Toegangsbeveiliging

BIO Thema-uitwerking

Mei 2026 [versie 3.0 definitief]

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.



©Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen (CC BY-NC-SA 4.0) verleend. Voor meer informatie zie: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl.

BIO Thema-uitwerking Toegangsbeveiliging

Titel	BIO Thema-uitwerking Toegangsbeveiliging
Datum	Mei 2026
Versie en status	3.0 definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	CIP-kernteamleden
Reviewers	Versie 1.0: Professionals uit het CIP-netwerk en het CIP-kernteam Versie 2.0: CIP-kernteam Versie 2.1: CIP-kernteam Versie 2.2: CIP-kernteam Versie 2.3: CIP-kernteam Versie 3.0 CIP-kernteamleden

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt. Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Wijzigingsbeheer

In de onderstaande tabel worden alle relevante wijzigingen in dit document bijgehouden, om eenvoudig inzicht te krijgen in de uitgevoerde aanpassingen.

Versie	Datum	Wijziging	Door
1.0	Maart 2021		CIP-kernteamleden
2.0	Oktober 2020	Verwijzingen op control niveau aangepast in B.04/05/06 en U.01/12N	CIP-kernteamleden
2.1	Oktober 2021	Opdrachtgever aangepast	CIP-kernteamleden
2.2	Maart 2023	Verwijzingen op control niveau aangepast in U.05/06	CIP-kernteamleden
2.3	November 2023	Tekstverbeteringen, BUC-afbeeldingen in tabelvorm, harde	CIP-kernteamleden

		enters verwijderd, doelstellingen en risico's geüniformeerd, BIO2.0-opmaat verwerkt).	
3.0	Mei 2026	BIO2 1.3 verwerkt	CIP-kernteamleden

Leeswijzer

Voorafgaand aan hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein, de kern van dit document, heeft elke BIO Thema-uitwerking een inleiding met een standaard paragraafindeling.

Aanvullend geldt:

- Voor de aanduiding van personen wordt de mannelijke vorm aangehouden (hij/hem/zijn) ongeacht het geslacht.
- De controls en maatregelen vermeld in deze thema-uitwerking zijn in het beleids-, uitvoerings- en control-domein georganiseerd, waarmee ze bij de overeenkomstige functionarissen kunnen worden geadresseerd. Deze functionarissen zijn niet benoemd omdat dit organisatie-afhankelijk is.
- Bijlagen zijn opgenomen alleen voor specifieke informatie uit hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en/of 5 Control-domein.
- Van best practices (open standaarden al dan niet toegankelijk met een licentie) zijn de meest actuele versies afgekort vermeld, tenzij de actuele versie niet toereikend is.
- Waar formuleringen uit de nieuwe BIO extra scherpte toevoegen, zijn controls en maatregelen uitgebreid met tekstgedeelten en verwijzingen uit de BIO2.0-opmaat.

