

ISO 27001	kwakeitsmanagementsysteem	Van toepassing	Geïmplementeerd	Wettelijke eis	Contractuele eis	Business requirement	Risico analyse	Verklaring indien niet van toepassing
A.5	A.5 Informatiebeveiligingsbeleid							
A.5.1	Aansturing door de directie van de informatiebeveiliging							
A.5.1.1	- Beleidsregels voor informatiebeveiliging	Ja	Ja			1		
A.5.1.2	- Beoordelen van het informatiebeveiligingsbeleid	Ja	Ja			1		
A.6	A.6 Organiseren van informatiebeveiliging							
A.6.1	Interne organisatie							
A.6.1.1	- Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	Ja			1	1	
A.6.1.2	- Scheiding van taken	Ja	Ja			1	1	
A.6.1.3	- Contact met overheidsinstanties	Ja	Ja			1	1	
A.6.1.4	- Contact met speciale belangengroepen	Ja	Ja			1	1	
A.6.1.5	- Informatiebeveiliging in projectbeheer	Ja	Ja			1	1	
A.6.2	Mobiele apparatuur en telewerken							
A.6.2.1	- Beleid voor mobiele apparatuur	Ja	Ja			1	1	
A.6.2.2	- Telewerken	Ja	Ja			1	1	
A.7	A.7 Veilig personeel							
A.7.1	Voorafgaand aan het dienstverband							
A.7.1.1	- Screening	Ja	Ja	1	1	1	1	
A.7.1.2	- Arbeidsvoorwaarden	Ja	Ja			1	1	
A.7.2	Tijdens het dienstverband							
A.7.2.1	- Directieverantwoordelijkheden	Ja	Ja			1	1	
A.7.2.2	- Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Ja	Ja			1	1	
A.7.2.3	- Disciplinaire procedure	Ja	Ja	1		1	1	
A.7.3	Beeindiging en wijziging van dienstverband							
A.7.3.1	- Beeindiging en wijziging van verantwoordelijkheden van het dienstverband	Ja	Ja			1	1	
A.8	A.8 Beheer van bedrijfsmiddelen							
A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen							
A.8.1.1	- Inventariseren van bedrijfsmiddelen	Ja	Ja			1	1	
A.8.1.2	- Eigendom van bedrijfsmiddelen	Ja	Ja			1		
A.8.1.3	- Aanvaardbaar gebruik van bedrijfsmiddelen	Ja	Ja			1	1	
A.8.1.4	- Teruggeven van bedrijfsmiddelen	Ja	Ja			1		
A.8.2	Informatieclassificatie							
A.8.2.1	- Classificatie van informatie	Ja	Ja			1	1	
A.8.2.2	- Informatie labelen	Ja	Ja			1	1	
A.8.2.3	- Behandelen van bedrijfsmiddelen	Ja	Ja			1	1	
A.8.3	Behandelen van media							
A.8.3.1	- Beheer van verwijderbare media	Ja	Ja			1		
A.8.3.2	- Verwijderen van media	Ja	Ja			1	1	
A.8.3.3	- Media fysiek overdragen	Ja	Ja			1	1	
A.9	A.9 Toegangsbeveiliging							
A.9.1	Bedrijfseisen voor toegangsbeveiliging							
A.9.1.1	- Beleid voor toegangsbeveiliging	Ja	Ja			1	1	
A.9.1.2	- Toegang tot netwerken en netwerkdiensten	Ja	Ja			1	1	
A.9.2	Beheer van toegangsrechten van gebruikers							
A.9.2.1	- Registratie en uitschrijving van gebruikers	Ja	Ja			1	1	
A.9.2.2	- Gebruikers toegang verlenen	Ja	Ja			1	1	
A.9.2.3	- Beheren van speciale toegangsrechten	Ja	Ja			1	1	
A.9.2.4	- Beheer van geheime authenticatie-informatie van gebruikers	Ja	Ja				1	
A.9.2.5	- Beoordelen van toegangsrechten van gebruikers	Ja	Ja			1		
A.9.2.6	-Toegangsrechten intrekken of aanpassen	Ja	Ja			1	1	
A.9.3	Gebruikersverantwoordelijkheden							
A.9.3.1	- Geheime authenticatie-informatie gebruiken	Ja	Ja			1	1	
A.9.4	Toegangsbeveiliging van systeem en toepassing							

A.9.4.1	- Beperking toegang tot informatie	Ja	Ja			1	1	
A.9.4.2	- Beveiligde inlogprocedures	Ja	Ja			1	1	
A.9.4.3	- Systeem voor wachtwoordbeheer	Ja	Ja			1	1	
A.9.4.4	- Speciale systeemhulpmiddelen gebruiken	Ja	Ja			1	1	
A.9.4.5	- Toegangsbeveiliging op programmaprocedure	Nee	Nee					Software ontwikkeling is uitbesteed en wordt extern onderhouden
