



# **Verklaring van toepasselijkheid**

**NEN-EN-ISO/IEC 27002+A11:2020 - NL**

## **PUBLICATIEGEGEVENS**

Auteur: r.peeters@archive-it.nl

Datum: 03-03-2021

Archive-IT

Reuver

[www.archive-it.nl](http://www.archive-it.nl)

# 1. Inleiding

## 1.1. Algemene informatie

Norm:	NEN-EN-ISO/IEC 27002+A11:2020 - NL
Omschrijving	Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging
Totaal aantal controls:	114
Aantal controls van toepassing	114
Totaal aantal maatregelen:	114
Aantal maatregelen volledig geïmplementeerd:	114

## 1.2. Scope

Beheren en archiveren van fysieke informatie en transformeren van deze informatie naar digitale vorm, ontwikkelen van software interfaces en toepassingen om gedigitaliseerde informatie te integreren in de informatiesystemen en werkprocessen, zoals vastgesteld door het management en in overeenstemming met de Verklaring van Toepasselijkheid.

Versie 1.6 (datum 03-03-2021)

## 1.3. Risicoaanpak

## 2. Controls - Van toepassing

In deze verklaring van toepasselijkheid is inzichtelijk welke maatregelen er geïdentificeerd zijn om te voldoen aan de gestelde eisen in de norm. De volgende kolommen zijn opgenomen:

**Baseline:** Als een maatregel wordt beschouwd als een minimaal te nemen maatregel, bijvoorbeeld voor de opzet, bestaan en werking van een managementsysteem of het bereiken van het basisniveau van beveiliging of kwaliteit, dan is deze aangevinkt als baseline.

**Effectiviteit:** Als er een controle op de werking van de maatregel heeft plaatsgevonden, dan wordt de percentuele score hier weergegeven.

**Aantal implementaties:** Als een maatregel daadwerkelijk geïmplementeerd is, dan staat het aantal implementaties in de kolom vermeld. De kolom geeft het aantal middelen/processen weer waarvoor de maatregel geïmplementeerd is.

**Aantal implementaties afgerond:** Met deze kolom wordt zichtbaar hoeveel implementaties er zijn afgerond. Hiermee wordt ook zichtbaar of er nog openstaande implementaties zijn door dit aantal te vergelijken met de kolom 'Aantal implementaties'.

**De kolom tags bevat aanvullende informatie over de geselecteerde maatregel :** De reden van selectie van de maatregel t.g.v. een wettelijke verplichting, contractuele verplichting of bedrijfsvereisten is terug vinden in deze kolom als de maatregel daarmee gemarkeerd is.

**Volgnummer risicobehandeling en volgnummer doelstelling :** Als een maatregel één of meerdere keren geïmplementeerd is, dan wordt in deze kolommen zichtbaar in welke risicobehandeling(en) en/of bij welke doelstelling(en) de maatregel geselecteerd is. Elke risicobehandeling en doelstelling heeft een uniek nummer. In het rapport 'Risicobehandelingen en doelstellingen' zijn de genummerde risicobehandelingen en doelstellingen te raadplegen voor meer informatie.



	01	Beleid voor mobiele apparatuur									
		CLMS.02.A.06.02.01 Beleid voor mobiele apparatuur	--	100	2	2		1; 11	RA (risico analyse)		
	02	Telewerken									
		CLMS.02.A.06.02.02 Telewerken	--	100	3	3	58	1; 11	RA (risico analyse)		
<b>A.07</b>	<b>Veilig Personeel</b>										
	01	Voorafgaand aan het dienstverband									
	01	Screening									
		CLMS.02.A.07.01.01 Screening	--	100	2	2		1; 11	RA (risico analyse)		
	02	Arbeidsvoorwaarden									
		CLMS.02.A.07.01.02 Arbeidsvoorwaarden	--		2	2		1; 11	RA (risico analyse)		
	02	Tijdens het dienstverband									
	01	Directieverantwoordelijkheden									
		CLMS.02.A.07.02.01 Directieverantwoordelijkheid	--	100	2	2		1; 11	BP (best practice)		
	02	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging									
		CLMS.02.A.07.02.02 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	--	100	2	2		1; 11	RA (risico analyse)		
	03	Disciplinaire procedure									
		CLMS.02.A.07.02.03 Disciplinaire procedure	--	50	2	2		1; 11	BP (best practice)		
	03	Beëindiging en wijziging van dienstverband									
	01	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband									
		CLMS.02.A.07.03.01 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	--	100	2	2		1; 11	BP (best practice)		
<b>A.08</b>	<b>Beheer van bedrijfsmiddelen</b>										
	01	Verantwoordelijkheid voor bedrijfsmiddelen									
	01	Inventariseren van bedrijfsmiddelen									
		CLMS.02.A.08.01.01 Inventariseren van bedrijfsmiddelen	--	100	2	2		1; 11	RA (risico analyse)		
	02	Eigendom van bedrijfsmiddelen									
		CLMS.02.A.08.01.02 Eigendom van bedrijfsmiddelen	--	100	2	2		1; 11	RA (risico analyse)		
	03	Aanvaardbaar gebruik van bedrijfsmiddelen									
		CLMS.02.A.08.01.03 Aanvaardbaar gebruik van bedrijfsmiddelen	--	50	2	2		1; 11	RA (risico analyse)		

