Auditdienst Rijk
Ministerie van Financiën

ADR ITGC-Kader

Versie: 1.1
Datum: 12-5-2026

IT General Controls (ITGC) kader

Het ITGC-kader is het basisraamwerk van de Auditdienst Rijk (ADR) voor IT-onderzoeken. Dit kader is bedoeld voor iedereen die werkt met de BIO2, van interne controles tot audits. Het wordt bijvoorbeeld gebruikt bij de jaarrekeningcontrole (voor de onderwerpen authenticatie-, gebruikers- en wijzigingsbeheer) en bij onderzoeken naar digitale weerbaarheid. Elk onderwerp in het ITGC-kader omvat een aantal basismaatregelen die samen een beheersingsdoel bereiken. In de nieuwe BIO2 kunnen maatregelen niet meer geïsoleerd getoetst worden; de koppeling met risicomanagement is vereist. Het kader volgt dan ook de structuur van de BIO2 door te beginnen met het toetsen van het risicomanagement (binnenste cirkel), gevolgd door de basismaatregelen die relevant zijn voor het onderzoek (buitenste cirkel).

Hoe gebruik ik het kader?

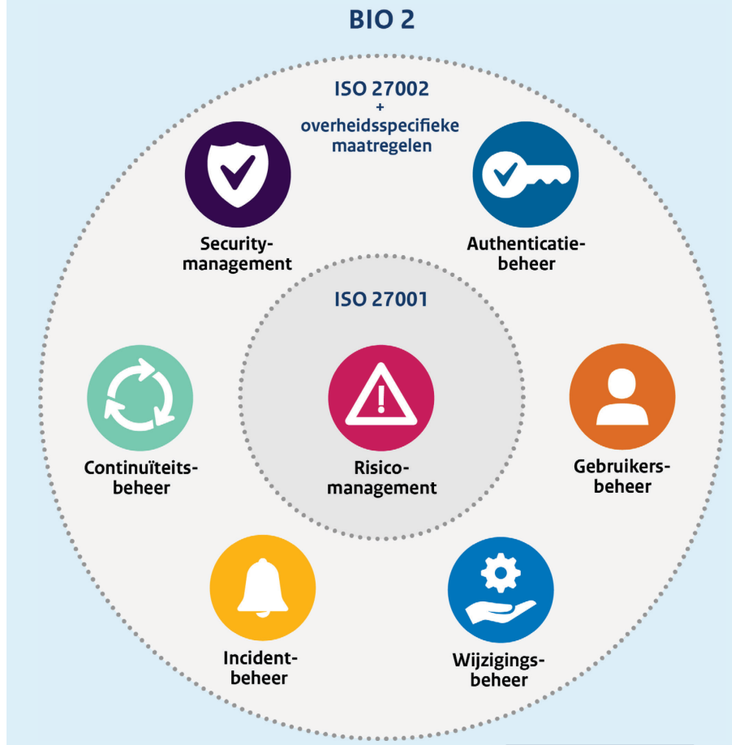
1. **Begin bij het ISMS**
   Risicomanagement is het beginpunt van het onderzoek. In het kader is hiervoor Risicobeoordeling (R1) en Risicobehandeling (R2) opgenomen. Hiermee wordt aan de hand van de ISO 27001 onderzocht hoe de organisatie risico's in kaart brengt en hoe deze vertaald zijn naar beheersmaatregelen. Dit is de binnenste cirkel van de figuur.

2. **Kies de juiste maatregelen**
   Selecteer, specifiek voor het onderzoek, welk(e) onderwerp(en) uit de buitenste cirkel je wilt onderzoeken en bepaal daarbinnen welke maatregelen relevant zijn voor het onderzoek. Deze onderwerpen zijn opgebouwd uit de beheersmaatregelen in de ISO 27002 plus de overheidsmaatregelen uit de BIO2.

3. **Controleer en pas aan**
   Vergelijk de beheersmaatregelen uit het kader met die van de organisatie.
   Voeg maatregelen of testcriteria toe of pas deze aan waar nodig. Stem de gekozen maatregelen en testcriteria met de organisatie af.

4. **Voer het onderzoek uit**
   Gebruik de testcriteria om te bepalen hoe de organisatie er voor staat. Maak bevindingen en/of conclusies bij elk onderwerp inzichtelijk, stem af en rapporteer.

Welke onderwerpen bevat het ITGC kader?



Aandachtspunten

Het ITGC-kader bevat een selectie van de ISO 27001, 27002 en van de overheidsmaatregelen uit de BIO2. Deze selectie is specifiek gericht op basis IT-beheer. Als aan dit kader wordt voldaan, betekent dat niet dat aan alle eisen van de BIO2 wordt voldaan.

De eerste basismaatregel van ieder onderwerp gaat over de interne beheersing, waar de auditor werkzaamheden uitvoert of de organisatie zelf bestaan/werking van de beheersingsmaatregel(en) vaststelt (Attest).

De overige basismaatregelen gaan over het door de auditor vaststellen van het bestaan/werking van de beheersmaatregel(en) (Direct).

Risicomanagement

Beheerproces	Beheersdoelstelling	Risico beheerproces	ID	Titel	JRC/Beheer
R1. Risicobeoordeling IB	Risicobeoordelingen worden uitgevoerd om actuele risicoprofielen met betrekking tot bedrijfsdoelstellingen te bepalen. De waarschijnlijkheid en impact van alle geïdentificeerde risico's worden regelmatig beoordeeld, met behulp van kwalitatieve en kwantitatieve methoden. De waarschijnlijkheid en impact van inherente en restrisico's worden bepaald per categorie, op portefeuillebasis.	Inherente en restrisico's worden niet (tijdig) geïdentificeerd en beoordeeld. Kans en impact zijn niet vastgesteld, waardoor actieplannen, beperkende maatregelen of risico-initiatieven niet worden ingevoerd.	R1.1	Risicocriteria in de Risicobeoordelingsprocedure	Beheer
			R1.2	Uniform uitvoeren en vastleggen risicobeoordelingen	Beheer
			R1.3	Identificeren van informatiebeveiligingsrisico’s	Beheer
			R1.4	Classificeren van informatiebeveiligingsrisico’s	Beheer
			R1.5	Prioriteren van informatiebeveiligingsrisico’s	Beheer
R2. Behandeling van IB-risico's	Beheersactiviteiten worden op alle niveaus geprioriteerd en gepland om de benodigde mitigerende maatregelen te implementeren, inclusief het bepalen van kosten en baten en de verantwoordelijkheid voor de uitvoering. Goedkeuring wordt verkregen voor aanbevolen acties en acceptatie van restrisico's en er wordt voor gezorgd dat uitgevoerde acties onder verantwoordelijkheid van betrokken proceseigenaar(s) vallen. De uitvoering van plannen wordt bewaakt en eventuele afwijkingen worden gerapporteerd aan het senior management.	Risicobeperkende maatregelen worden niet geïdentificeerd en geïmplementeerd. Vereiste acties worden niet gecommuniceerd en uitgevoerd, wat leidt tot mogelijke manifestatie van risico's. Hoge kosten/lage baten gerelateerd aan matige of lage risico's. Het niet prioriteren van risico's kan leiden tot hogere kosten, lagere uitkeringen of reputatieschade.	R2.1	Criteria voor het afhandelen van risico's	Beheer
			R2.2	Verifiëren en Selecteren van beheersmaatregelen	Beheer
			R2.3	Verantwoorden gekozen beheersingsmaatregelen	Beheer
			R2.4	Implementeren beheersmaatregelen en restrisico's accepteren	Beheer
			R2.5	Monitoren doeltreffendheid van beheersmaatregelen	Beheer

Risicomanagement R1 (1)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
R1.1	Risicocriteria in de Risico-beoordelings-procedure	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die risicocriteria voor informatiebeveiliging vaststelt en onderhoudt, waaronder: 1) de risicoacceptatiecriteria 2) criteria voor het uitvoeren van risicobeoordelingen van informatiebeveiliging	Beheersmaatregelen R1.1 t/m R1.5 samen zijn onderdeel van de "plan" fase van het ISMS. Een opzet beheersmaatregel die de criteria/eisen aan de uitvoering van risicobeoordeling en de risicoacceptatie (RISK appetite) stelt.	**R1.1.1** De Risicoacceptatiecriteria staan opgenomen in de risicobeoordelingsprocedure (Informatiebeveiligingsbeleid).	Opzet	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2a
				R1.1.2 De criteria voor het uitvoeren van de risicobeoordelingen staan beschreven in de risicobeoordelingsprocedure (Informatiebeveiligingsbeleid).	Opzet	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2a
R1.2	Uniform uitvoeren en vastleggen risico-beoordelingen	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die waarborgt dat herhaalde risicobeoordelingen van informatiebeveiliging consistente, valide en vergelijkbare resultaten opleveren.	Vervolg op **R1.1.1** er wordt een criteria eis gesteld dat er gezorgd wordt dat de risicobeoordeling consistente resultaten opleveren. Hiermee wordt bedoeld dat de resultaten van verschillende systemen te vergelijken zijn met elkaar en bij herhaaldelijk uitvoeren tot dezelfde conclusie komt.	**R1.2.1** De criteria gesteld aan de risicobeoordeling borgen dat er een uniforme werkwijze voor de uitvoer van de risicobeoordeling is.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2b
				R1.2.2 De criteria gesteld aan de risicobeoordeling borgen dat er een uniforme vastlegging is voor de uitkomsten van de beoordeling.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2b
				R1.2.3 Bij de uitgevoerde risico-beoordelingen is de uniforme werkwijze (R1.2.1) gevolgd en heeft de vastlegging (R1.2.2) conform procedure plaatsgevonden.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2b
R1.3	Identificeren van informatie-beveiligings-risico's	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die de informatiebeveiligingsrisico's identificeert: 1) pas de risicobeoordelings-procedure voor informatiebeveiliging toe om de risico's in verband met het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen het toepassingsgebied van het managementsysteem voor informatiebeveiliging te identificeren; en 2) identificeer de risico-eigenaren	Deze beheersmaatregel heeft betrekking op het uitvoeren van de risicobeoordelingsprocedure, zoals deze is onderzocht bij **R1.2.1** en **R1.2.2**. Er worden twee eisen gesteld: Eis 1: De risico's moeten geïdentificeerd worden die te maken hebben met de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie. Eis 2: De Risico-eigenaren moeten worden geïdentificeerd per risico.	**R1.3.1** De risicobeoordelingsprocedure bevat in het proces voor de risicobeoordeling: • Het classificeren aan de BIV-factoren; • dat risico's worden gekoppeld aan een risico-eigenaar.	Opzet	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2c
				R1.3.2 De uitkomsten van de te risicobeoordelingen zijn te relateren aan de BIV-factoren.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2c
				R1.3.3 Stel vast dat de risico's die voortkomen uit de risicobeoordeling zijn gekoppeld aan een risico-eigenaar.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2c

