek]	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	JB
8 Technologische beheersmaatregelen				
8.1 ‘User endpoint devices’	[Ong-Toegang], [Hacking], [Spionage], [Diefstal], [Verlies-Gegevens]	[Technologie]	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	JB
8.2 Speciale toegangsrechten	[Onv-Toegang], [Onv-Wijziging]	[Technologie]	#Identiteits-_en_toegangsbeheer	JB
8.3 Beperking toegang tot informatie	[Ong-Toegang], [Hacking], [Spionage]	[Technologie]	#Identiteits-_en_toegangsbeheer	JB
8.4 Toegangsbeveiliging op broncode	[Ong-Toegang], [Ong-Wijziging], [Onv-Integriteit], [Hacking], [Spionage]	[Technologie]	#Identiteits-_en_toegangsbeheer #Toepassingsbeveiliging #Veilige_configuratie	JB
8.5 Beveiligde authenticatie	[Ong-Toegang], [Ong-Wijziging], [Hacking], [Spionage]	[Technologie]	#Identiteits-_en_toegangsbeheer	JB
8.6 Capaciteitsbeheer	[Verlies-Dienst]	[Technologie]	#Continuïteit	JB
8.7 Bescherming tegen malware	[Verlies-Dienst], [Verlies-Gegevens], [Hacking], [Spionage]	[Technologie]	#Systeem-_en_netwerkbeveiliging #Informatiebescherming	JB
8.8 Beheer van technische kwetsbaarheden	[Hacking], [Spionage], [Verlies-Dienst], [Onv-Naleving]	[Technologie]	#Beheer_van_dreigingen_en_kwetsbaarheden	JB

ISO 27002:2022	Motivatie	Locatie/Toelichting	Operationele capaciteiten	Selectie (N, J, B)
8.9 Configuratiebeheer	[Ong-Toegang], [Ong-Wijziging], [Hacking], [Spionage]	[Technologie]	#Veilige_configuratie	JB
8.10 Wissen van informatie	[Verlies-Gegevens], [Non-Compliance]	[Technologie]	#Informatiebescherming #Juridisch_en_compliance	JB
8.11 Maskeren van gegevens	[Verlies-Gegevens], [Non-Compliance]	[Technologie]	#Informatiebescherming	JB
8.12 Voorkomen van gegevenslekken (Data leakage prevention)	[Verlies-Gegevens], [Non-Compliance]	[Technologie]	#Informatiebescherming	JB
8.13 Back-up van informatie	[Verlies-Gegevens], [Calamiteit]	[Technologie]	#Continuïteit	JB
8.14 Redundantie van informatieverwerkende faciliteiten	[Verlies-Gegevens], [Verlies-Dienst], [Calamiteit] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Technologie]	#Continuïteit #Beheer_van_bedrijfsmiddelen	J
8.15 Logging	[Onv-Naleving], [Verlies-Gegevens]	[Technologie]	#Beheer_van_informatiebeveiligingsgebeurtenissen	JB
8.16 Monitoren van activiteiten	[Hacking], [Spionage], [Ong-Toegang], [Ong-Wijziging], [Onv-Integriteit]	[Technologie]	#Beheer_van_informatiebeveiligingsgebeurtenissen	
8.17 Kloksynchronisatie	[Onv-Naleving]	[Technologie]	#Beheer_van_informatiebeveiligingsgebeurtenissen	JB
8.18 Gebruik van speciale systeemhulpmiddelen	[Ong-Toegang], [Ong-Wijziging], [Onv-Integriteit]	[Technologie]	#Systeem-_en_netwerkbeveiliging #Veilige_configuratie #Toepassingsbeveiliging	JB
8.19 Installeren van software op operationele systemen	[Fouten], [Verlies-Dienst], [Hacking], [Spionage], [Verlies-Gegevens]	[Technologie]	#Veilige_configuratie #Toepassingsbeveiliging	JB
8.20 Beveiliging netwerkcomponenten	[Onv-Man-Stu], [Onv-All-Verant]	[Technologie]	#Systeem-_en_netwerkbeveiliging	JB
8.21 Beveiliging van netwerkdiensten	[Spionage], [Hacking]	[Technologie]	#Systeem-_en_netwerkbeveiliging	JB
8.22 Netwerksegmentatie	[Ong-Toegang], [Hacking], [Spionage], [Fouten], [Onv-Integriteit]	[Technologie]	#Systeem-_en_netwerkbeveiliging	JB
8.23 Toepassen van webfilters	[Hacking], [Spionage], [Verlies-Gegevens], [Verlies-Dienst]	[Technologie]	#Systeem-_en_netwerkbeveiliging	

ISO 27002:2022	Motivatie	Locatie/Toelichting	Operationele capaciteiten	Selectie (N, J, B)
8.24 Gebruik van cryptografie	[Ong-Wijziging], [Onv-All-Verant], [Ong-Toegang], [Hacking], [Spionage] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Technologie]	#Veilige_configuratie	J
8.25 Beveiligen tijdens de ontwikkelcyclus	[Onv-Man-Stu], [Onv-All-Verant]	[Technologie]	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	JB
8.26 Toepassingsbeveiligingseisen	[Ong-Toegang], [Ong-Wijziging], [Hacking], [Contractbreuk] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Technologie]	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	JB
8.27 Veilige systeemarchitectuur en technische uitgangspunten	[Fouten], [Verlies-Dienst]	[Technologie]	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	JB
8.28 Veilig coderen	[Hacking], [Spionage], [Verlies-Gegevens], [Verlies-Dienst], [Ong-Toegang], [Ong-Wijziging]	[Technologie]	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	
8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie	[Fouten], [Verlies-Dienst], [Ong-Toegang]	[Technologie]	#Toepassingsbeveiliging #Borging_van_informatiebeveiliging #Systeem-_en_netwerkbeveiliging	JB
8.30 Uitbestede systeemontwikkeling	[Fouten], [Verlies-Dienst], [Ong-Toegang] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Technologie], [ISMS]	#Systeem-_en_netwerkbeveiliging #Toepassingsbeveiliging #Beveiliging_in_leveranciersrelaties	J
8.31 Scheiding van ontwikkel-, test- en productieomgevingen	[Ong-Toegang], [Ong-Wijziging], [Hacking], [Fouten]	[Technologie]	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	JB
8.32 Wijzigingsbeheer	[Fouten], [Verlies-Dienst]	[Technologie], [ISMS]	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	JB
8.33 Testgegevens	[Onv-Man-Stu], [Onv-All-Verant]	[Technologie]	#Informatiebescherming	JB
8.34 Bescherming van informatiesystemen tijdens audits	[Fouten], [Ong-Toegang], [Ong-Wijziging], [Verlies-Dienst] *Alleen voor Essentiële informatiesystemen indien relevantie uit RBB naar voren komt.*	[Technologie]	#Systeem-_en_netwerkbeveiliging #Informatiebescherming	J