Inhoudsopgave

Leeswijzer 3

1 Inleiding 7

1.1 Opzet BIO Thema-uitwerking 7

1.2 Scope en begrenzing toegangsbeveiliging 7

1.3 Context en globale structuur toegangsbeveiliging 8

2 Beveiligingsobjecten toegangsbeveiliging 10

2.1 Globale relaties tussen geïdentificeerde beveiligingsobjecten 10

2.1.1 Beleidsdomein 11

2.1.2 Uitvoeringsdomein 11

2.1.3 Control-domein 12

3 Beleidsdomein 13

3.1 Doelstelling 13

3.2 Risico's 13

3.3 Objecten, controls en maatregelen 13

3.3.1 B.01 Toegangsbeveiligingsbeleid 13

Objectdefinitie 13

Objecttoelichting 13

3.3.2 B.02 Inventarislijst en eigenaarschap 14

Objectdefinitie 14

Objecttoelichting 15

3.3.3 B.03 Beveiligingsfunctie 16

Objectdefinitie 16

Objecttoelichting 16

3.3.4 B.04 Cryptografie 17

Objectdefinitie 17

Objecttoelichting 17

3.3.5 B.05 Beveiligingsorganisatie 18

Objectdefinitie 18

Objecttoelichting 18

3.3.6 B.06 Toegangsbeveiligingsarchitectuur 19

Objectdefinitie 19
Objecttoelichting 19
4 Uitvoeringsdomein 20
4.1 Doelstelling 20
4.2 Risico's 20
4.3 Objecten, controls en maatregelen 20
4.3.1 U.01 Registratieprocedure 20
Objectdefinitie 20
Objecttoelichting 21
4.3.2 U.02 Toegangsverleningsprocedure 21
Objectdefinitie 21
Objecttoelichting 22
4.3.3 U.03 Inlogprocedure 22
Objectdefinitie 22
Objecttoelichting 22
4.3.4 U.04 Wachtwoordenbeheer 23
Objectdefinitie 23
Objecttoelichting 23
4.3.5 U.05 Speciale toegangsrechtenbeheer 24
Objectdefinitie 24
Objecttoelichting 24
4.3.6 U.06 Functiescheiding 25
Objectdefinitie 25
Objecttoelichting 25
4.3.7 U.07 Autorisatie 26
Objectdefinitie 26
Objecttoelichting 26
4.3.8 U.08 Autorisatievoorzieningen 27
Objectdefinitie 27
Objecttoelichting 27
4.3.9 U.09 Fysieke toegangsbeveiliging 27
Objectdefinitie 27

Objecttoelichting 27
5 Control-domein 29
5.1 Doelstelling 29
5.2 Risico's 29
5.3 Objecten, controls en maatregelen 29
5.3.1 C.01 Beoordelingsprocedure 29
Objectdefinitie 29
Objecttoelichting 30
5.3.2 C.02 Beoordeling toegangsrechten 30
Objectdefinitie 30
Objecttoelichting 30
5.3.3 C.03 Logging en monitoring 31
Objectdefinitie 31
Objecttoelichting 31
5.3.4 C.04 Beheersorganisatie toegangsbeveiliging 33
Objectdefinitie 33
Objecttoelichting 33
Bijlage 1: Scenario voor toegangsbeveiliging 35
Indiensttreding nieuwe medewerkers 35
Tijdens het dienstverband 37
Uitdiensttreding 37

1 Inleiding

BIO Thema-uitwerking Toegangsbeveiliging geeft overheidsorganisaties een beeld van de meest relevante onderwerpen die een rol spelen bij het inrichten en beveiligen van toegangsvoorzieningen. Dit document is geënt op controls uit de Baseline Informatiebeveiliging Overheid (BIO2) en andere best practices zoals: NEN-EN-ISO/IEC 27001:2022 (hierna genoemd ISO 27001) en NEN-EN-ISO/IEC 27002:2022 (hierna genoemd ISO 27002), The Standard of Good Practice (SoGP) 2018 en de National Institute of Standards and Technology (NIST).

1.1 Opzet BIO Thema-uitwerking

In deze BIO Thema-uitwerking zijn de objecten geïdentificeerd die een rol spelen bij toegangsbeveiliging. De objecten zijn ingedeeld in de domeinen Beleid, Uitvoering en Control (BUC), en daarbinnen naar een viertal invalshoeken. Deze objecten vormen de verschillende inhoudelijke onderwerpen van toegangsbeveiliging. Ze zijn in het document verder uitgewerkt naar controls en onderliggende maatregelen.

Deze thema-uitwerking volgt de standaard opzet voor BIO Thema-uitwerkingen:

- scope en begrenzing van de thema-uitwerking (zie paragraaf 1.2);
- context en globale structuur van de thema-uitwerking (zie paragraaf 1.3);
- globale relaties tussen de geïdentificeerde beveiligingsobjecten (zie paragraaf 2.1).