Risicomanagement R1 (2)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
R1.4	Classificeren van informatie-beveiligings-risico's	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die de informatiebeveiligingsrisico's analyseert: 1) beoordeel de potentiële gevolgen indien de risico's die in beheersmaatregel R1.3 zijn vastgesteld, zich zouden voordoen; 2) beoordeel de realistische waarschijnlijkheid dat de risico's die zijn vastgesteld in beheersmaatregel R1.3 zich voordoen; 3) stel de risiconiveaus vast.	Deze beheersmaatregel heeft betrekking op de Kans x Impact = risiconiveau berekening. In stap 1 wordt gevraagd dat de auditee de impact bepaald per risico. In stap 2 wordt de auditee gevraagd om de kans te hebben bepaald per risico. En stap 3 een risiconiveau te hebben bepaald per risico.	**R1.4.1** In de risicobeoordelingsprocedure zijn de volgende stappen onderdeel van het proces: • bepaling van de kans en impact; • en hoe het risiconiveau wordt bepaald.	Opzet	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2d
				R1.4.2 Voor de geconstateerde risico's bij **R1.3** is de kans bepaald.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2d
				R1.4.3 Voor de geconstateerde risico's bij **R1.3** is de impact is bepaald.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2d
				R1.4.4 Voor de geconstateerde risico's bij **R1.3** is het risiconiveau bepaald.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2d
R1.5	Prioriteren van informatie-beveiligings-risico's	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die de informatiebeveiligingsrisico's evalueert: 1) vergelijk de resultaten van de risicoanalyse met de risicocriteria die zijn vastgesteld in beheers-maatregel R1.1; 2) prioriteer de geanalyseerde risico's voor risico-behandeling.	Deze beheersmaatregel heeft betrekking op het komen tot een prioriteitenlijst voor de risicobehandeling (R2). • Welk risico pakt de organisatie als eerste op? Risicocriteria interpreteren wij als de risicoacceptatiecriteria waar deze risico's tegen moeten worden vergeleken door de organisatie.	**R1.5.1** In de risicobeoordelingsprocedure zijn de volgende stappen onderdeel zijn van het proces: • vergelijken van de risico's met de risicoacceptatiecriteria; • een prioriteiten bepaling maken voor de risicobehandeling.	Opzet	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2e
				R1.5.2 De resultaten van de risicoanalyse worden vergeleken met de risico-acceptatiecriteria.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2e
				R1.5.3 De resultaten van de risicoanalyse zijn geprioriteerd voor de risicobehandeling.	Bestaan/ Werking	NBA VI 3.0 - RM.02 ISO 27001/2022 - 6.1.2e

Risicomanagement R2 (1)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
R2.1	Criteria voor het afhandelen van risico's	De organisatie moet een procedure voor de behandeling van informatiebeveiligings-risico's definiëren en toepassen om passende opties voor de behandeling van informatie-beveiligingsrisico's te selecteren, rekening houdend met de resultaten van de risicobeoordeling.	Beheersmaatregelen R2.1 t/m R2.5 samen zijn onderdeel van de "do" fase van het ISMS. Er moet een procedure zijn hoe risico's worden behandeld waarin geborgd wordt dat er gepaste opties worden geselecteerd. Onder opties verstaan wij het ontwijken, mitigeren, accepteren of verzekeren. Deze procedure borgt dat op basis van de resultaten van de risicobeoordeling inzichtelijk wordt welke opties worden geselecteerd. Doorgaans wordt voor deze keuze een risicomatrix gebruikt.	**R2.1.1** Er is een procesbeschrijving voor de afhandeling van geïdentificeerde risico's met daarin: • de mogelijke opties voor het behandelen van risico's; • de stappen om te komen tot een keuze van welke risico's worden gemitigeerd en welke risico's worden geaccepteerd (bijvoorbeeld met een risicomatrix); • de stappen om na te gaan of de geselecteerde beheersings-maatregelen volledig zijn. Dit door een vergelijking te maken met de standaard beheersingsmaatregelen die in de ISO27002 staan beschreven.	Opzet	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3a
R2.2	Verifiëren en Selecteren van beheers-maatregelen	De organisatie moet een procedure voor de behandeling van informatiebeveiligings-risico's definiëren en toepassen om alle beheersmaatregelen vast te stellen die nodig zijn om de gekozen optie(s) voor de behandeling van informatie-beveiligingsrisico's te implementeren. De organisatie moet een procedure voor de behandeling van informatiebeveiligings-risico's definiëren en toepassen om de in beheersmaatregel R2.1 vastgestelde beheers-maatregelen te vergelijken met de beheersmaatregelen uit de ISO27002 en te verifiëren of er geen noodzakelijke beheersmaatregelen zijn weggelaten.	Voor de risico's waarbij de optie mitigeren is geselecteerd moeten passende beheersingsmaatregelen worden geselecteerd. De organisatie moet in zijn processen stappen hebben opgenomen waarmee het selecteren van gepaste beheersingsmaatregelen is geborgd en hoe deze maatregelen moeten worden geïmplementeerd. Organisaties kunnen beheersmaatregelen naar behoefte ontwerpen of ze uit een bepaalde bron halen. Als tweede gaat deze beheersmaatregel over het toetsen van de volledigheid van de maatregelen die worden geselecteerd. Door deze te vergelijken met de beheersingsmaatregelen uit de ISO27002 wordt inzichtelijk of er nog beheersingsmaatregelen ontbreken. Voor de jaarrekeningcontrole zijn de maatregelen op integriteit onze focus. ISO27002 bevat een lijst van mogelijke beheersmaatregelen voor informatiebeveiliging. Gebruikers van dit document worden op bijlage A in de 27001 gewezen om ervoor te zorgen dat er geen noodzakelijke beheersmaat-regelen voor informatie-beveiliging over het hoofd worden gezien.	**R2.2.1** De procesbeschrijving die voorziet in het mitigeren van geïdentificeerde risico's bevat de volgende stappen: • het selecteren van geschikte beheersings-maatregelen; • het implementeren van beheersings-maatregelen.	Opzet	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3b,c
				R2.2.2 Voor de geïdentificeerde risico's zijn passende beheersmaatregelen geselecteerd.	Bestaan/ Werking	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3b
				R2.2.3 Stel vast dat de organisatie gepaste beheersingsmaatregelen heeft getroffen bij de geïdentificeerde risico's.	Bestaan/ Werking	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3c

Risicomanagement R2 (2)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
R2.3	Verantwoorden gekozen beheersings-maatregelen	De organisatie moet een procedure voor de behandeling van informatiebeveiligings-risico's definiëren en toepassen om een verklaring van toepasselijkheid op te stellen die het volgende bevat: • de noodzakelijke beheersmaatregelen (zie R2.2); • een rechtvaardiging voor het opnemen ervan; • de informatie of de benodigde beheersmaatregelen zijn geïmplementeerd of niet; • de rechtvaardiging voor het uitsluiten van beheers-maatregelen uit de ISO27002.	Dit is het document waarin vastgelegd wordt welke maatregelen worden getroffen en waarom deze maatregelen noodzakelijk zijn. Dit hoeft niet perse een verklaring van toepasselijkheid te zijn voor onze jaarrekeningcontrole werkzaamheden, zolang de elementen maar zijn beschreven. Daarnaast legt de beheersmaatregel op dat er wordt beschreven welke beheersingsmaatregelen al zijn geïmplementeerd en welke nog geïmplementeerd moeten worden. Tot slot dat er een toelichting vereist indien er afgeweken wordt van de beheersings-maatregelen uit de ISO27002.	**R2.3.1** De procesbeschrijving die voorziet in het mitigeren van geïdentificeerde risico's bevat de stappen om een vastlegging te maken die de volgende elementen bevat: • de noodzakelijke beheersings-maatregelen; • rechtvaardiging voor het opnemen van de beheersingsmaatregelen; • informatie of de beheersings-maatregelen zijn geïmplementeerd; • een toelichting wanneer afgeweken wordt van de beheersings-maatregelen uit de ISO27002.	Opzet	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3d
				R2.3.2 Stel vast dat er vastlegging is die volgende elementen bevat: • de noodzakelijke beheersings-maatregelen; • rechtvaardiging voor het opnemen van de beheersingsmaatregelen; • informatie of de beheersings-maatregelen zijn geïmplementeerd; • een toelichting wanneer afgeweken wordt van de beheersings-maatregelen uit de ISO27002.	Bestaan/ Werking	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3d
R2.4	Implemen-teren beheers-maatregelen en restrisico's accepteren	De organisatie moet een procedure voor de behandeling van informatiebeveiligings-risico's definiëren en toepassen om: • een plan voor de behandeling van informatiebeveiligingsrisico's te formuleren; • de goedkeuring van risico-eigenaren voor het plan voor de behandeling van informatiebeveiligingsrisico's en hun acceptatie van de resterende informatiebeveiligingsrisico's te verkrijgen; • Dat de geaccepteerde risico's voorzien zijn van een einddatum.	Betreft een plan die de organisatie moet opstellen om de beheersingsmaatregelen te implementeren zodat de geïdentificeerde risico's gemitigeerd gaan worden. Dit plan van aanpak moet worden goedgekeurd door de risico eigenaar en de risico-eigenaar moet de restrisico's accepteren.	**R2.4.1** De procesbeschrijving die voorziet in het mitigeren van geïdentificeerde risico's bevat het opstellen van een plan om beheersmaatregelen te implementeren en het uitvoeren van een risicoacceptatie.	Opzet	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3e,f
				R2.4.2 De organisatie heeft een door de risico-eigenaar goedgekeurd plan opgesteld om de beheersmaatregelen te implementeren.	Bestaan/ Werking	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3e,f
				R2.4.3 De beheersmaatregelen uit het plan van **R2.3.2** zijn geïmplementeerd.	Bestaan/ Werking	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3e,f
				R2.4.4 De risico-eigenaar heeft de restrisico's geaccepteerd en voorzien van een einddatum.	Bestaan/ Werking	NBA VI 3.0 - RM.03 ISO 27001/2022 - 6.1.3e,f

Risicomanagement R2 (3)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
R2.5	Monitoren doeltreffend-heid van beheers maatregelen	De organisatie monitort, analyseert en evalueert de processen & maatregelen die voortkomen uit de behandeling van informatiebeveiligings-risico's en geaccepteerde rest risico's. (R2.4)	Bij deze beheersmaatregel ligt de focus op de processen die bij R1 en R2 zijn onderzocht en de beheersingsmaatregelen die de organisatie heeft gedefinieerd om de risico's te mitigeren.	**R2.5.1** Er is een beschrijving voor het monitoren van de geïmplementeerde beheersmaatregelen, deze bevat de volgende onderdelen: • wat moet worden gemonitord en gemeten; • de methoden voor het, monitoren, meten, analyseren en evalueren om valide resultaten te bewerkstelligen; • wanneer moet worden gemonitord en gemeten; • wie moet monitoren en meten; • wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd; • wie deze resultaten moet analyseren en evalueren.	Opzet	NBA VI 3.0 - RM.03 ISO 27001/2022 - 9.1
				R2.5.2 De activiteiten voor monitoren, meten, analyseren en evalueren zijn uitgevoerd. Stel vast; • of de monitoring en analyse conform de procedure en periodiciteit (R5.2.1) zijn uitgevoerd; • of analyse en evaluatie is uitgevoerd op de doeltreffendheid van de beheersmaatregelen; • of opvolging is gegeven indien beheersmaatregelen niet als doeltreffendheid zijn geëvalueerd; • of de risico acceptaties nog tijdig zijn.	Bestaan/ Werking	NBA VI 3.0 - RM.03 ISO 27001/2022 - 9.1