A.10	A.10 Cryptografie							
A.10.1	Cryptografische beheersmaatregelen							
A.10.1.1	- Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ja	Ja				1	
A.10.1.2	- Sleutelbeheer	Ja	Ja				1	
A.11	A.11 Fysieke beveiliging en beveiliging van de omgeving							
A.11.1	Beveiligde gebieden							
A.11.1.1	- Fysieke beveiligingszone	Ja	Ja			1	1	
A.11.1.2	- Fysieke toegangsbeveiliging	Ja	Ja			1	1	
A.11.1.3	- Kantoren, ruimten, faciliteiten beveiligen	Ja	Ja			1	1	
A.11.1.4	- Beschermen tegen bedreigingen van buitenaf	Ja	Ja			1	1	
A.11.1.5	- Werken in beveiligde gebieden	Ja	Ja			1	1	
A.11.1.6	- Laad- en loslocatie	Ja	Ja					
A.11.2	Apparatuur					1	1	
A.11.2.1	- Plaatsing en bescherming van apparatuur	Ja	Ja			1	1	
A.11.2.2	- Nutsvoorzieningen	Ja	Ja			1	1	
A.11.2.3	- Beveiliging van bekabeling	Ja	Ja			1		
A.11.2.4	- Onderhoud van apparatuur	Ja	Ja			1	1	
A.11.2.5	- Verwijdering van bedrijfsmiddelen	Ja	Ja			1	1	
A.11.2.6	- Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Ja	Ja			1	1	
A.11.2.7	- Veilig verwijderen of hergebruiken van apparatuur	Ja	Ja			1	1	
A.11.2.8	- Onbeheerde gebruikersapparatuur	Ja	Ja			1	1	
A.11.2.9	- 'Clear desk'- en 'clear screen'-beleid	Ja	Ja			1	1	
A.12	A.12 Beveiliging bedrijfsvoering							
A.12.1	Bedieningsprocedures en verantwoordelijkheden							
A.12.1.1	- Gedocumenteerde bedieningsprocedures	Ja	Ja				1	
A.12.1.2	- Wijzigingsbeheer	Ja	Ja				1	
A.12.1.3	- Capaciteitsbeheer	Ja	Ja				1	
A.12.1.4	- Scheiding van ontwikkel-, test- en productieomgevingen	Ja	Ja			1	1	
A.12.2	Bescherming tegen malware							
A.12.2.1	- Beheersmaatregelen tegen malware	Ja	Ja			1	1	
A.12.3	Back-up							
A.12.3.1	- Back-up van informatie	Ja	Ja			1	1	
A.12.4	Verslaglegging en monitoren							
A.12.4.1	- Gebeurtenissen registreren	Ja	Ja			1	1	
A.12.4.2	- Beschermen van informatie in logbestanden	Ja	Ja			1	1	
A.12.4.3	- Logbestanden van beheerders en operators	Ja	Ja			1	1	
A.12.4.4	- Kloksynchronisatie	Ja	Ja			1	1	
A.12.5	Beheersing van operationele software							
A.12.5.1	- Software installeren op operationele systemen	Ja	Ja				1	
A.12.6	Beheer van technische kwetsbaarheden							
A.12.6.1	- Beheer van technische kwetsbaarheden	Ja	Ja			1	1	
A.12.6.2	- Beperkingen voor het installeren van software	Ja	Ja			1	1	
A.12.7	Overwegingen betreffende audits van informatiesystemen							
A.12.7.1	- Beheersmaatregelen betreffende audits van informatiesystemen	Ja	Ja				1	
A.13	A.13 Communicatiebeveiliging							
A.13.1	Beheer van netwerkbeveiliging							
A.13.1.1	- Beheersmaatregelen voor netwerken	Ja	Ja			1	1	
A.13.1.2	- Beveiliging van netwerkdiensten	Ja	Ja			1	1	
A.13.1.3	- Scheiding in netwerken	Ja	Ja			1	1	

A.13.2	Informatietransport						
A.13.2.1	- Beleid en procedures voor informatietransport	Ja	Ja		1	1	
A.13.2.2	- Overeenkomsten over informatietransport	Ja	Ja			1	
A.13.2.3	- Elektronische berichten	Ja	Ja		1	1	
A.13.2.4	- Vertrouwelijkheids- of geheimhoudingsovereenkomst	Ja	Ja	1	1	1	
A.14	A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen						
A.14.1	Beveiligingseisen voor informatiesystemen						
A.14.1.1	- Analyse en specificatie van informatiebeveiligingseisen	Ja	Ja			1	
A.14.1.2	- Toepassingsdiensten op openbare netwerken beveiligen	Nee	Nee				Alles vindt plaats in een gesloten circuit binnen AFAS