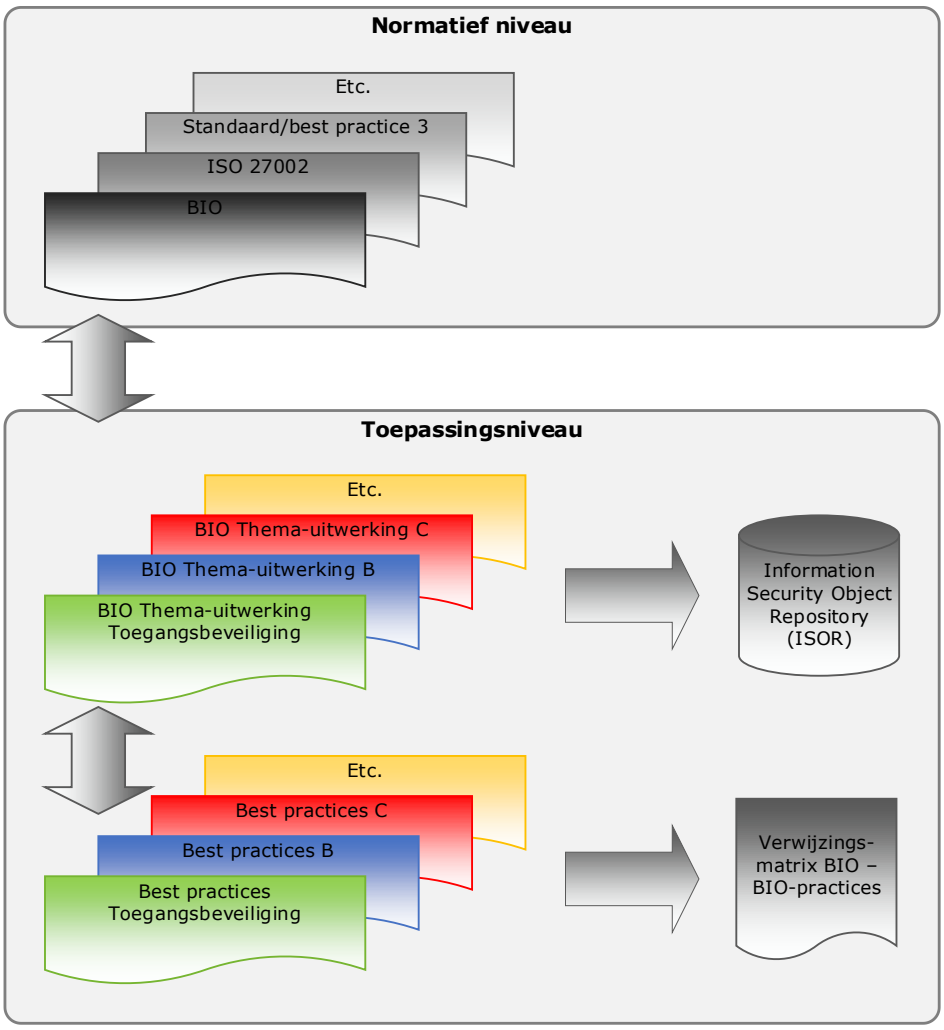
1.2 Scope en begrenzing toegangsbeveiliging

De uitwerking van logische toegangsbeveiliging is in deze BIO Thema-uitwerking gericht op identificatie, authenticatie en autorisatie van (interne en externe) medewerkers.

De uitwerking van fysieke beveiliging is in deze thema-uitwerking gericht op de fysieke toegang tot terreinen, gebouwen en ruimten (bijvoorbeeld rekencentra).

Specifieke apparaat-gebonden mechanismen voor toegangsbeveiliging, zoals toegang tot besturingssystemen, netwerken, mobiele computers en telewerken vallen buiten de scope van deze thema-uitwerking.

De begrenzing van deze BIO Thema-uitwerking is weergegeven in afbeelding 1.



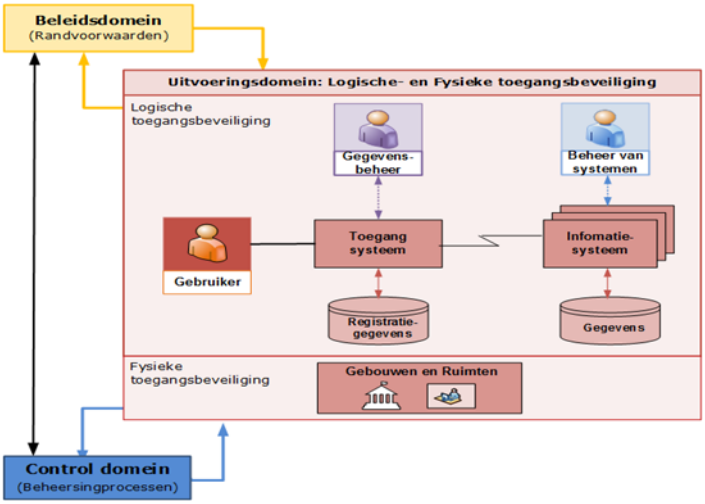
Afbeelding 1: Relatie BIO Thema-uitwerking Toegangsbeveiliging met aanpalende documenten

1.3 Context en globale structuur toegangsbeveiliging

Informatiesystemen maken gebruik van cruciale data van de organisatie zelf en van derden. Deze informatiesystemen moeten worden beveiligd en beheerst om het risico van inbreuk, misbruik en (data)diefstal te mitigeren. Toegangsbeveiliging speelt hierbij een cruciale rol. Toegangsbeveiliging richt zich op informatiesystemen (logische toegangsbeveiliging) en op gebouwen en ruimten waarin medewerkers gehuisvest zijn (fysieke toegangsbeveiliging).