Authenticatiebeheer

Beheerproces	Beheersdoelstelling	Risico beheerproces	ID	Titel	JRC/Beheer
A1. Authenticatiebeheer	De beheersmaatregelen waarborgen met redelijke mate van zekerheid dat systemen voor authenticatiebeheer interactief behoren te zijn en dat wachtwoorden van geschikte kwaliteit worden gekozen.	Als authenticatiebeheer niet effectief is, dan kan een account worden misbruikt om handelingen te kunnen verrichten waar de betreffende persoon niet voor bevoegd is, waardoor application controls worden omzeild, aangepast of verwijderd of de integriteit van de data wordt aangetast.	A1.1	Monitoren van authenticatie	JRC & Beheer
			A1.2	Multi-factor authenticatie (MFA)	JRC & Beheer
			A1.3	Vergrendeling bij inactiviteit	JRC & Beheer
			A1.4	Wijzigen wachtwoorden systeem-/ beheeraccounts	JRC & Beheer
			A1.5	Wachtwoorden zijn van adequate sterkte	JRC & Beheer
			A1.6	Versleuteld opslaan van wachtwoorden	JRC & Beheer
			A1.7	Blokkeren account na foutieve inlogpogingen	JRC & Beheer

Authenticatiebeheer (1)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
A1.1	Monitoren van authenticatie	De organisatie houdt zelf toezicht op de naleving van de eisen voor authenticatie. Daarvoor voert het periodieke controles uit zoals het evalueren van ingestelde wachtwoordeisen, beoordelen van uitgevoerde risico-afwegingen en op basis hiervan gemaakte inrichtingskeuzes. De uitkomsten van de evaluaties en de opvolging daarvan worden vastgelegd.	Deze beheersmaatregel is een deel van het ISMS in werking, maar dan specifiek ingezoomd op de onderwerpen van de beheersmaatregelen van A1.2 t/m A1.7. Controle dient uitgevoerd te worden op applicatie, database en OS niveau. Deze beheersmaatregel is gebaseerd op de onderliggende beheersmaatregelen van Authenticatiebeheer en focust zich op de controle vanuit de tweedelijn. Derhalve zijn de referenties bij deze beheers-maatregelen ook van toepassing op A1.1. De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**A1.1.1** Er is een procedure waarin de uit te voeren periodieke controles op de inrichting van de authenticatie zijn vastgelegd. Deze is gebaseerd op een risicoafweging en bevat minimaal: • de uit te voeren controlewerk-zaamheden • de interval periodes (minimaal jaarlijks) • wijze van vastlegging • wijze van rapportering • de verantwoordelijkheden voor omgang met de bevindingen • escalatiepaden bij niet oplossen van bevindingen.	Opzet	
				A1.1.2 Minimaal de volgende aspecten zijn beoordeeld: • Uitvoer en actualisatie van risicoanalyses op basis waarvan authenticatie wordt ingericht • MFA voor Inloggen accounts met beheerrechten • Voldoen van wachtwoordinstellingen aan de eisen die komen uit de risico-analyse • Toegang en beheer met accounts die zijn uitgezonderd van het wachtwoordbeleid.	Bestaan/ Werking	
				A1.1.3 Er wordt opvolging gegeven aan de evaluatie en de uitkomsten zijn vastgelegd.	Bestaan/ Werking	
A1.2	Multi-factor authenticatie (MFA)	Pas multi-factor authenticatie (MFA) toe ten minste voor het primaire aanloggen op de digitale werkomgeving, bij accounts voor via het internet bereikbare voorzieningen en accounts die beheerrechten hebben en in andere situaties waar uit de risicoanalyse blijkt dat dit een passende oplossing is. Indien MFA niet mogelijk is voor deze accounts, zijn mitigerende maatregelen getroffen in afstemming met de CISO en met goedkeuring door de proceseigenaar.	De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**A1.2.1** Er is beleid dat voorziet in toepassing voor multi-factor authenticatie (MFA) voor ten minste het primaire aanloggen op de digitale werkomgeving, bij accounts voor via het internet bereikbare voorzieningen en accounts die beheer-rechten hebben en in andere situaties waar uit de risicoanalyse blijkt dat dit een passende oplossing is.	Opzet	BIO2 - 5.17.01
				A1.2.2 Er is een risico-analyse uitgevoerd waarmee bepaald is of twee-factor authenticatie een passende oplossing is voor de applicatie. Zo ja dan wordt twee-factor authenticatie ook afgedwongen. Zo niet, stel vast dat mitigerende maatregelen zijn getroffen die zijn afgestemd met de CISO/systeemeigenaar.	Opzet	BIO2 - 5.17.01
				A1.2.3 Indien het systeem via internet bereikbaar is, wordt twee-factor authenticatie toegepast.	Bestaan/ Werking	BIO2 - 5.17.01
				A1.2.4 Accounts met beheerrechten loggen in met twee-factor authenticatie.	Bestaan/ Werking	BIO2 - 5.17.01

Authenticatiebeheer (2)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
A1.3	Vergrendeling bij inactiviteit	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een passende periode.	De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**A1.3.1** De periode totdat de toegang tot de applicatie wordt vergrendelt is gebaseerd op een risicoafweging en is gedocumenteerd.	Opzet	BIO2 - 7.07
				A1.3.2 De ingestelde periode voor vergrendeling is conform de risicoafweging.	Bestaan/ Werking	BIO2 - 7.07
A1.4	Wijzigen wachtwoorden systeem-/ beheer-accounts	Alle wachtwoorden van systeem-/beheeraccounts die uitgezonderd zijn van het algemene wachtwoordbeleid dienen periodiek te worden gewijzigd wanneer dat nodig is, bijv. na een beveiligings-incident. Voor initiële wachtwoorden (bijvoorbeeld bij een nieuw account voor een eindgebruiker) dient deze wijziging al direct bij het eerste gebruik afgedwongen te worden. Daarnaast moet worden voorkomen dat wachtwoorden hergebruikt kunnen worden. Bij toegang vanuit een vertrouwde zone mag op basis van een risicoafweging voor **A1.1.1** afgeweken worden.	Voor testcriteria **A1.4.3** denk ook aan de standaard wachtwoorden van de gebruikers die meegeleverd zijn door de fabrikant. Deze initiële wachtwoorden dienen ook veranderd te zijn. **G2.5.4** De mogelijkheid bestaat dat dit proces overeenkomt met het proces dat bij A.1.4.2 is getoetst. Bij G2.5.4 ligt de focus op er geen misbruikt is gemaakt met de verhoogde rechten account. Bij A.1.4.2 ligt de focus op of er terecht toegang is verkregen tot het account. De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**A1.4.1** De eisen voor het wijzigen van wachtwoorden voor systeem-/ beheer-accounts zijn gebaseerd op een risicoafweging en zijn gedocumenteerd.	Opzet	ISO 27002/2022 - 5.17
				A1.4.2 Indien wachtwoorden voor systeem-/beheeraccounts zijn uitgezonderd van het algemene wachtwoordbeleid zijn er aanvullende procedures aanwezig (bijvoorbeeld enveloppe procedure of logging) en worden deze nageleefd.	Opzet	ISO 27002/2022 - 5.17
				A1.4.3 Initiële wachtwoorden dienen direct bij het eerste gebruik gewijzigd te worden.	Bestaan/ Werking	ISO 27002/2022 - 5.17
				A1.4.4 Het hergebruik van wachtwoorden dient voorkomen te worden.	Bestaan/ Werking	ISO 27002/2022 - 5.17 BIO2 - 5.17.03
A1.5	Wachtwoorden zijn van adequate sterkte	Een wachtwoord moet een minimumlengte hebben en van voldoende complexiteit zijn in overeenstemming met de eisen die de organisatie heeft bepaald.	Bekijk hier de best practices of de adviezen vanuit de leverancier. De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**A1.5.1** De eisen voor de sterkte van wachtwoorden zijn gebaseerd op een risicoafweging en zijn gedocumenteerd.	Opzet	ISO 27002/2022 - 5.17 BIO2 - 5.17.03
				A1.5.2 De ingestelde minimale wachtwoordlengte en de complexiteitseisen zijn conform de risicoafweging.	Bestaan/ Werking	ISO 27002/2022 - 5.17 BIO2 - 5.17.03
A1.6	Versleuteld opslaan van wachtwoorden	Wachtwoorden mogen niet in originele vorm (plaintext) worden opgeslagen, maar dienen in plaats daarvan versleuteld te worden.	De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**A1.6.1** De eisen voor het versleuteld/ gehashed opslaan van wachtwoorden en de toegang tot bestanden met wachtwoorden zijn gebaseerd op een risicoafweging en zijn gedocumenteerd.	Opzet	ISO 27002/2022 - 5.17 BIO2 - 8.24.04
				A1.6.2 De versleuteling/hashing van wachtwoorden is conform de risicoafweging en is gebaseerd op de actuele adviezen van het NCSC en de Unit Weerbaarheid van de AIVD.	Bestaan/ Werking	ISO 27002/2022 - 5.17 BIO2 - 8.24.04
				A1.6.3 Toegang tot het bestand met wachtwoorden is beveiligd conform de risicoafweging en passend bij de data waartoe toegang verkregen kan worden.	Bestaan/ Werking	ISO 27002/2022 - 5.17

Authenticatiebeheer (3)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
A1.7	Blokkeren account na foutieve inlogpogingen	Het aantal inlogpogingen en de tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is bepaald middels een risico overweging en is vastgelegd.	Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) is een soort veiligheidsmaatregel die bekend staat als challenge-response-authenticatie. Captcha helpt bij de bescherming tegen spam en ontsleuteling van wachtwoorden doordat u een eenvoudige test moet uitvoeren waarmee u aantoont dat u een mens bent en geen computer die probeert in te breken in een met een wachtwoord beschermd account. De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**A1.7.1** De eisen voor het blokkeren en vrijgeven van accounts zijn gebaseerd op een risicoafweging en zijn gedocumenteerd.	Opzet	ISO 27002/2022 - 8.5
				A1.7.2 Het blokkeren van accounts vindt plaats conform de risicoafweging.	Bestaan/ Werking	ISO 27002/2022 - 8.5

Gebruikersbeheer

Beheerproces	Beheersdoelstelling	Risico beheerproces	ID	Titel	JRC/Beheer
G1. Gebruikersbeheer	De beheersingsmaatregelen waarborgen dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen.	Als gebruikersbeheer niet effectief is kunnen gebruikersaccounts in omloop zijn die te ruime of verkeerde bevoegdheden hebben waardoor functiescheiding wordt doorbroken, application controls worden omzeild, aangepast of verwijderd of de integriteit van de data wordt aangetast.	G1.1	Monitoren van gebruikersbeheer	JRC & Beheer
			G1.2	Gebruikers en beheerders hebben alleen de toegangsrechten die voor hun functie noodzakelijk zijn	JRC & Beheer
			G1.3	Goedkeuring en functiescheiding bij toekennen autorisaties	JRC & Beheer
			G1.4	Tijdig verwerken functiewijzigingen en uitdiensttredingen	JRC & Beheer
			G1.5	Generieke accounts en accounts met verhoogde rechten zijn zo veel mogelijk beperkt en verklaard	JRC & Beheer