A.14.1.3	- Transacties van toepassingsdiensten beschermen	Ja	Ja			1	
A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen						
A.14.2.1	- Beleid voor beveiligd ontwikkelen	Nee	Nee				AIMS Improve ontwikkeld zelf geen software of systemen
A.14.2.2	- Procedures voor wijzigingsbeheer met betrekking tot systeem	Ja	Ja		1	1	
A.14.2.3	- Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Ja	Ja		1	1	
A.14.2.4	- Beperkingen op wijzigingen aan softwarepakketten	Ja	Ja		1	1	
A.14.2.5	- Principes voor engineering van beveiligde systemen	Nee	Nee				AIMS Improve ontwikkeld zelf geen software of systemen
A.14.2.6	- Beveiligde ontwikkelomgeving	Nee	Nee				AIMS Improve ontwikkeld zelf geen software of systemen
A.14.2.7	- Uitbestede softwareontwikkeling	Ja	Ja	1	1	1	
A.14.2.8	- Testen van systeembeveiliging	Nee	Nee				AIMS Improve ontwikkeld zelf geen software of systemen
A.14.2.9	- Systeemacceptatietests	Ja	Ja		1	1	
A.14.3	Testgegevens						
A.14.3.1	- Bescherming van testgegevens	Ja	Ja		1	1	
A.15	A.15 Leveranciersrelaties						
A.15.1	Informatiebeveiliging in leveranciersrelaties						
A.15.1.1	- Informatiebeveiligingsbeleid voor leveranciersrelaties	Ja	Ja		1	1	
A.15.1.2	- Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Ja	Ja		1	1	
A.15.1.3	- Toeleveringsketen van informatie- en communicatietechnologie	Ja	Ja		1	1	
A.15.2	Beheer van dienstverlening van leveranciers						
A.15.2.1	- Monitoring en beoordeling van dienstverlening van leveranciers	Ja	Nee		1	1	
A.15.2.2	- Beheer van veranderingen in dienstverlening van leveranciers	Ja	Ja		1	1	
A.16	A.16 Beheer van informatiebeveiligingsincidenten						
A.16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen						
A.16.1.1	- Verantwoordelijkheden en procedures	Ja	Ja		1	1	
A.16.1.2	- Rapportage van informatiebeveiligingsgebeurtenissen	Ja	Ja		1	1	
A.16.1.3	- Rapportage van zwakke plekken in informatiebeveiliging	Ja	Ja		1	1	
A.16.1.4	- Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Ja	Ja		1	1	
A.16.1.5	- Respons op informatiebeveiligingsincidenten	Ja	Ja	1	1	1	
A.16.1.6	- Lering uit informatiebeveiligingsincidenten	Ja	Ja		1	1	
A.16.1.7	- Verzamelen van bewijsmateriaal	Ja	Ja		1	1	
A.17	A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer						
A.17.1	Informatiebeveiligingscontinuïteit						
A.17.1.1	- Informatiebeveiligingscontinuïteit plannen	Ja	Ja		1	1	
A.17.1.2	- Informatiebeveiligingscontinuïteit implementeren	Ja	Ja		1	1	
A.17.1.3	- Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Ja	Ja		1	1	
A.17.2	Redundante componenten						
A.17.2.1	- Beschikbaarheid van informatieverwerkende faciliteiten	Ja	Ja		1	1	
A.18	A.18 Naleving						
A.18.1	Naleving van wettelijke en contractuele eisen						
A.18.1.1	- Vaststellen van toepasselijke wetgeving en contractuele eisen	Ja	Ja		1	1	
A.18.1.2	- Intellectuele eigendomsrechten	Ja	Ja	1	1	1	
A.18.1.3	- Beschermen van registraties	Ja	Ja		1	1	
A.18.1.4	- Privacy en bescherming van persoonsgegevens	Ja	Ja	1	1	1	
A.18.1.5	- Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja	Ja	1	1	1	
A.18.2	Informatiebeveiligingsbeoordelingen						

A.18.2.1	- Onhankelijke beoordeling van informatiebeveiliging	Ja	Ja			1	1	
A.18.2.2	- Naleving van beveiligingsbeleid en -normen	Ja	Ja			1	1	
A.18.2.3	- Beoordeling van technische naleving	Ja	Ja			1	1	