Logische toegangsbeveiliging omvat het geheel van richtlijnen, procedures, beheersingsprocessen en faciliteiten die noodzakelijk zijn voor het verschaffen van toegang tot informatiesystemen, besturingssystemen, netwerken, mobiele apparaten en telewerken van een organisatie. Fysieke toegangsbeveiliging omvat het geheel van richtlijnen, procedures, beheersingsprocessen en systemen die noodzakelijk zijn voor het verschaffen van fysieke toegang tot terreinen, gebouwen en ruimten.

Zie hiervoor afbeelding 2.



Afbeelding 2: Globale opzet logische en fysieke toegangsbeveiliging

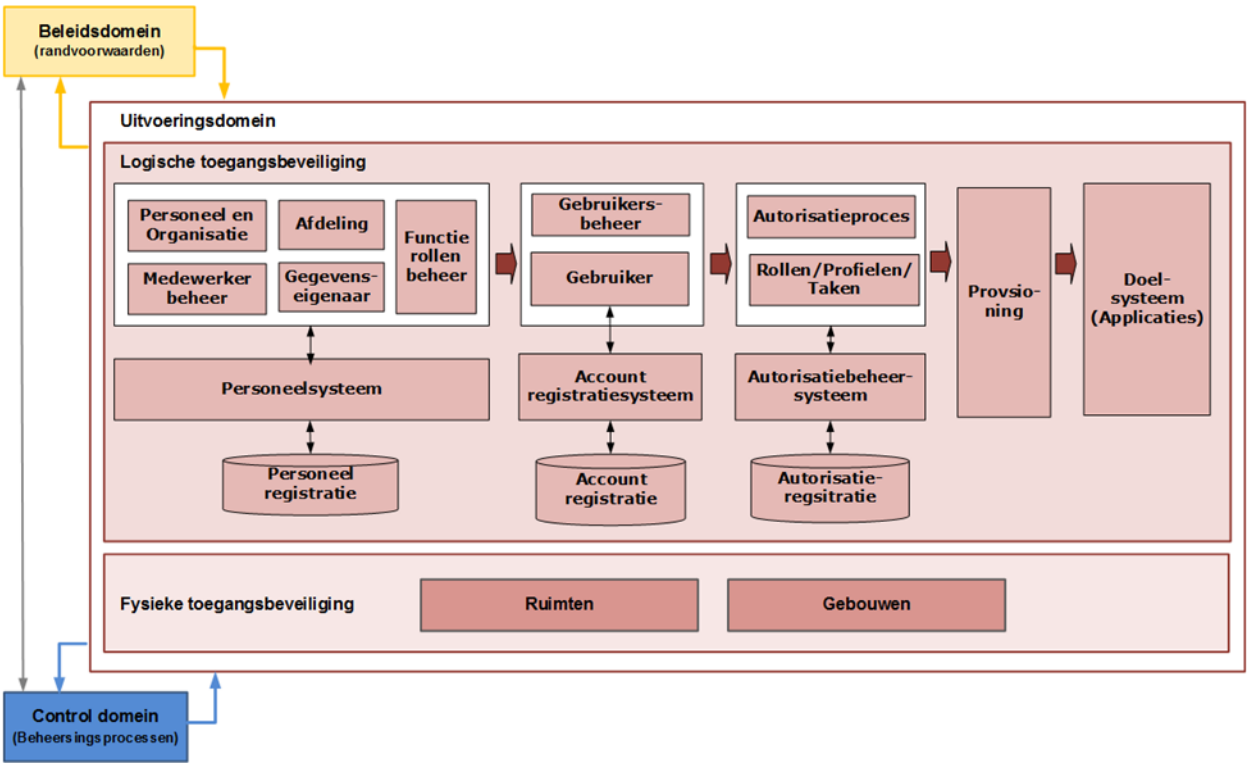
2 Beveiligingsobjecten toegangsbeveiliging

Objecten worden geïdentificeerd met onderzoeksvragen en risicogebieden. De objecten, met hun uitwerking naar controls en maatregelen, hebben tot doel risico's te mitigeren. Ze zijn afgeleid vanuit de optiek van de kwaliteitscriteria: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid (BIVC) en vervolgens ingedeeld in het beleids-, uitvoerings- en control-domein.