	04	Teruggeven van bedrijfsmiddelen										
		CLMS.02.A.08.01.04 Teruggeven van bedrijfsmiddelen	--	100	2	2			1; 11	RA (risico analyse)		
02		Informatieclassificatie										
	01	Classificatie van informatie										
		CLMS.02.A.08.02.01 Classificatie van informatie	--	100	2	2			1; 11	RA (risico analyse)		
	02	Informatie labelen										
		CLMS.02.A.08.02.02 Informatie labelen	--	100	2	2			1; 11	RA (risico analyse)		
	03	Behandelen van bedrijfsmiddelen										
		CLMS.02.A.08.02.03 Behandelen van bedrijfsmiddelen	--	50	2	2			1; 11	RA (risico analyse)		
03		Behandelen van media										
	01	Beheer van verwijderbare media										
		CLMS.02.A.08.03.01 Beheer van verwijderbare media	--	100	2	2			1; 11	RA (risico analyse)		
	02	Verwijderen van media										
		CLMS.02.A.08.03.02 Verwijderen van media	--	100	3	3	68		1; 11	RA (risico analyse)		
	03	Media fysiek overdragen										
		CLMS.02.A.08.03.03 Media fysiek overdragen	--	100	3	3	68		1; 11	RA (risico analyse)		
<b>A.09 Toegangsbeveiliging</b>												
01		Bedrijfseisen voor toegangsbeveiliging										
	01	Beleid voor toegangsbeveiliging										
		CLMS.02.A.09.01.01 Beleid voor toegangsbeveiliging	--	100	2	2			1; 11	RA (risico analyse)		
	02	Toegang tot netwerken en netwerkdiensten										
		CLMS.02.A.09.01.02 Toegang tot netwerken en netwerkdiensten	--	100	2	2			1; 11	RA (risico analyse)		
02		Beheer van toegangsrechten van gebruikers										
	01	Registratie en afmelden van gebruikers										
		CLMS.02.A.09.02.01 Registratie en afmelden van gebruikers	--	100	2	2			1; 11	RA (risico analyse)		
	02	Gebruikers toegang verlenen										
		CLMS.02.A.09.02.02 Gebruikers toegang verlenen	--	100	2	2			1; 11	RA (risico analyse)		
	03	Beheren van speciale toegangsrechten										
		CLMS.02.A.09.02.03 Beheren van speciale toegangsrechten	--		1	1			1			
	04	Beheer van geheime authenticatie-informatie van gebruikers										