Gebruikersbeheer (1)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
G1.1	Monitoren van gebruikers-beheer	De organisatie houdt zelf toezicht op het gebruikers-beheer. Daarvoor voert het periodieke controles uit zoals het minimaal jaarlijks evalueren van toegangsrechten van gebruikers en beheerders op onderliggende componenten. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau. De uitkomsten van de evaluatie en de opvolging daarvan worden vastgelegd.	Deze beheersmaatregel is een deel van het ISMS in werking, maar dan specifiek ingezoomd op de onderwerpen van de beheersmaatregelen van G1.2 t/m G1.5. Let op dat de uitgegeven rechten de selectiebron zijn voor de controle. Deze beheersmaatregel is gebaseerd op de onderliggende beheersmaatregelen van Gebruikersbeheer en focust zich op de controle vanuit de tweedelijn. Derhalve zijn de referenties bij deze beheersmaatregelen ook van toepassing op **G1.1**. De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**G1.1.1** Er is een procedure waarin de uit te voeren periodieke controles op toegangsrechten en gebruikersaccounts zijn vastgelegd. Deze is gebaseerd op een risicoafweging en bevat minimaal: • de uit te voeren controlewerkzaamheden • de interval periodes (minimaal jaarlijks) • wijze van vastlegging • wijze van rapportering • de verantwoordelijkheden voor omgang met de bevindingen • escalatiepaden bij niet oplossen van bevindingen	Opzet	BIO2 - 5.18.02
				G1.1.2 Minimaal de volgende aspecten zijn beoordeeld: • Accounts (zijn medewerkers nog in dienst/werkzaam in hun functie?) • Toegangsrechten (passen de toegangsrechten nog bij de taken van de medewerker?) • Functiescheiding (wordt functiescheiding doorbroken?) • Niet persoonsgebonden accounts (zijn deze accounts beperkt en verklaard?) • Naleving procedures (functiescheiding tussen gebruiker en goedkeurder, functiescheiding tussen goedkeuren, doorvoeren en controleur, toekenning conform autorisatiematrix) • Monitoring vindt plaats op het gebruik van accounts met hoge rechten en het toekennen van hoge rechten	Bestaan/ Werking	
				G1.1.3 Er wordt opvolging gegeven aan de evaluatie en de uitkomsten zijn vastgelegd.	Bestaan/ Werking	
G1.2	Gebruikers en beheerders hebben alleen de toegangs-rechten die voor hun functie noodzakelijk zijn	Gebruikers en beheerders krijgen slechts toegang tot functionaliteit (rol) die zij uit hoofde van hun functie nodig hebben waarbij functie-vermenging wordt uitgesloten (need to know, need to use). Daartoe is een beschrijving beschikbaar welke rollen en rechten per applicatie bij een functie horen. Hierbij is het van belang dat ongewenste functievermenging (conflicterende rechten) zowel binnen een applicatie als over applicaties heen wordt voorkomen.	Bij **G1.2.3** controleer je of gebruikers de juiste rollen hebben conform autorisatie-matrix en functiescheidings-matrix. Gezien de complexiteit van gebruikersbeheer bij grote ERP systemen, is het gebruik van monitoringstool randvoorwaardelijk (denk hierbij aan GRC tooling). Bij **G1.2.4** is het niet mogelijk om voor alle rollen inhoudelijk vast te stellen dat deze enkel over de autorisaties beschikken zoals deze in opzet zijn beschreven. Selecteer daarom in afstemming met de accountant enkele kritische rollen en ga voor deze rollen na of deze uitsluitend beschikken over de autorisaties zoals deze in opzet zijn beschreven. Maak hiervoor indien beschikbaar gebruik van door de organisatie zelf uitgevoerde test. Om een goed autorisatiebeheer te kunnen inrichten is een actuele autorisatiematrix en functiescheidingsmatrix een noodzaak. In de ISO en de BIO worden deze matrices niet specifiek benoemd. Een vervangend middel is ook mogelijk.	**G1.2.1** Er is een autorisatiematrix aansluitend op het autorisatieconcept van het systeem waarin is vastgelegd welke toegangsrechten horen bij elke functie. Hierin zijn alle functies en toegangsrechten/ autorisaties opgenomen. Denk hierbij aan eindgebruikers en functioneel applicatiebeheerders.	Opzet	BIO2 - 5.15 ISO 27002/2022 - 5.18
				G1.2.2 Er is een functiescheidingsmatrix aanwezig waarin is vastgelegd welke functievermenging (conflicterende rechten/rollen) ongewenst is.	Opzet	BIO2 - 5.03 ISO 27002/2022 - 5.18
				G1.2.3 Gebruikers hebben slechts toegang tot de functionaliteit (autorisaties) die zij uit hoofde van hun functie nodig hebben, daarbij wordt functiescheiding niet doorbroken (conform autorisatie- en functiescheidingsmatrix).	Bestaan/ Werking	BIO2 - 5.18 BIO2 - 8.03 BIO2 - 8.03.02 ISO 27002/2022 - 5.3
				G1.2.4 De autorisatierollen beschikken over de autorisaties die in opzet zijn beschreven.	Bestaan/ Werking	BIO2 - 8.03.02

Gebruikersbeheer (2)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
G1.3	Goedkeuring en functie-scheiding bij toekennen autorisaties	Het verlenen en muteren van gebruikersaccounts en toegangsrechten vindt plaats na goedkeuring door een bevoegde functionaris. Er is een actueel mandaat-register aanwezig waaruit blijkt welke personen beslissende bevoegdheden hebben voor het verlenen van een bepaald type (niveau) toegangsrechten dan wel functieprofielen. Daarnaast bestaat er functiescheiding tussen het autoriseren en doorvoeren van wijzigingen in gebruikersaccounts en toegangsrechten.		**G1.3.1** Er is een actuele procedure voor het toekennen van autorisaties. Deze voorziet in functiescheiding en maatregelen om het toekennen conform het need to know principe te borgen.	Opzet	BIO2 - 5.16.01
				G1.3.2 Er is een actueel overzicht waarin staat wie bevoegd is om toegangsrechten te verlenen.	Bestaan/ Werking	BIO2 - 5.16.01 ISO 27002/2022 - 5.18a
				G1.3.3 Een bevoegde functionaris heeft goedkeuring gegeven voor het verlenen en muteren van gebruikersaccounts en toegangsrechten.	Bestaan/ Werking	BIO2 - 5.16.01 BIO2 - 5.18 ISO 27002/2022 - 5.18a
				G1.3.4 Het aanmaken van een account/toekennen van de toegangsrechten is pas gebeurd nadat de aanvraag is goedgekeurd.	Bestaan/ Werking	ISO 27002/2022 - 5.18g
				G1.3.5 De autorisaties voor het account zijn conform de aanvraag toegevoegd.	Bestaan/ Werking	BIO2 - 5.18 ISO 27002/2022 - 5.18a
				G1.3.6 Er is functiescheiding tussen het autoriseren en doorvoeren van wijzigingen in gebruikersaccounts en toegangsrechten.	Bestaan/ Werking	BIO2 - 5.03 ISO 27002/2022 - 5.18c
G1.4	Tijdig verwerken functie-wijzigingen en uitdienst-tredingen	Functiewijzigingen en uitdiensttredingen worden bewaakt voor aanpassen van de toegangsrechten en voor intrekken van de identiteits- en authenticatiemiddelen.	**G1.4.2** Aanvullend is het voor deze beheersmaatregel ook aan te bevelen om een analyse te maken of actieve accounts die 90 dagen niet meer gebruikt zijn worden verwijderd of worden gedeactiveerd.	**G1.4.1** Er is een procedure die voorziet in beheersmaatregelen om tijdig intrekken van rechten bij functiewijziging of uitdiensttreding te borgen.	Opzet	BIO2 - 5.16.01 ISO 27002/2022 - 5.18d
				G1.4.2 Toegangsrechten (en eventueel gebruikersaccount) van de medewerker zijn tijdig ingetrokken.	Bestaan/ Werking	BIO2 - 5.16.01 ISO 27002/2022 - 5.18d

Gebruikersbeheer (3)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
G1.5	Generieke accounts en accounts met verhoogde rechten zijn zo veel mogelijk beperkt en verklaard	Het aantal (generieke) accounts met verhoogde rechten is beperkt en verklaard, en staat in logische verhouding tot de beheerders en of ICT afdeling. Procedures voorzien erin dat handelingen altijd te herleiden zijn naar één verantwoordelijke.	Het gaat hier zowel om persoonsgebonden (beheer)accounts met verhoogde rechten als systeemaccounts waaraan verhoogde rechten zijn toegekend. Controle dient plaats te vinden op zowel de accounts waaraan verhoogde rechten zijn toegekend als het gebruik van deze accounts. **G1.5.4** De mogelijkheid bestaat dat dit proces overeenkomt met het proces dat bij A.1.1.3 is getoetst. Bij G1.5.4 ligt de focus op dat er geen misbruik is gemaakt met het verhoogde rechten account. Bij A.1.1.3 ligt de focus op of er terecht toegang is verkregen tot het account. De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**G1.5.1** Er is beleid voor omgang met speciale toegangsrechten. Dit voorziet in maatregelen om verhoogde rechten beperkt en beheerst uit te geven.	Opzet	BIO2 - 8.02
				G1.5.2 Er zijn procedures aanwezig voor het gebruik van generieke accounts (zoals systeem-, service, interface accounts) waardoor handelingen te herleiden zijn en risico's geminimaliseerd en beheerst worden. Deze procedures worden nageleefd.	Opzet	BIO2 - 5.16.02
				G1.5.3 Het aantal (generieke) accounts met verhoogde rechten is beperkt en verklaard. Let bijvoorbeeld op accounts met de mogelijkheid tot het muteren van gebruikersrechten en controleer of dit aantal in verhouding staat tot het aantal beheerders.	Bestaan/ Werking	BIO2 - 8.02
				G1.5.4 Beoordeling vindt minimaal ieder kwartaal plaats van: • actieve accounts met verhoogde rechten • toewijzen en intrekken van verhoogde rechten. Indien wijzigingen ongeautoriseerd zijn, is dit een informatie-beveiligingsincident en wordt dit als zodanig vastgelegd en afgehandeld.	Bestaan/ Werking	BIO2 - 8.02.01 BIO2 - 5.18.01
				G1.5.5 Toegang van externe leveranciers vind uitsluitend plaats onder voorwaarden, die op basis van een risicoafweging zijn opgesteld.	Bestaan/ Werking	BIO2 - 8.05.01

Wijzigingsbeheer

Beheerproces	Beheersdoelstelling	Risico beheerproces	ID	Titel	JRC/Beheer
W1. Wijzigingsbeheer	De beheersingsmaatregelen waarborgen dat wijzigingen (inclusief datafixes) in de informatiesystemen op een gecontroleerde wijze worden uitgevoerd om het risico op ongeautoriseerde wijzigingen in de informatiesystemen te voorkomen.	Als wijzigingsbeheer niet effectief is, kan een wijziging kwetsbaarheden, fouten of ongewenste functionaliteiten aanbrengen in de productie omgeving die de werking van de application controls of de integriteit van de data aantast.	W1.1	Monitoren van wijzigingsbeheer	JRC & Beheer
			W1.2	Testen wijzigingen	JRC & Beheer
			W1.3	Goedkeuren wijzigingen met inachtneming van testresultaten	JRC & Beheer
			W1.4	Functiescheiding tussen goedkeuren en doorvoeren van wijzigingen	JRC & Beheer
			W1.5	Borging voorkomen en signaleren wijzigingen buiten regulier proces om	JRC & Beheer