De vragen die hierbij een rol spelen zijn:

1. Beleidsdomein: Welke elementen spelen een rol bij de conditionering en sturing op de inrichting van toegangsbeveiliging vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?
2. Uitvoeringsdomein: Welke elementen spelen een rol bij de inrichting van toegangsbeveiliging vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?
3. Control-domein: Welke elementen spelen een rol bij de beheersing van toegangsbeveiliging vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?

Afbeelding 3 toont de positionering en het onderlinge verband van toegangsbeveiligingselementen binnen het uitvoeringsdomein. De elementen kunnen direct of indirect voorkomen als beveiligingsobjecten.



Afbeelding 3: Schematische weergave componenten toegangsbeveiliging in drielagenstructuur

2.1 Globale relaties tussen geïdentificeerde beveiligingsobjecten

De BIO is ingedeeld volgens de hoofdstukindeling van de ISO 27002. Bij het ontwikkelen van een BIO Thema-uitwerking is het noodzakelijk om na te gaan uit welke onderdelen (objecten) het thema precies

bestaat. Zonder een beeld over de samenhang tussen de objecten is het lastig om de normen in de juiste samenhang uit de BIO te selecteren.

Toegangsbeveiliging omvat het geheel van actoren, beleid, richtlijnen, procedures, processen en registratiesystemen dat nodig is voor een vertrouwd en betrouwbaar gebruik van informatiesystemen. De essentiële onderdelen van toegangsbeveiliging zijn weergegeven in afbeelding 3. Lees hieronder de toelichting van deze onderdelen per domein (beleid, uitvoering en control).

2.1.1 *Beleidsdomein*

Het beleidsdomein bevat algemene conditionele elementen voor de inrichting van de toegangsbeveiliging zoals toegangsbeleid. Het bevat ook andere conditionele en voorwaardelijke aspecten die van toepassing zijn op het uitvoeringsdomein en het control-domein. Het bevat over het algemeen de objecten: beleid, cryptografie, organisatiestructuur en architectuur.

2.1.2 *Uitvoeringsdomein*

Het uitvoeringsdomein omvat verschillende organisatieonderdelen die betrokken zijn bij de inrichting van de toegangsbeveiliging. Toegangsbeveiliging is een continu proces dat de samenwerking van deze bedrijfsonderdelen nodig heeft. Deze bedrijfsonderdelen zijn gezamenlijk verantwoordelijk voor de juiste inrichting van de beveiligingsobjecten van toegangsbeveiliging. De betrokken organisatieonderdelen zijn onder andere:

- Personeelsafdeling
  De personeelsafdeling zorgt ervoor dat medewerkers in het personeelsregistratiesysteem worden opgenomen en zorgt, in samenwerking met de business, dat vanuit een organisatorische en procedurele invalshoek elementen worden vastgelegd. De van belang zijnde elementen zijn: gegevens/proceseigenaar, gebruiker, rol, profiel en taak. De relatie tussen deze elementen kan gelezen worden als:
  - Een gebruiker heeft een rol.
  - Met deze rol wordt zijn profiel bepaald.
  - Met zijn profiel worden de rechten bepaald waarmee hij zijn taak kan uitvoeren.
- ICT-afdeling
  De ICT-afdeling zorgt voor ICT-voorzieningen en de geautoriseerde toegang tot benodigde applicaties en het authenticatiemiddel. Dit wordt vastgelegd in termen van identificatie, authenticatie en autorisatie. Er zijn verschillende typen gebruikers: eindgebruikers en beheerders, die al of niet op afstand werken. Deze gebruikers moeten aan specifieke toegangseisen voldoen.
  De gebruikersgegevens, de rollen en profielen worden vastgelegd in registratiesystemen. In dit geval zijn er drie registratiesystemen vermeld. In de praktijk is dit afhankelijk van het type organisatie.
- Facilitair bedrijf
  Het Facilitair bedrijf zorgt voor een fysieke toegang tot terreinen, gebouwen en ruimten met een toegangsmiddel. Hierbij ontvangen de medewerkers bijvoorbeeld een toegangspas (is een identificatiemiddel).

2.1.3 *Control-domein*

Het control-domein bevat evaluatie-, meet- en beheersingsaspecten waarmee toegangsbeveiliging wordt beheerst en bijgestuurd. Het vervult hiermee een control-functie die kort en lang cyclisch van aard kunnen zijn. Dit domein bevat beheersprocessen, zoals de ITIL-processen, die noodzakelijk zijn voor de beheersing van de configuraties van IT-componenten en de instandhouding van het beveiligingsniveau. De informatie uit de evaluaties en de beheerprocessen is niet alleen gericht op het bijsturen en/of aanpassen van het eerder geformuleerde beleid maar ook op implementatie van de toegangsbeveiliging. In afbeelding 3 wordt de hiervoor uitgelegde domeinenstructuur geïllustreerd.