		CLMS.02.A.09.02.04 Beheer van geheime authenticatie-informatie van gebruikers	--	50	2	2		1; 11	RA (risico analyse)
	05	Beoordeling van toegangsrechten van gebruikers							
		CLMS.02.A.09.02.05 Beoordeling van toegangsrechten van gebruikers	--	100	2	2		1; 11	RA (risico analyse)
	06	Toegangsrechten intrekken of aanpassen							
		CLMS.02.A.09.02.06 Toegangsrechten intrekken of aanpassen	--	100	2	2		1; 11	RA (risico analyse)
03		Verantwoordelijkheden van gebruikers							
	01	Geheime authenticatie-informatie gebruiken							
		CLMS.02.A.09.03.01 Geheime authenticatie-informatie gebruiken	--	100	2	2		1; 11	RA (risico analyse)
04		Toegangsbeveiliging van systeem en toepassing							
	01	Beperking toegang tot informatie							
		CLMS.02.A.09.04.01 Beperking toegang tot informatie	--	100	2	2		1; 11	RA (risico analyse)
	02	Beveiligde inlogprocedures							
		CLMS.02.A.09.04.02 Beveiligde inlogprocedures	--	100	2	2		1; 11	RA (risico analyse)
	03	Systeem voor wachtwoordbeheer							
		CLMS.02.A.09.04.03 Systeem voor wachtwoordbeheer	--	100	2	2		1; 11	RA (risico analyse)
	04	Speciale systeemhulpmiddelen gebruiken							
		CLMS.02.A.09.04.04 Speciale systeemhulpmiddelen gebruiken	--	100	2	2		1; 11	BP (best practice)
	05	Toegangsbeveiliging op programmabroncode							
		CLMS.02.A.09.04.05 Toegangsbeveiliging op programmabroncode	--	100	2	2		1; 11	RA (risico analyse)
<b>A.10</b>		<b>Cryptografie</b>							
	01	Cryptographic controls							
		01 Beleid inzake het gebruik van cryptografische beheersmaatregelen							
		CLMS.02.A.10.01.01 Beleid inzake het gebruik van cryptografische beheersmaatregelen	--	50	2	2		1; 11	RA (risico analyse)
		02 Sleutelbeheer							
		CLMS.02.A.10.01.02 Sleutelbeheer	--	100	2	2		1; 11	RA (risico analyse)
<b>A.11</b>		<b>Fysieke beveiliging en beveiliging van de omgeving</b>							
	01	Beveiligde gebieden							
		01 Fysieke beveiligingszone							

	CLMS.02.A.11.01.01 Fysieke beveiligingszone	--	100	2	2		1; 11	RA (risico analyse)
02	Fysieke toegangsbeveiliging							
	CLMS.02.A.11.01.02 Fysieke toegangsbeveiliging	--	100	2	2		1; 11	RA (risico analyse)
03	Kantoren, ruimten en faciliteiten beveiligen							
	CLMS.02.A.11.01.03 Kantoren, ruimten en faciliteiten beveiligen	--	100	2	2		1; 11	RA (risico analyse)
04	Beschermen tegen bedreigingen van buitenaf							
	CLMS.02.A.11.01.04 Beschermen tegen bedreigingen van buitenaf	--	50	2	2		1; 11	RA (risico analyse)
05	Werken in beveiligde gebieden							
	CLMS.02.A.11.01.05 Werken in beveiligde gebieden	--	100	2	2		1; 11	RA (risico analyse)
06	Laad- en loslocatie							
	CLMS.02.A.11.01.06 Laad- en loslocatie	--	100	2	2		1; 11	RA (risico analyse)
02	Apparatuur							
01	Plaatsing en bescherming van apparatuur							
	CLMS.02.A.11.02.01 Plaatsing en bescherming van apparatuur	--	100	2	2		1; 11	RA (risico analyse)
02	Nutsvoorzieningen							
	CLMS.02.A.11.02.02 Nutsvoorzieningen	--		2	2		1; 11	RA (risico analyse)
03	Beveiliging van bekabeling							
	CLMS.02.A.11.02.03 Beveiliging van bekabeling	--	50	2	2		1; 11	RA (risico analyse)
04	Onderhoud van apparatuur							
	CLMS.02.A.11.02.04 Onderhoud van apparatuur	--	50	2	2		1; 11	RA (risico analyse)
05	Verwijdering van bedrijfsmiddelen							
	CLMS.02.A.11.02.05 Verwijdering van bedrijfsmiddelen	--	100	2	2		1; 11	RA (risico analyse)
06	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein							
	CLMS.02.A.11.02.06 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	--	50	2	2		1; 11	RA (risico analyse)
07	Veilig verwijderen of hergebruiken van apparatuur							
	CLMS.02.A.11.02.07 Veilig verwijderen of hergebruiken van apparatuur	--	100	2	2		1; 11	RA (risico analyse)
08	Onbeheerde gebruikersapparatuur							
	CLMS.02.A.11.02.08 Onbeheerde gebruikersapparatuur	--		2	2		1; 11	RA (risico analyse)
09	'Clear desk'- en 'clear screen'-beleid							