Wijzigingsbeheer (1)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
W1.1	Monitoren van wijzigings-beheer4	De organisatie houdt zelf toezicht dat wijzigingen, inclusief datafixes juist, tijdig en volledig worden doorgevoerd. Daarvoor voert het periodieke controles naar bijvoorbeeld wijzigingen die buiten het reguliere proces om zijn doorgevoerd of wijzigingen die ongeautoriseerd zijn doorgevoerd naar de productie omgeving. Het interval is beschreven in het beleid en is bepaald op basis van het risiconiveau. De uitkomsten van de evaluatie en de opvolging daarvan worden vastgelegd.	Deze beheersmaatregel is een deel van het ISMS in werking, maar dan specifiek ingezoomd op de onderwerpen van de beheersmaatregelen van W1.2 t/m W1.5. Let op dat de organisatie bij de controle op wijzigingen een juiste en volledige populatiebron heeft gebruikt. Als er bij het trekken van de populatie niet gebruik kan worden gemaakt van logging, maar alleen van het registratie systeem, dan loop je het risico dat je niet alle changes in scope hebt. Dus kijk dan bij W1.5 of de organisatie hiervoor beheersmaatregelingen voor heeft, voordat je verdere werkzaamheden uitvoert. Indien niet, stem dan aanpak wijzigingsbeheer verder af met accountant. Deze beheersmaatregel is gebaseerd op de onderliggende beheersmaatregelen van wijzigingsbeheer en focust zich op de controle vanuit de tweedelijn. Derhalve zijn de referenties bij deze beheers-maatregelen ook van toepassing op W1.1.	**W1.1.1** De organisatie heeft in opzet beschreven hoe controles op het wijzigingsbeheer uitgevoerd worden en wat de periodiciteit is van deze controles.	Opzet	
				W1.1.2 Periodiek wordt door de organisatie beoordeeld of • wijzigingen/datafixes conform het proces zijn verlopen (functie-scheiding, mandaat autoriseerder en goedkeurder, vastlegging (logging) en uitvoer tests) • er wijzigingen/datafixes zijn die buiten het proces om zijn doorgevoerd en derhalve niet geregistreerd zijn, bijvoorbeeld door logreview. • stel vast dat de gebruikte populatie voor deze controles volledig en juist is.	Bestaan/ Werking	ISO 27002/2022 - 6.8
				W1.1.3 Correctieve acties zijn door de organisatie ondernomen indien er naar aanleiding van de periodieke controle oneigenlijke wijzigingen zijn gesignaleerd.	Bestaan/ Werking	
W1.2	Testen wijzigingen	Wijzigingen worden getest in een andere omgeving dan de productieomgeving. Bij het testen is aandacht voor de belangrijkste bedrijfskritische functionaliteiten (denk hierbij aan een testscript of testplan).	Neem voor het wijzigingsbeheer ook datafixes mee in de beoordeling indien dit van toepassing is bij de organisatie. Indien de organisatie niet zelf de datafixes uitvoert, heeft de organisatie dan afspraken gemaakt met de service-organisatie over: • de onderlinge rolverdeling • de administratie van datafixes • de risico-afweging • testen • goedkeuring van datafixes en vastlegging daarvan • logging van datafixes • termijn en controle van de logging. Bij Agile systeemontwikkeling kan het testen van een wijziging ook vastgelegd zijn in bijv. Jira wanneer het om de ontwikkeling van een user story gaat. Daarnaast kunnen de testresultaten blijken uit de logging van de geautomati-seerde (test)tooling. Bij geautomatiseerd testen is het dan wel van belang dat je ziet welke scope wordt gehanteerd. **W1.2.3** De BIO is geschreven vanuit IB perspectief. Voor de jaarrekening zijn de functionele aspecten ook belangrijk. Let op dat bij grote releases/ patches met functionele wijzigingen testen worden uitgevoerd om vast te stellen dat de functionaliteiten (application controls) niet zijn gewijzigd.	**W1.2.1** De organisatie heeft in opzet beschreven op welke wijze wijzigingen worden getest door de organisatie.	Opzet	BIO2 - 8.32.02 BIO2 - 8.29.01
				W1.2.2 Wijziging worden in een andere omgeving dan de productieomgeving getest.	Bestaan/ Werking	BIO2 - 8.31.01 BIO2 - 8.32
				W1.2.3 Voor wijzigingen is een testscript en/of testplan aanwezig waarin de belangrijkste functionaliteiten zijn beschreven. Indien gebruik wordt gemaakt van een script, wordt dit script door een andere functionaris gereviewd. Let op dat hierbij ook aandacht is voor de functionele aspecten.	Bestaan/ Werking	BIO2 - 8.32.02 BIO2 - 8.29.01 BIO2 - 8.31.02
				W1.2.4 Wijzigingen zijn conform het testscript en/of testplan getest en het bijbehorende testresultaat is gedocumenteerd. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken. Fouten en andere afwijkingen die zich tijdens het testproces voordoen, worden vastgelegd, opgelost dan wel verklaard. Bij agile blijken de testresultaten uit de logging van de geautomatiseerde (test)tooling.	Bestaan/ Werking	BIO2 - 8.29.01 BIO2 - 8.31.02

Wijzigingsbeheer (2)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
W1.3	Goedkeuren wijzigingen met inacht-neming van testresultaten	Wijzigingen worden door een bevoegde functionaris goedgekeurd op basis van gedocumenteerde testresultaten en pas daarna doorgevoerd in de productieomgeving. Kijk bij Agile systeemontwikkeling, indien beschikbaar, ook naar de definition of done.	Bij Agile systeemontwikkeling kan goedkeuring ook het aanklikken van een vinkje zijn door de product owner in de geautomatiseerde tooling. Indien dit het geval is dan moet rekening gehouden worden met de volgende punten: • Zijn goedkeuringsstappen ingebouwd in de pipeline, denk hierbij aan merge requests (MR), pull requests (PR)	**W1.3.1** De organisatie heeft in opzet beschreven welke medewerkers (of functies) goedkeuring mogen geven op wijzigingen.	Opzet	BIO2 - 8.32.01
				W1.3.2 Een bevoegde functionaris keurt op basis van gedocumenteerde testresultaten de wijziging goed. Bij Agile systeemontwikkeling kan goedkeuring ook het aanklikken van een vinkje zijn door de product owner in de geautomatiseerde tooling.	Bestaan/ Werking	BIO2 - 8.32.01
				W1.3.3 De wijziging is pas na goedkeuring door een bevoegde functionaris in de productieomgeving doorgevoerd.	Bestaan/ Werking	BIO2 - 8.32.01
W1.4	Functie-scheiding tussen goedkeuren en doorvoeren van wijzigingen	Er dient functiescheiding te zijn ingericht tussen het goedkeuren en doorvoeren van wijzigingen om onbevoegde en onbedoelde wijzigingen te beperken. Niemand in een organisatie of proces mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een kritisch informatie-systeem te beheersen. **W1.4.4** is alleen van toepassing indien het om een zelfontwikkelde systemen gaat.	Bij Agile systeemontwikkeling is deze functiescheiding onder andere terug te zien door de prioritering op de product backlog (autorisatie), goedkeuring na testresultaten door de product owner (of bijv. een CAB) en de doorvoering door het team. Bij een Agile of DevOps omgeving kan hier ook gedacht worden aan goed autorisatie-beheer, logging en monitoring binnen de geautomatiseerde Continuous Delivery pipeline en afgedwongen procesgang naar productie. Het kan voorkomen dat een organisatie middels een Agile methode werkt en daarbij gebruik maakt van een CI/CD pipeline. Indien dit het geval is dan moet rekening gehouden worden met de volgende punten: • Audit trail voor versiebeheer. Worden alle code- en configuratiewijzigingen bijgehouden in bijvoorbeeld Github? • Worden Changelogs of release notes automatisch gegenereerd waarin de wijzigingen zijn gedocumenteerd? Voor de jaarrekeningcontrole is het belangrijkste dat er scheiding is ingericht tussen goedkeuring en doorvoeren (4-ogen principe).	**W1.4.1** De organisatie heeft in opzet beschreven hoe het wijzigingsbeheer verloopt en op welke wijze functiescheiding wordt gewaarborgd.	Opzet	BIO2 - 5.03 BIO2 - 8.18.01
				W1.4.2 Er zijn regels vastgesteld m.b.t. het veilig ontwikkelen van software en systemen.	Opzet	BIO2 - 8.25
				W1.4.3 Er is functiescheiding ingericht tussen het goedkeuren en doorvoeren van wijzigingen.	Bestaan/ Werking	BIO2 - 5.03 BIO2 - 8.18.01
				W1.4.4 De lees- en schrijftoegang voor de ontwikkelomgeving worden op passende wijze beheerd.	Bestaan/ Werking	BIO2 - 8.04
				W1.4.5 Er worden regels toegepast m.b.t. het veilig ontwikkelen van software en systemen.	Bestaan/ Werking	BIO2 - 8.25

Wijzigingsbeheer (3)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
W1.5	Borging voorkomen en signaleren wijzigingen buiten regulier proces om.	Er zijn beheersmaatregelen getroffen om te borgen dat wijzigingen buiten het reguliere change proces om naar productie kunnen worden gebracht. Tevens vindt er periodiek controle plaats om wijzigingen buiten het proces om te signaleren.	Bij Agile systeemontwikkeling is deze functiescheiding onder andere terug te zien door de prioritering op de product backlog (autorisatie), goedkeuring na testresultaten door de product owner (of bijv. een CAB) en de doorvoering door het team. Bij een Agile of DevOps omgeving kan hier ook gedacht worden aan goed autorisatie-beheer, logging en monitoring binnen de geautomatiseerde Continuous Delivery pipeline en afgedwongen procesgang naar productie. Het kan voorkomen dat een organisatie middels een Agile methode werkt en daarbij gebruik maakt van een CI/CD pipeline. Indien dit het geval is dan moet rekening gehouden worden met de volgende punten: • Audit trail voor versiebeheer. Worden alle code- en configuratiewijzigingen bijgehouden in bijvoorbeeld Github? • Worden Changelogs of release notes automatisch gegenereerd waarin de wijzigingen zijn gedocumenteerd?	**W1.5.1** De organisatie heeft beheers-maatregelen beschreven die de mogelijkheden beperken om wijzigingen buiten het proces om door te voeren. Denk aan het tijdelijk toekennen van rechten voor het doorvoeren van wijzigingen.	Opzet	BIO2 - 8.32.02 BIO2 - 8.18
				W1.5.2 De organisatie heeft beheers-maatregelen geïmplementeerd die de mogelijkheden beperken om wijzigingen buiten het proces om door te voeren. Denk aan het tijdelijk toekennen van rechten voor het doorvoeren van wijzigingen.	Bestaan/ Werking	BIO2 - 8.32.02 BIO2 - 8.18

Incidentbeheer IB

Beheerproces	Beheersdoelstelling	Risico beheerproces	ID	Titel	JRC/Beheer
I1. Incidentbeheer IB	Er is aandacht voor IB incidenten als onderdeel van beveiligingsincidenten teneinde een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligings-gebeurtenissen, te bewerkstelligen.	Indien een organisatie geen plannen heeft, en zich niet heeft voorbereid op het beheren van informatiebeveiligingsincidenten, is een organisatie bij informatiebeveiligingsincidenten niet in staat om tijdig te reageren, te communiceren en te leren van deze incidenten.	I1.1	Monitoren van incidentbeheer	Beheer
			I1.2	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Beheer
			I1.3	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Beheer
			I1.4	Reageren op informatiebeveiligingsincidenten	Beheer
			I1.5	Leren van informatiebeveiligingsincidenten	Beheer