De domeinindeling is verder uitgewerkt in hoofdstuk 5 Control-domein.

Tot slot van dit hoofdstuk zij opgemerkt dat de objecten die een rol spelen bij toegangsbeveiliging van fysieke systemen, dezelfde zijn als die van gevirtualiseerde omgevingen.

3 Beleidsdomein

3.1 Doelstelling

De doelstelling van het beleidsdomein is het identificeren en beschrijven van de conditionele elementen die voorwaardelijk zijn voor het inrichten, beveiligen en beheersen van toegangsbeveiliging. De hierbij van belang zijnde beveiligingsobjecten zijn uitgewerkt in controls en gerelateerde maatregelen.

In dit domein zijn normatieve eisen opgenomen die de individuele technische omgevingen (zoals toegangsvoorziening, applicatie, operating system en netwerk) overstijgen. Met randvoorwaarden in de vorm van beleid geven organisaties de kaders aan, waarbinnen de realisatie en operatie van het autorisatiesysteem moet plaatsvinden.

3.2 Risico's

Als een door het management uitgevaardigd toegangsbeleid ontbreekt, is het risico dat onvoldoende sturing wordt gegeven aan de veilige inrichting van de toegang tot ICT-voorzieningen en ruimten waar de voorzieningen zich bevinden. Dit zal een negatieve impact hebben op het bereiken van doelstellingen voor toegangsbeveiliging.

3.3 Objecten, controls en maatregelen

De onderwerpen die specifiek voor toegangsbeveiliging in het beleidsdomein een rol spelen, zijn vermeld in tabel 1. Is een cel geel gekleurd, dan komt de bijbehorende control voor in de BIO. Betreft het een wit gemarkeerde cel, dan heeft de BIO geen control gedefinieerd, maar is dit object wel noodzakelijk voor deze BIO Thema-uitwerking. Tabel 1 geeft ook een overzicht en ordening van objecten naar de invalshoeken Intentie, Functie, Gedrag en Structuur (IFGS).

Intentie	Functie	Gedrag	Structuur
B.01 Toegangsbeveiligingsbeleid ((Operationeel) beleid)	B.03 Beveiligingsfunctie (Organisatorische functie)	B.04 Cryptografie (Interactie)	B.05 Beveiligingsorganisatie (IT-organisatiestructuur)
B.02 Inventarislijst en eigenaarschap (Eigenaar)	/	/	B.06 Toegangsbeveiligingsarchitectuur (IT-architectuur)

Tabel 1: Beleidsobjecten met -basiselementen voor toegangsbeveiliging per invalshoek

3.3.1 *B.01 Toegangsbeveiligingsbeleid*

Objectdefinitie

Resultaat van een besluitvorming omtrent de eisen die de organisatie stelt aan toegang, de middelen die daarbij ingezet worden en beperkingen die gelden bij de inrichting en het beheer.

Objecttoelichting

Het toegangsbeveiligingsbeleid maakt deel uit van het informatiebeveiligingsbeleid en geeft regels en voorschriften voor de organisatorische en technische inrichting van de fysieke toegang tot ruimten waar

ICT-middelen zich bevinden en voor toegang tot de informatie en informatieverwerkende faciliteiten zelf, zoals toegang voor gebruikers tot applicaties en toegang voor beheerders tot ICT-componenten. Het toegangsbeveiligingsbeleid beschrijft onder andere de manier waarop de klantorganisatie omgaat met identiteits- en toegangsbeheer.

De control behorende bij het object 'Toegangsbeveiligingsbeleid' is bedoeld om richting te geven aan de invulling van operationele activiteiten binnen het uitvoeringsdomein.