		CLMS.02.A.11.02.09 'Clear desk'- en 'clear screen'-beleid	--		2	2		1; 11	RA (risico analyse)
<b>A.12</b>	<b>Beveiliging bedrijfsvoering</b>								
01	Bedieningsprocedures en verantwoordelijkheden								
01	Gedocumenteerde bedieningsprocedures								
		CLMS.02.A.12.01.01 Gedocumenteerde bedieningsprocedures	--	100	2	2		1; 11	RA (risico analyse)
02	Wijzigingsbeheer								
		CLMS.02.A.12.01.02 Wijzigingsbeheer	--	100	2	2		1; 11	RA (risico analyse)
03	Capaciteitsbeheer								
		CLMS.02.A.12.01.03 Capaciteitsbeheer	--	100	3	3	68	1; 11	RA (risico analyse)
05	Scheiding van ontwikkel-, test- en productieomgevingen								
		CLMS.02.A.12.01.04 Scheiding van faciliteiten voor ontwikkeling, testen en productie	--	100	2	2		1; 11	RA (risico analyse)
02	Bescherming tegen malware								
01	Beheersmaatregelen tegen malware								
		CLMS.02.A.12.02.01 Beheersmaatregelen tegen malware	--	100	2	2		1; 11	RA (risico analyse)
03	Back-up								
01	Back-up van informatie								
		CLMS.02.A.12.03.01 Back-up van informatie	--	34	2	2		1; 11	RA (risico analyse)
04	Verslaglegging en monitoren								
01	Gebeurtenissen registreren								
		CLMS.02.A.12.04.01 Gebeurtenissen registreren	--	100	2	2		1; 11	RA (risico analyse)
02	Beschermen van informatie in logbestanden								
		CLMS.02.A.12.04.02 Beschermen van informatie in logbestanden	--	100	2	2		1; 11	RA (risico analyse)
03	Logbestanden van beheerders en operators								
		CLMS.02.A.12.04.03 Logbestanden van beheerders en operators	--	100	2	2		1; 11	RA (risico analyse)
04	Kloksynchronisatie								
		CLMS.02.A.12.04.04 Kloksynchronisatie	--	100	2	2		1; 11	RA (risico analyse)
05	Beheersing van operationele software								
01	Software installeren op operationele systemen								
		CLMS.02.A.12.05.01 Software installeren op operationele systemen	--	100	2	2		1; 11	RA (risico analyse)

06	Beheer van technische kwetsbaarheden								
	01	Beheer van technische kwetsbaarheden							
		CLMS.02.A.12.06.01 Beheer van technische kwetsbaarheden	--	100	2	2		1; 11	RA (risico analyse)
	02	Beperkingen voor het installeren van software							
CLMS.02.A.12.06.02 Beperkingen voor het installeren van software		--	100	2	2		1; 11	BP (best practice)	
07	Overwegingen betreffende audits van informatiesystemen								
	01	Beheersmaatregelen betreffende audits van informatiesystemen							
CLMS.02.A.12.07.01 Beheersmaatregelen betreffende audits van informatiesystemen		--	100	2	2		1; 11	RA (risico analyse)	
<b>A.13</b>	<b>Communicatiebeveiliging</b>								
01	Beheer van netwerkbeveiliging								
	01	Beheersmaatregelen voor netwerken							
		CLMS.02.A.13.01.01 Beheersmaatregelen voor netwerken	--	100	2	2		1; 11	RA (risico analyse)
	02	Beveiliging van netwerkdiensten							
		CLMS.02.A.13.01.02 Beveiliging van netwerkdiensten	--	50	2	2		1; 11	RA (risico analyse)
	03	Scheiding in netwerken							
		CLMS.02.A.13.01.03 Scheiding van netwerken	--	100	2	2		1; 11	RA (risico analyse)
	02	Informatietransport							
		01	Beleid en procedures voor informatietransport						
			CLMS.02.A.13.02.01 Beleid en procedures voor informatietransport	--	50	2	2		1; 11
02		Overeenkomsten over informatietransport							
		CLMS.02.A.13.02.02 Overeenkomsten over informatietransport	--	100	2	2		1; 11	BP (best practice)
03		Elektronische berichten							
		CLMS.02.A.13.02.03 Elektronisch berichtenuitwisseling	--	100	2	2		1; 11	RA (risico analyse)
04		Vertrouwelijkheids- of geheimhoudingsovereenkomst							
	CLMS.02.A.13.02.04 Vertrouwelijkheids- of geheimhoudingsovereenkomst	--		2	2		1; 11	W en R (wet en regelgeving)	
<b>A.14</b>	<b>Acquisitie, ontwikkeling en onderhoud van informatiesystemen</b>								
01	Beveiligingseisen voor informatiesystemen								
	01	Analyse en specificatie van informatiebeveiligingseisen							