Incidentbeheer IB (1)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
I1.1	Monitoren van incidentbeheer	De organisatie houdt zelf toezicht op de juistheid, volledigheid, tijdigheid van de incidentenregistratie en afwikkeling.	Deze beheersmaatregel is een deel van het ISMS in werking, maar dan specifiek ingezoomd op de onderwerpen van de beheersmaatregelen van I1.2 t/m I1.5. Deze beheersmaatregel is gebaseerd op de onderliggende beheersmaatregelen van Incidentenmanagement en focust zich op de controle vanuit de tweedelijn. Derhalve zijn de referenties bij deze beheersmaatregelen ook van toepassing op **I1.1**.	**I1.1.1** De organisatie heeft in opzet beschreven hoe monitoring op het incidentenbeheer uitgevoerd wordt.	Opzet	
				I1.1.2 Monitoring vindt plaats op: • Juiste, tijdige en volledige registratie van meldingen • tijdige afhandeling en melding	Bestaan/ Werking	
				I1.1.3 Correctieve acties en/of verbeteringen zijn door de organisatie ondernomen n.a.v. de monitoring.	Bestaan/ Werking	
I1.2	Plannen en voorbereiden van het beheer van informatie-beveiligings-incidenten	De organisatie behoort plannen op te stellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligings-incidenten door processen, rollen en verantwoordelijk-heden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Voor Defensie en J&V gelden andere regels voor de meldingsplicht.	**I1.2.1** Er zijn procedures voor het melden en afhandelen van beveiligingsincidenten, waarbij er specifieke aandacht is voor IB incidenten. In de procedure zijn opgenomen: • de taken en verantwoordelijkheden van het meldloket; • kennisdeling meldprocedure incidenten; • de taken, verantwoordelijken en mandaat voor het oplossen van beveiligingsincidenten; • een koppeling met crisisbeheersing (extern) en calamiteitenbeheersing (intern); • de rapportering over de opvolging van IB incidenten; • het proces om incidenten tijdig te melden bij het nationale CSIRT.	Opzet	BIO2 - 5.24.01 BIO2 - 5.24.02 BIO2 - 5.24.03 BIO2 - 5.24.04 BIO2 - 5.24.05 BIO2 - 5.24.06 BIO2 - 5.24.07
				I1.2.2 Alle medewerkers (intern en extern) hebben aantoonbaar kennisgenomen van de meldings-procedure van incidenten.	Bestaan/ Werking	BIO2 - 6.08 BIO2 - 6.08.01
I1.3	Beoordelen van en besluiten over informatie-beveiligings-gebeurtenissen	De organisatie behoort informatiebeveiligings-gebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligings-incidenten.		**I1.3.1** Het incidentbeheerproces bevat criteria voor het beoordelen, categoriseren en besluiten over informatiebeveiligingsgebeurtenissen.	Opzet	BIO2 - 5.25
				I1.3.2 Informatiebeveiligingsgebeurtenissen worden afgedaan en gecategoriseerd via het incidentbeheerproces. Ze worden indien relevant gemeld bij toezichthouders conform de bepalingen uit de betrokken wet- en regelgeving zoals de CBW en de AVG.	Bestaan/ Werking	BIO2 - 5.25.01 BIO2 - 8.16.01 BIO2 - 8.16.03

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
I1.4	Reageren op informatie-beveiligings-incidenten	Op informatiebeveiligings-incidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. Over de opvolging wordt gerapporteerd.	Er kunnen zich ook incidenten hebben voorgedaan waardoor beheersmaatregelen in de processen waarop de accountant steunt voor de jaarrekening mogelijk (tijdelijk) niet of niet goed hebben gefunctioneerd. Verkrijg inzicht of zich zulke incidenten hebben voorgedaan en wat de (mogelijke) invloed is geweest op de jaarrekening.	**I1.4.1** Het incidentbeheerproces bevat criteria voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligings-gebeurtenissen.	Opzet	BIO2 - 5.28
				I1.4.2 Op informatiebeveiligingsincidenten is gereageerd in overeenstemming met de procedures, hierbij zijn de volgende handelingen verricht: • inperken van de getroffen systemen; • zo snel mogelijk na het incident bewijs verzamelen; • escalatie met inbegrip van crisisbeheersingsactiviteiten en inroepen continuiteïtsplannen; • vastleggen responsactiviteiten voor latere analyse; • communiceren van het IB incident (of relevante details) volgens het need-to-know principe aan belanghebbenden; • postincidentanalyse uitvoeren om de oorzaak te identificeren.	Bestaan/ Werking	BIO2 - 5.26
				I1.4.3 De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	Bestaan/ Werking	BIO2 - 5.24.04
I1.5	Leren van informatie-beveiligings-incidenten	Kennis die is opgedaan met informatiebeveiligings-incidenten behoort te worden gebruikt om de beheers-maatregelen voor informatie-beveiliging te versterken en te verbeteren.	De organisatie heeft zelf criteria uitgewerkt waaraan de uitvoering van de oorzaken-analyse moet voldoen. De organisatie brengt zelf de relevante partners in kaart voor het delen van de analyses van beveiligingsincidenten.	**I1.5.1** Het incidentbeheerproces bevat criteria voor het analyseren en leren van beveiligingsincidenten. Het uitvoeren van een oorzakenanalyse en het delen van de analyses met relevante partners is onderdeel van de criteria.	Opzet	BIO2 - 5.27.01
				I1.5.2 Beveiligingsincidenten zijn geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen. Onderdeel van de analyse is een oorzakenanalyse.	Bestaan/ Werking	BIO2 - 5.27.01
				I1.5.3 De analyses van de beveiligingsincidenten zijn gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	Bestaan/ Werking	BIO2 - 5.27.02

Continuïteitsbeheer

Beheerproces	Beheersdoelstelling	Risico beheerproces	ID	Titel	JRC/Beheer
C1. Continuïteitsbeheer	De beheersingsmaatregelen waarborgen de continuïteit van de bedrijfsprocessen, verminderen het effect van onderbrekingen en maken volledig herstel mogelijk na een calamiteit.	Als de periodiciteit en de gegevens op de back-up niet aansluiten bij het belang, de back-ups niet voldoende beveiligd worden of het terugzetten niet (goed) getest wordt, dan bestaat de mogelijkheid dat de RTO en/of RPO niet behaald wordt, en kan de downtime en/of verloren data bij een calamiteit groter zijn dan wat acceptabel is voor de organisatie. Ook kan bij een calamiteit niet de juiste back-up gegevens beschikbaar zijn om terug te keren naar een werkbare situatie. Na het terugkeren tot een werkbare situatie is het mogelijk dat niet de juiste gegevens beschikbaar zijn om de bedrijfsprocessen weer volledig te hervatten.	C1.1	Monitoren van continuïteitsbeheer	Beheer
			C1.2	Uitvoeren risicoafweging voor toegestane dataverlies en hersteltijd	Beheer
			C1.3	De periodiciteit van, en het type gegevens op, de back-up sluiten aan bij het belang van de systemen	Beheer
			C1.4	De back-up gegevens worden op een veilige locatie bewaard waarbij de integriteit van de back-up geborgd blijft	Beheer
			C1.5	Periodiek testen van het terugzetten van de back-ups	Beheer
			C1.6	Beheersmaatregelen voorzien in voldoende redundantie	Beheer
			C1.7	Periodiek testen van uitwijk voorzieningen	Beheer

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
C1.1	Monitoren van continuïteits-beheer	De organisatie houdt zelf toezicht op de kwaliteit van het continuïteitsmanagement. Daarvoor voert het periodieke controles uit. Het interval hiervoor is bepaald op basis van het risiconiveau. De uitkomsten van de evaluatie en de opvolging daarvan worden vastgelegd.	Deze beheersmaatregel is een deel van het ISMS in werking, maar dan specifiek ingezoomd op de onderwerpen van de beheersmaatregelen van C1.2 t/m C1.7. Deze beheersmaatregel is gebaseerd op de onderliggende beheersmaatregelen van Continuïteitsbeheer en focust zich op de controle vanuit de tweedelijn. Derhalve zijn de referenties bij deze beheers-maatregelen ook van toepassing op **C1.1**.	**C1.1.1** De organisatie heeft in opzet beschreven hoe controles op het continuïteitsbeheer uitgevoerd worden en wat de periodiciteit is van deze controles.	Opzet	
				C1.1.2 Er is een 2e lijns controle uitgevoerd die voorziet in controle-werkzaamheden voor ten minste het: • Uitvoeren en tijdig actualiseren van risicoafwegingen ten aanzien van dataverlies, hersteltijd & back-up strategied • Vaststellen of de periodiciteit van de back-up aansluit bij de eisen van de berijfsvoering. • Vaststellen dat de back-up beveiligd is tegen onbevoegde wijzigingen • Vaststellen dat de back-up opgeslagen wordt op een locatie waarbij een incident op de ene locatie niet kan leiden tot schade op de andere. • Vaststellen of de getroffen maatregelen voor redundantie aansluiten bij de eisen die vanuit de bedrijfsvoering zijn gesteld. • Periodiek testen van terugzetten van back-ups • Periodiek testen van uitwijk	Bestaan/ Werking	
C1.2	Uitvoeren risicoafweging voor toegestane dataverlies en hersteltijd	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria. Er zijn twee referenties opgenomen waarbij 8.13.02 geld voor alle systemen. De referentie bij 5.30.02 is een aanscherping specifiek voor kritieke systemen waarbij het risico overzicht minimaal eens per 3 jaar is geactualiseerd.	**C1.2.1** Er is een actuele risicoafweging aanwezig die ten grondslag ligt aan de gemaakte afspraken over continuïteit. De afspraken zijn passend bij de risico-inschatting. De gemaakte afspraken omvatten minimaal: • Maximale toegestane dataverlies • Maximale hersteltijd na een incident	Opzet	BIO2 - 5.30.02 BIO2 - 8.13.02
C1.3	De periodiciteit van, en het type gegevens op, de back-up sluiten aan bij het belang van de systemen	De periodiciteit van de back-up dient aan te sluiten bij de maximaal toegestane periode waarover gegevens verloren mogen raken. Stel vast dat de back-up de juiste systemen en data bestanden omvat die relevant zijn voor de jaarrekening.	In C1.3.3. wordt met relevante applicaties en databases bedoeldt wat noodzakelijk is om de bedrijfsprocessen weer volledig te hervatten. Daarmee kan het bijvoorbeeld zijn dat een applicatie niet noodzakelijk is om te back-upen als deze na een nieuwe installatie direct bruikbaar is (Denk bijvoorbeeld aan een e-mail client/office applicaties).	**C1.3.1** Er zijn afspraken vastgelegd met de klant omtrent de periodiciteit, het type gegevens, de soort (OS/DB) en retentietijd van back-ups (bijvoorbeeld SLA, DAP, etc.). RPO en RTO moeten voor de keten zijn bepaald.	Opzet	BIO2 - 8.13.01
				C1.3.2 De ingestelde periodiciteit van de back-up, het type gegevens, soort back-up en retentietijd van back-ups (back-upschema) sluit aan bij de eisen vanuit de bedrijfsvoering en de keten.	Bestaan/ Werking	BIO2 - 8.13.01
				C1.3.3 De instellingen van **C1.2.1** en **C1.3.2** gelden voor alle relevante applicatie en database servers in de productie-omgeving.	Bestaan/ Werking	BIO2 - 8.13.01