Doelstelling	Toegang voor bevoegden bewerkstelligen en toegang voor onbevoegden tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.		
Risico	Onvoldoende sturing op toegangsbeveiliging en autorisatiebeheer leidt tot verhoogde kans op ongeautoriseerde toegang en onvoldoende verantwoordingsinformatie.		
Control	Er behoren **regels** op basis van **bedrijfs-** en **informatiebeveiligingseisen** te worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.		BIO2: 5.15 ISO 27002:2022: 5.15
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	De regels om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen worden vastgesteld, gedocumenteerd en onderhouden in een toegangsbeveiligingsbeleid.	ISO 27002:2022: 5.15
Bedrijfseisen	2.	Bij de bescherming van logische- en fysieke toegang wordt rekening gehouden met relevante wet- en regelgeving en contractuele verplichtingen met betrekking tot het beperken van de toegang tot gegevens of diensten.	ISO 27002:2022: 5.15
	3.	Er is vastgesteld welke entiteiten welke soort toegang tot informatie en andere gerelateerde bedrijfsmiddelen vereist.	ISO 27002:2022: 5.15
Informatie-beveiligings-eisen	4.	Regels voor informatieverspreiding en -autorisatie, informatiebeveiligingsniveau's en -classificatie zijn vastgesteld, waarbij rekening is gehouden met de 'least privilege', 'need-to-know' en 'need-to-use' principes.	ISO 27002:2022: 5.15 Principes: BIO2 deel 1 paragraaf 11
	5.	Het autorisatiebeheer is procesmatig ingericht (zoals: aanvragen, toekennen, controleren, implementeren, intrekken/beëindigen en periodiek beoordelen).	ISO 27002:2022: 5.15
	6.	Toegang tot een vertrouwde zone waarin gevoelige overheidsinformatie is opgeslagen, is uitsluitend toegestaan vanaf een apparaat van de organisatie dat voldoet aan de beveiligingseisen of vanuit programmatuur die wordt uitgevoerd binnen een extra beveiligde omgeving.	BIO2: 5.15.01

3.3.2 *B.02 Inventarislijst en eigenaarschap*

Objectdefinitie

Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen en de toewijzing van de verantwoordelijkheid voor het toegangsbeveiligingssysteem.

Objecttoelichting

Om de toegang tot de logische als fysieke componenten van het toegangsbeveiligingssysteem betrouwbaar in te richten, is het van belang om inventarislijsten voor alle informatie en bedrijfsmiddelen op te stellen en te onderhouden. Het eigenaarschap van bedrijfsmiddelen dient goed te worden belegd. Dit maakt duidelijk wie aanspreekbaar is voor de inrichting van de verschillende onderdelen van het toegangsbeveiligingssysteem.

De coördinatie en beslissingen over specifieke acties (wie mag wat zien, raadplegen, muteren) vindt plaats onder de verantwoordelijkheid van de eigenaar.

Doelstelling	De informatie en andere gerelateerde bedrijfsmiddelen van de organisatie identificeren om de informatiebeveiliging ervan te behouden en passend eigenaarschap toe te wijzen.		
Risico	Als informatie en bedrijfsmiddelen niet expliciet zijn geïdentificeerd en geen eigenaar hebben, blijven noodzakelijke beveiligingsmaatregelen uit, met als gevolg verhoogde risico's op datalekken, misbruik of verstoring van dienstverlening.		
Control	De organisatie heeft inzicht en grip op welke informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van verantwoordelijkheden en **eigenaren**, binnen de organisatie gebruikt worden.		ISO 27002:2022: 5.9 SoGP 2018: PM1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Inventarislijst	1.	Alle informatie en andere gerelateerde bedrijfsmiddelen worden geïdentificeerd en vastgelegd in nauwkeurige, actuele en consistente inventarislijsten, zoals lijsten voor informatie, hardware, software, virtuele machines, faciliteiten, personeel en competenties. Hierbij worden tevens Operationele Technologie (OT), cloud-omgevingen, SaaS-applicaties en andere bedrijfsmiddelen opgenomen die regelmatig zijn verbonden met de netwerkinfrastructuur maar niet onder controle van de organisatie staan.	BIO2: 5.9.01 ISO 27002:2022: 5.9
	2.	De inventarislijsten worden periodiek beoordeeld en bij wijzigingen bijgewerkt, zodat een betrouwbare basis ontstaat voor risicobeheer, toegangsbeveiliging en de bescherming van kritieke assets.	BIO2: 5.9.01 ISO 27002:2022: 5.9
	3.	De bedrijfsmiddelen zijn geclassificeerd in lijn met de classificatie van de informatie die eraan is gerelateerd, zodat de beschermingsmaatregelen consistent zijn met de beveiligingseisen van die informatie.	ISO 27002:2022: 5.9
Eigenaren	4.	Voor elk geïdentificeerd informatie- en gerelateerd bedrijfsmiddel wordt een eigenaar (een persoon of groep) aangewezen die verantwoordelijk is voor het beheer en de beveiliging ervan.	ISO 27002:2022: 5.9 SoGP 2018: PM1.2.1