		CLMS.02.A.14.01.01 Analyse en specificatie van informatiebeveiligingseisen	--	100	2	2		1; 11	RA (risico analyse)
02		Toepassingen op openbare netwerken beveiligen							
		CLMS.02.A.14.01.02 Toepassingen op openbare netwerken beveiligen	--	100	2	2		1; 11	BP (best practice)
03		Transacties van toepassingen beschermen							
		CLMS.02.A.14.01.03 Transacties van toepassingen beschermen	--	100	2	2		1; 11	RA (risico analyse)
02		Beveiliging in ontwikkelings- en ondersteunende processen							
01		Beleid voor beveiligd ontwikkelen							
		CLMS.02.A.14.02.01 Beleid voor beveiligd ontwikkelen	--	50	2	2		1; 11	RA (risico analyse)
02		Procedures voor wijzigingsbeheer met betrekking tot systemen							
		CLMS.02.A.14.02.02 Procedures voor wijzigingsbeheer met betrekking tot systemen	--	100	2	2		1; 11	RA (risico analyse)
03		Technische beoordeling van toepassingen na wijzigingen besturingsplatform							
		CLMS.02.A.14.02.03 Technische beoordeling van toepassingen na wijzigingen besturingsplatform	--	100	2	2		1; 11	RA (risico analyse)
04		Beperkingen op wijzigingen aan softwarepakketten							
		CLMS.02.A.14.02.04 Beperkingen op wijzigingen aan softwarepakketten	--	100	2	2		1; 11	BP (best practice)
05		Principes voor engineering van beveiligde systemen							
		CLMS.02.A.14.02.05 Principes voor engineering van beveiligde systemen	--	50	2	2		1; 11	BP (best practice)
06		Beveiligde ontwikkelomgeving							
		CLMS.02.A.14.02.06 Beveiligde ontwikkelomgevingen	--	100	2	2		1; 11	BP (best practice)
07		Uitbestede softwareontwikkeling							
		CLMS.02.A.14.02.07 Uitbestede softwareontwikkeling	--	50	2	2		1; 11	BP (best practice)
08		Testen van systeembeveiliging							
		CLMS.02.A.14.02.08 Testen van systeembeveiliging	--	100	2	2		1; 11	BP (best practice)
09		Systeemacceptatietests							
		CLMS.02.A.14.02.09 Systeemacceptatietests	--	100	2	2		1; 11	RA (risico analyse)
03		Testgegevens							
01		Bescherming van testgegevens							

		CLMS.02.A.14.03.01 Bescherming van testgegevens	--	100	2	2		1; 11	RA (risico analyse)
<b>A.15</b>	<b>Leveranciersrelaties</b>								
	01	Informatiebeveiliging in leveranciersrelaties							
	01	Informatiebeveiligingsbeleid voor leveranciersrelaties							
		CLMS.02.A.15.01.01 Informatiebeveiligingsbeleid voor leveranciersrelaties	--	100	2	2		1; 11	RA (risico analyse)
	02	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten							
		CLMS.02.A.15.01.02 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	--	100	2	2		1; 11	W en R (wet en regelgeving)
	03	Toeleveringsketen van informatie- en communicatietechnologie							
		CLMS.02.A.15.01.03 Toeleveringsketen van informatie- en communicatietechnologie	--	100	2	2		1; 11	W en R (wet en regelgeving)
	02	Beheer van dienstverlening van leveranciers							
	01	Monitoring en beoordeling van dienstverlening van leveranciers							
		CLMS.02.A.15.02.01 Monitoring en beoordeling van dienstverlening van leveranciers	--	100	2	2		1; 11	RA (risico analyse)
	02	Beheer van veranderingen in dienstverlening van leveranciers							
		CLMS.02.A.15.02.02 Beheer van wijzigingen in dienstverlening door een derde partij	--	100	2	2		1; 11	W en R (wet en regelgeving)
<b>A.16</b>	<b>Beheer van informatiebeveiligingsincidenten</b>								
	01	Beheer van informatiebeveiligingsincidenten en -verbeteringen							
	01	Verantwoordelijkheden en procedures							
		CLMS.02.A.16.01.01 Verantwoordelijkheden en procedures	--	100	2	2		1; 11	RA (risico analyse)
	02	Rapportage van informatiebeveiligingsgebeurtenissen							
		CLMS.02.A.16.01.02 Rapportage van informatiebeveiligingsgebeurtenissen	--	100	2	2		1; 11	RA (risico analyse)
	03	Rapportage van zwakke plekken in de informatiebeveiliging							
		CLMS.02.A.16.01.03 Rapportage van zwakke plekken in de informatiebeveiliging	--	100	2	2		1; 11	RA (risico analyse)
	04	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen							
		CLMS.02.A.16.01.04 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	--	100	2	2		1; 11	RA (risico analyse)