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
C1.4	De back-up gegevens worden op een veilige locatie bewaard waarbij de integriteit van de back-up geborgd blijft	Stel vast, nadat in **C1.3** is bepaald dat de back-up tijdig en volledig tot stand is gekomen, op welke wijze de back-up wordt opgeslagen. Stel vast dat de opgeslagen back-up beveiligd is tegen onbevoegde wijzigingen en op dusdanige afstand van de bron is opgeslagen dat een mogelijke calamiteit bij de bron geen effect heeft op de back-up.		**C1.4.1** Er is een back-up strategie waarin is opgenomen op welke wijze back-ups worden opgeslagen, beveiligd zijn tegen onbevoegde wijzigingen en effecten op back-ups door calamiteiten worden beheerst.	Opzet	BIO2 - 8.13.01
				C1.4.2 Opgeslagen back-ups zijn beveiligd tegen onbevoegde wijzigingen waaronder ransomware-aanvallen.	Bestaan/ Werking	BIO2 - 8.13.01
				C1.4.3 Back-ups worden opgeslagen op een locatie waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	Bestaan/ Werking	BIO2 - 8.13.03
C1.5	Periodiek testen van het terugzetten van de back-ups	Om te bepalen of back-ups ook correct kunnen worden teruggezet is het van belang te bepalen of deze procedure betrouwbaar heeft gefunctioneerd. Dit dient minimaal jaarlijks te worden getest.		**C1.5.1** Er is een procedure waarin is uitgewerkt hoe getest moet worden dat back-ups terug gezet kunnen worden. De procedure voorziet in beheersmaatregelen waarmee de integriteit van de gegevens na restore van de back-up wordt gevalideerd.	Opzet	BIO2 - 8.13.04
				C1.5.2 Stel vast dat uitgevoerde tests conform de procedure zijn uitgevoerd, over de resultaten is gerapporteerd en vervolgacties zijn genomen bij eventuele bevindingen.	Bestaan/ Werking	BIO2 - 5.30
C1.6	Beheers-maatregelen voorzien in voldoende redundantie	Beheersmaatregelen voorzien in voldoende redundantie om aan de beschikbaarheidseisen te voldoen.		**C1.6.1** Getroffen maatregelen voor redundantie sluiten aan bij de eisen die vanuit de bedrijfsvoering zijn gesteld.	Opzet	BIO2 - 8.14
C1.7	Periodiek testen van uitwijk- voorzieningen	Er zijn business continuiteïts-plannen (BCP's) en disaster recovery plannen (DRP's) en deze worden minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.		**C1.7.1** Er zijn business continuïteit plannen (BCP's) en/of Disaster Recovery Plannen (DRP's) die voorzien in procedures om de uitwijk- en fallbackvoorziening in gebruik te nemen bij ernstige verstoringen of calamiteiten. De maatregelen, testfrequentie en scope sluiten aan bij de eisen die vanuit de bedrijfsvoering zijn gesteld.	Opzet	BIO2 - 5.30.01
				C1.7.2 Jaarlijks wordt de uitwijkvoorziening getest en de bruikbaarheid vastgesteld.	Bestaan/ Werking	BIO2 - 5.30 BIO2 - 5.30.01

Securitymanagement

Beheerproces	Beheersdoelstelling	Risico beheerproces	ID	Titel	JRC/Beheer
S1. Security management	De beheersmaatregelen waarborgen dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.	Als de beheersing van de infrastructuur niet effectief is, kunnen kwaadwillenden toegang krijgen tot systemen door misbruik te maken van aanwezige kwetsbaarheden waardoor application controls worden omzeild, aangepast of verwijderd of de integriteit van de data wordt aangepast.	S1.1	Monitoren van security management	Beheer
			S1.2	Analyses over dreigingen	Beheer
			S1.3	Bescherming tegen malware	Beheer
			S1.4	Beheer van technische kwetsbaarheden	Beheer
			S1.5	Beveiliging van netwerkcomponenten	Beheer
			S1.6	Netwerksegmentatie	Beheer
			S1.7	Monitoren van activiteiten	Beheer
			S1.8	Configuratiebeheer	Beheer
			S1.9	Actueel inzicht in de applicaties en onderliggende componenten	Beheer

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.1	Monitoren van security management	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	Deze beheersmaatregel is een deel van het ISMS in werking, maar dan specifiek ingezoomd op de onderwerpen van de beheersmaatregelen van S1.2 t/m S1.8. Bij testcriteria S1.1.2 staan alle onderwerpen benoemd van beheersingsmaatregelen S1.2 t/m S1.8. Niet al deze onderwerpen hoeven relevant te zijn voor jouw audit scope, derhalve het testcriteria aanpassen op basis van de behoefte. Deze beheersmaatregel is gebaseerd op de onderliggende beheersmaatregelen van Security Management en focust zich op de controle vanuit de tweedelijn. Derhalve zijn de referenties bij deze beheers-maatregelen ook van toepassing op S1.1. De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**S1.1.1** Er is een beschrijving waarin de uit te voeren periodieke controles op security management zijn vastgelegd. Deze controles zijn gebaseerd op een risicoafweging en bevatten minimaal: • de uit te voeren controlewerk-zaamheden • de interval periodes (minimaal jaarlijks) • wijze van vastlegging • wijze van rapportering • de verantwoordelijkheden voor omgang met de bevindingen • escalatiepaden bij niet oplossen van bevindingen	Opzet	BIO2 - 5.35 BIO2 - 5.35.01 BIO2 - 5.35.02 BIO2 - 5.36
				S1.1.2 Minimaal de volgende aspecten zijn uitgewerkt in een auditplan en beoordeeld: • Het proces omtrent het analyseren van dreigingen (Zijn de dreigingen verzameld uit de juiste bronnen en geanalyseerd om vast te stellen welke betekenis deze hebben voor de organisatie) • Het proces omtrent de bescherming tegen malware (Is de malware scan software bijgewerkt en worden de scans uitgevoerd) • Het proces omtrent het beheer van technische kwetsbaarheden (Worden de kwetsbaarheden scans periodiek uitgevoerd, op de juiste systemen en wordt er tijdig opvolging gegeven aan de opvolging van geconstateerde technische kwetsbaarheden). • Het proces voor het beveiligen van het netwerk (Zijn de uitgangspunten voor het logisch scheiden van het netwerk gerapporteerd). • De notables en opvolging uit het monitoringsproces zijn gerapporteerd aan het betrokken management • Het proces voor configuratiebeheer (Is de configuratie conform de baseline ingesteld).	Opzet	BIO2 - 5.35.01 BIO2 - 5.35.02
				S1.1.3 Er wordt opvolging gegeven aan de evaluatie uit **S1.1.2** en de uitkomsten zijn vastgelegd	Bestaan/ Werking	BIO2 - 5.35.01
				S1.1.4 De evaluatie van de uitkomsten zijn meegenomen in de jaarlijkse afgegeven in controle verklaring (ICV).	Bestaan/ Werking	BIO2 - 5.36.01

Securitymanagement (2)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.2	Analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreiging-en behoort te worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	De organisatie heeft een monitoring geïmplementeerd waarmee informatie wordt verzameld en geanalyseerd om mogelijke dreigingen in kaart te brengen.	**S1.2.1**: De organisatie heeft een formeel proces ingericht voor het analyseren van dreigingen. Deze bevat de periodiciteit van uitvoer (op basis van risico-inschatting), welke bronnen worden geraadpleegd en een analyse stap waarin de betekenis voor de organisatie wordt bepaald.	Opzet	BIO2 - 5.07 ISO 27002/2022 - 5.7
				S1.2.2 De beheerteams hebben een actueel inzicht in de IT-componenten t.b.v. de analyses op de dreigingen.	Bestaan/ Werking	BIO2 - 5.09.01
				S1.2.3: Activiteiten op het gebied van informatie en analyses over dreigingen zijn geïmplementeerd. Deze activiteiten bevatten: • het identificeren, doorlichten en selecteren van interne en externe informatiebronnen die nodig en geschikt zijn om te voorzien in informatie die vereist is om de gewenste informatie en analyses over dreigingen te produceren; • het verzamelen van informatie uit geselecteerde interne en externe bronnen.	Bestaan/ Werking	BIO2 - 5.07 ISO 27002/2022 - 5.7
				S1.2.4: Activiteiten op het gebied van informatie en analyses over dreigingen zijn geïmplementeerd. Informatie wordt geanalyseerd om inzicht te krijgen hoe deze verband houdt met de organisatie en de betekenis ervan voor de organisatie.	Bestaan/ Werking	ISO 27002/2022 - 5.7

Securitymanagement (3)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.3	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Deze beheersmaatregel is minimaal van toepassing voor alle Windows servers en systemen waartoe eindgebruikers toegang hebben. Voor de overige servers moet een expliciete afweging gemaakt worden. TC **1.3.1** is alleen opzet, overige TC's zijn ook bestaan en werking. Voor de opvolging van malware constateringen die uit een scan worden gerapporteerd is hier geen opvolging testcriteria opgenomen, wij gaan er vanuit dat dit als een incident wordt behandeld en daardoor bij beheersingsmaatregel **I1.2** aan bod komt. Mocht dit toch onderdeel zijn van het malware proces van jouw auditee dan moet het testcriteria worden aangevuld in lijn met het proces van de auditee.	**S1.3.1**: Het proces hoe de organisatie omgaat met malware detectie is beschreven en bevat informatie over: • Welke scansoftware wordt gebruikt; • Hoe vaak de software wordt bijgewerkt; • Lijst met toegestane software per systeem; • Lijsten die voor detectie/preventie worden gebruikt.	Opzet	BIO2 - 8.07 ISO 27002/2022 - 8.7
				S1.3.2 De beheerteams hebben een actueel inzicht in de IT-componenten t.b.v. de bescherming tegen malware.	Bestaan/ Werking	BIO2 - 5.09.01
				S1.3.3 Het downloaden van bestanden wordt beheerst en beperkt op basis van risico en need-of-use. De antimalware software beoordeeld alle downloads (bijv. een lijst maken van toegestane toepassingen (‘allowlisting’).	Bestaan/ Werking	BIO2 - 8.07.01 ISO 27002/2022 - 8.7
				S1.3.4 De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	Bestaan/ Werking	BIO2 - 8.07.03
				S1.3.5 De malwarescan wordt uitgevoerd op: • alle omgevingen, bijvoorbeeld op (mail)servers, (desktop)computers en bij de toegangsverlening tot het netwerk van de organisatie; • alle gedownloade content voorafgaand aan executie of opslag; • alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, voor gebruik of opslag in de eigen omgeving.	Bestaan/ Werking	BIO2 - 8.07.04

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.4	Beheer van technische kwetsbaar-heden	Er behoort informatie te worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behorende passende maatregelen te worden getroffen.	De organisatie moet een proces hebben ingericht waarmee technische kwetsbaarheden worden geïdentificeerd en gemitigeerd. Aandachtspunt is hierbij de prioritering van kwetsbaarheden en de bijhorende oplostermijnen. Een mogelijke oplossing kan zijn het patchen van je systeem of het aanpassen van instellingen. De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**S1.4.1** Het proces voor identificeren en mitigeren van technische kwetsbaarheden op systemen is beschreven, hierin is opgenomen: • het ontvangen van meldingen van kwetsbaarheden van leveranciers & andere bronnen die geanalyseerd, beoordeeld en/of geïmplementeerd worden; • welke instrumenten gebruikt worden om kwetsbaarheden te identificeren en op te volgen; • de periodiciteit wanneer pentesten/ vulnerability scans periodiek worden uitgevoerd; • hoe bevindingen worden opgevolgd, met daarbij aandacht voor een aanpak om bevindingen te prioriteren op basis van een risicoafweging.	Opzet	BIO2 - 8.08 ISO 27002/2022 - 8.8
				S1.4.2 De beheerteams hebben een actueel inzicht in de IT-componenten t.b.v. het beheer van technische kwetsbaarheden.	Bestaan/ Werking	BIO2 - 5.09.01
				S1.4.3 Meldingen worden ontvangen van leveranciers & andere externe bronnen van kwetsbaarheden die relevant zijn voor de systemen van de auditscope.	Bestaan/ Werking	ISO 27002/2022 - 8.8
				S1.4.4 Geïdentificeerde kwetsbaarheden worden beoordeeld en geprioriteerd (bijvoorbeeld met een CVSS score). Mitigerende maatregelen worden op basis van een expliciete risicoanalyse getroffen. Bij een hoge kans op misbruik of verwachte schade worden passende mitigerende maatregelen zo snel mogelijk, maar uiterlijk binnen een week getroffen.	Bestaan/ Werking	BIO2 - 8.08.01 BIO2 - 8.08.02 BIO2 - 8.08.03 ISO 27002/2022 - 8.8
				S1.4.5 Periodiek worden kwetsbaarheden scans/pentesten uitgevoerd. Internetfacing informatiesystemen worden continue getest op zwakheden en kwetsbaarheden, pentesten worden uitgevoerd bij elke nieuwe release of major update.	Bestaan/ Werking	BIO2 - 8.08.04 BIO2 - 8.08.05
S1.5	Beveiliging van netwerk-componenten	Netwerken en netwerk-apparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	De risicoafweging wordt bij R1 en R2 beoordeeld en kan gebruikt worden voor de invulling van de testcriteria.	**S1.5.1** Er is een operationeel beleidsdocument waarin de uitgangspunten voor het minimale vertrouwelijkheidsniveau van het netwerk en hoe de beheerders toegang gescheiden wordt van het gebruikersnetwerk staat beschreven.	Opzet	BIO2 - 8.20.01 BIO2 - 8.20.02
				S1.5.2 Netwerkcomponenten moeten minimaal voldoen aan het vertrouwelijkheidsniveau van het netwerk waarvan ze onderdeel zijn.	Bestaan/ Werking	BIO2 - 8.20.01
				S1.5.3 Toegang tot beheerinterfaces van netwerkcomponenten is gescheiden van het gebruikersnetwerk.	Bestaan/ Werking	BIO2 - 8.20.02

Securitymanagement (5)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.6	Netwerk-segmentatie	Groepen informatiediensten, gebruikers en informatie-systemen behoren in de netwerken van de organisatie te worden gesegmenteerd.	Voor **S1.6.3** geldt dat als de continuïteit van de dienstverlening belangrijk is dat je deze testcriteria meeneemt in het onderzoek.	**S1.6.1** Er is een operationeel beleidsdocument waarin de uitgangspunten van zonering zijn opgenomen. De criteria voor het segmenteren van netwerken in domeinen, en de toegang die via de gateways wordt toegestaan, zijn gebaseerd op een beoordeling van de beveiligingseisen voor elk domein en is in overeenstemming het toegangsbeveiligingsbeleid.	Opzet	BIO2 - 8.22.01 ISO 27002/2022 - 8.22 ISO 27002/2022 - 8.7
				S1.6.2 Zonering is ingericht binnen de technische infrastructuur conform de uitgangspunten uit het operationeel beleid. Hierbij is er scheiding tussen vertrouwde en onvertrouwde netwerken.	Bestaan/ Werking	BIO2 - 8.22
				S1.6.3 In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en te mitigeren.	Bestaan/ Werking	BIO2 - 8.21.01

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.7	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatie-beveiligingsincidenten te evalueren.	Monitoren is alleen relevant als er voor het onderzoek relevante risico's worden gemitigeerd met detectieve maatregelen. Dit zou uit R1 Risicobeoordeling en R2 behandeling van IB-risico's moeten blijken welke type maatregels zijn getroffen voor het mitigeren van de risico's.	**S1.7.1**: Beschreven is hoe de organisatie omgaat met het monitoren van zijn omgeving. Dit bevat minstens de volgende onderdelen: • uitgaand en inkomend netwerk-, systeem- en toepassingsverkeer; • toegang tot systemen, servers, netwerkapparatuur, monitoringsysteem, essentiële toepassingen enz.; • logbestanden van beveiligings-instrumenten [bijv. antivirus, IDS, inbraakpreventiesysteem (IPS), webfilters, firewalls, voorkoming van gegevenslekken; • logbestanden van gebeurtenissen met betrekking tot systeem- en netwerk-activiteit; • eenduidige regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Opzet	ISO 27002/2022 - 8.16 BIO2 - 8.16.02
				S1.7.2 De beheerteams hebben een actueel inzicht in de IT-componenten t.b.v. van het monitoren van activiteiten.	Bestaan/ Werking	BIO2 - 5.09.01
				S1.7.3: De volgende bronnen zijn aangesloten op de monitorings-applicatie: • uitgaand en inkomend netwerk-, systeem- en toepassingsverkeer; • toegang tot systemen, servers, netwerkapparatuur, monitoringsysteem, essentiële toepassingen enz.; • logbestanden van beveiligings-instrumenten [bijv. antivirus, IDS, inbraakpreventiesysteem (IPS), webfilters, firewalls, voorkoming van gegevenslekken]; • logbestanden van gebeurtenissen met betrekking tot systeem- en netwerkactiviteit. Deze bronnen zijn voorzien van een actuele kloksynchronisatie.	Bestaan/ Werking	BIO2 - 8.16.04 ISO 27002/2022 - 8.16 ISO 27002/2022 - 8.17
				S1.7.4: Relevante logregels bevatten minimaal de volgende informatie: • actie: De gebeurtenis of handeling die heeft plaatsgevonden; • object: waarop de gebeurtenis of handeling effect had (bijv. welk bestand, proces of systeem); • resultaat: het resultaat van de gebeurtenis of handeling, d) oorsprong: het apparaat of de netwerklocatie van waaruit de gebeurtenis of handeling in gang is gezet; • actor: identificatie van de persoon die of het proces dat de gebeurtenis in gang heeft gezet; • tijdstempel: datum en tijdstip waarop de gebeurtenis of handling plaatsvond.	Bestaan/ Werking	BIO2 - 8.15.01

Securitymanagement (7)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.7				**S1.7.5** De organisatie monitort op basis van risico-inschatting. Minimaal de volgende activiteiten worden gemonitord: • geslaagde en mislukte pogingen om toegang te krijgen tot beschermde bronnen (bijv. (DNS-)servers, webportals en bestandssystemen); • ongebruikelijk gebruikers- en systeemgedrag in vergelijking met het verwachte gedrag.	Bestaan/ Werking	ISO 27002/2022 - 8.16
				S1.7.6: De organisatie geeft adequaat en tijdig opvolging aan de activiteiten die in beheersmaatregel **S1.7.4** zijn gedetecteerd.	Bestaan/ Werking	BIO2 - 8.16.03

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.8	Configuratie-beheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	De organisatie moet in kaart hebben hoe hardware, software diensten en netwerken geconfigureerd dienen te worden. Hierbij inachtneming van leveranciers guidelines (hardening), industry best practices. Hierbij dient ook rekening te worden gehouden met het beveiligingsniveau van de desbetreffende dienst of applicatie. Wijzigingen aan configuraties behoren het wijzigings-beheerproces te volgen (zie **W1**).	**S1.8.1**: De organisatie heeft standaard sjablonen beschreven waarin de beveiligde configuraties van hardware, software, (Cloud) diensten en netwerken zijn gedefinieerd. Deze zijn opgesteld: • met behulp van openbaar beschikbare richtlijnen (bijv. vooraf gedefinieerde sjablonen van verkopers en van onafhankelijke beveiligingsorganisaties); • met inachtneming van het beveiligingsniveau dat nodig is om een afdoende beveiligingsniveau vast te stellen; • met ondersteuning van het informatiebeveiligingsbeleid van de organisatie, onderwerpspecifieke beleidsregels en normen en andere beveiligingseisen van de organisatie; • rekening houdend met de haalbaarheid en toepasselijkheid van beveiligingsconfiguraties in de context van de organisatie; • met inachtneming dat standaard authenticatie-informatie van de leverancier en andere belangrijke standaardparameters (zoals standaardwachtwoorden) onmiddellijk na de installatie worden gewijzigd.	Opzet	ISO 27002/2022 - 8.9
				S1.8.2 De beheerteams hebben een actueel inzicht in de IT-componenten t.b.v. van het configuratiebeheer.	Bestaan/ Werking	BIO2 - 5.09.01
				S1.8.3: De configuraties van hardware, software, (Cloud)diensten en netwerken is geregistreerd en geïmplementeerd conform de sjablonen. De organisatie houdt een logbestand bij van alle configuratiewijzigingen.	Bestaan/ Werking	ISO 27002/2022 - 8.9
				S1.8.4: Configuraties worden gemonitord met een uitgebreide verzameling instrumenten voor systeembeheer (bijvoorbeeld onderhoudssysteemhulpmiddelen, ondersteuning op afstand, instrumenten voor bedrijfsbeheer en back-up- en herstelsoftware) en worden regelmatig beoordeeld om de configuratie-instellingen te verifiëren, de sterkte van wachtwoorden te evalueren en de uitgevoerde activiteiten te beoordelen. Eventuele afwijkingen worden beoordeeld en aangepakt.	Bestaan/ Werking	ISO 27002/2022 - 8.9

Securitymanagement (9)

ID	Titel	Beheersmaatregel	Nadere concretisering (optioneel)	Testcriteria	Type TC	Ref
S1.9	Actueel inzicht in de applicaties en onderliggende componenten.	Er is een inventaris van bedrijfsmiddelen die van belang zijn voor informatieverwerking met inbegrip van operationele technologie. De inventaris omvat alle eigenschappen die nodig zijn voor het beheer en onderhoud. In de inventaris zijn ook opgenomen: bedrijfsmiddelen op afstand, Cloud-omgevingen en bedrijfsmiddelen die regelmatig zijn verbonden met de netwerkinfrastructuur maar niet onder controle van de organisatie staan. De volledigheid en actualiteit van de inventaris wordt periodiek gecontroleerd met tussenpozen die passend zijn voor de frequentie waarmee wijzigingen optreden.	Deze beheersmaatregel is ook opgenomen als onderdeel van de andere security management beheers-maatregelen, omdat het hebben van een CMDB vaak randvoorwaardelijk is voor het goed uitoefenen van deze beheersmaatregelen. Wij hebben hem ook nog apart opgevoerd voor de auditees waarbij het CMDB nog nadere aandacht behoeft, omdat bijvoorbeeld uit eerdere audits blijkt het CMDB niet op orde is. Een randvoorwaarde om te beoordelen of de IT-infrastructuur voldoende is beveiligd is een accuraat inzicht in de beoogde opzet van de IT-infrastructuur (de architectuur) en een actueel inzicht in de werkelijk geconfigureerde hard- en software.	**S1.9.1** De beheerteams hebben een actueel inzicht in de IT-componenten t.b.v. patchmanagement, hardening, scanning, monitoring en configuratie-management.	Bestaan/ Werking	BIO2 - 5.09.01
				S1.9.2 De volledigheid en actualiteit wordt periodiek gecontroleerd met tussenpozen die passend zijn voor de frequentie waarmee wijzigingen optreden.	Bestaan/ Werking	BIO2 - 5.09.01

Auditdienst Rijk 2026