	05	Respons op informatiebeveiligingsincidenten										
		CLMS.02.A.16.01.05 Respons op informatiebeveiligingsincidenten	--	100	2	2		1; 11	RA	(risico analyse)		
	06	Lering uit informatiebeveiligingsincidenten										
		CLMS.02.A.16.01.06 Leren van informatiebeveiligingsincidenten	--	50	2	2		1; 11	RA	(risico analyse)		
	07	Verzamelen van bewijsmateriaal										
		CLMS.02.A.16.01.07 Verzamelen van bewijsmateriaal	--	100	2	2		1; 11	RA	(risico analyse)		
<b>A.17</b>	<b>Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer</b>											
	01	Informatiebeveiligingscontinuïteit										
		01 Informatiebeveiligingscontinuïteit plannen										
		CLMS.02.A.17.01.01 Informatiebeveiligingscontinuïteit plannen	--	100	2	2		1; 11	RA	(risico analyse)		
		02 Informatiebeveiligingscontinuïteit implementeren										
		CLMS.02.A.17.01.02 Informatiebeveiligingscontinuïteit implementeren	--	50	2	2		1; 11	RA	(risico analyse)		
		03 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren										
		CLMS.02.A.17.01.03 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	--	100	2	2		1; 11	RA	(risico analyse)		
	02	Redundante componenten										
		01 Beschikbaarheid van informatieverwerkende faciliteiten										
		CLMS.02.A.17.02.01 Beschikbaarheid van informatieverwerkende faciliteiten	--	100	2	2		1; 11	RA	(risico analyse)		
<b>A.18</b>	<b>Naleving</b>											
	01	Naleving van wettelijke en contractuele eisen										
		01 Vaststellen van toepasselijke wetgeving en contractuele eisen										
		CLMS.02.A.18.01.01 Vaststellen van toepasselijke wetgeving en contractuele eisen	--	100	2	2		1; 11	W en R (wet en regelgeving)			
		02 Intellectuele-eigendomsrechten										
		CLMS.02.A.18.01.02 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)	--	100	2	2		1; 11	W en R (wet en regelgeving)			
		03 Beschermen van registraties										
		CLMS.02.A.18.01.03 Beschermen van registraties	--	100	2	2		1; 11	RA	(risico analyse)		
		04 Privacy en bescherming van persoonsgegevens										
		CLMS.02.A.18.01.04 Privacy en bescherming van persoonsgegevens	--	100	3	3	63	1; 11	W en R (wet en regelgeving)			

	05	Voorschriften voor het gebruik van cryptografische beheersmaatregelen								
		CLMS.02.A.18.01.05 Voorschriften voor het gebruik van cryptografische beheersmaatregelen	--	100	2	2		1; 11	RA (risico analyse)	
02		Informatiebeveiligingsbeoordelingen								
	01	Onafhankelijke beoordeling van informatiebeveiliging								
		CLMS.02.A.18.02.01 Onafhankelijke beoordeling van informatiebeveiliging	--	100	2	2		1; 11	BP (best practice)	
	02	Naleving van beveiligingsbeleid en -normen								
		CLMS.02.A.18.02.02 Naleving van beveiligingsbeleid en -normen	--	34	2	2		1; 11	BP (best practice)	
	03	Beoordeling van technische naleving								
		CLMS.02.A.18.02.03 Beoordeling van technische naleving	--	100	2	2		1; 11	BP (best practice)	

### **3. Controls - Niet van toepassing**

Geen controls.