	5.	De eigenaar van een bedrijfsmiddel is verantwoordelijk voor het juiste beheer gedurende de gehele levenscyclus en zorgt ervoor dat: • het bedrijfsmiddel correct wordt geïnventariseerd en gekoppeld aan ondersteunende componenten; • het passend wordt geclassificeerd, beschermd en dat de classificatie periodiek wordt beoordeeld; • eisen voor aanvaardbaar gebruik worden vastgesteld; • toegangsbeperkingen aansluiten bij de classificatie, doeltreffend zijn en periodiek worden beoordeeld; • bedrijfsmiddelen bij verwijdering veilig worden gewist en uit de inventaris worden gehaald; • risico's rond het bedrijfsmiddel worden geïdentificeerd en beheerst; • ondersteunend personeel wordt begeleid bij het uitvoeren van hun rollen en verantwoordelijkheden.	ISO 27002:2022: 5.9 SoGP 2018: PM1.2.2 SoGP 2018: PM1.2.3

3.3.3 *B.03 Beveiligingsfunctie*

Objectdefinitie

Specialistische adviesfunctie binnen de organisatie, ter bevordering van het behalen van beveiligingsdoelstellingen.

Objecttoelichting

De organisatie beschikt over middelen en informatie die beveiligd moeten worden. Hiervoor moeten de juiste rollen zijn benoemd binnen een centraal orgaan, de beveiligingsfunctie. De functionarissen binnen deze functies hebben specifieke verantwoordelijkheden voor het realiseren van toegangsbeveiliging binnen de gehele organisatie, waaronder het toegangsbeveiligingssysteem.

Doelstelling	Het zorgen dat de toegangsbeveiliging effectief wordt ingericht.		
Risico	Onvoldoende gecoördineerde en tijdige uitvoering van toegangsbeveiligingsactiviteiten en het ontbreken van corrigerende acties leidt tot ineffectieve toegangsbeveiliging en verhoogde kans op ongeautoriseerde toegang.		
Control	Een gespecialiseerde **beveiligingsfunctie** dient te zijn vastgesteld die verantwoordelijk is voor het bevorderen van toegangsbeveiliging binnen de gehele organisatie.		SoGP 2018: SM2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-functie	1.	De rollen binnen de beveiligingsfunctie moeten zijn benoemd en de taken en verantwoordelijkheden vastgelegd, zoals: HRM, Proceseigenaar, Autorisatiebeheerder, Chief Information Security Officer (CISO) en Beveiligingsambtenaar (BVA) als het gaat om de Rijksoverheid.	ISO 27001:2022: 5.3 SoGP 2018: SM2.1
	2.	De functionarissen binnen de beveiligingsfunctie moeten periodiek het toegangsbeveiligingssysteem (laten) evalueren inclusief de implicatie van businessinitiatieven voor het toegangsbeveiligingssysteem.	SoGP 2018: SA1.1.10

3.3.4 *B.04 Cryptografie*

Objectdefinitie

Coderingstechniek ter bescherming van informatie vanuit het oogpunt van vertrouwelijkheid, authenticiteit, onweerlegbaarheid en authenticatie.

Objecttoelichting

Voor toegangsbeveiliging is het van cruciaal belang dat de geheime authenticatie-informatie, zoals wachtwoorden en pincodes, worden beschermd tijdens de verwerking, het transport en de opslag. Een solide (en goed doorgevoerd) encryptiebeleid garandeert de vertrouwelijkheid van geheime authenticatie-informatie.

Met cryptografiebeleid geeft de organisatie aan op welke wijze het omgaat met voorzieningen, procedures en certificaten voor versleuteling van gegevens.

Doelstelling	Het zorgen dat cryptografie correct en doeltreffend wordt gebruikt, om de vertrouwelijkheid, authenticiteit en/of integriteit van authenticatie-informatie te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.		
Risico	Onvoldoende of onjuist gebruik van cryptografie leidt tot verlies van vertrouwelijkheid en integriteit van data en risico's op niet-naleving van wettelijke en contractuele eisen.		
Control	**Regels** voor het doeltreffende **gebruik van cryptografie**, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.		BIO2: 8.24
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Authentica-tie-informatie	1.	Authenticatie-informatie wordt beschermd door versleuteling.	SoGP 2018: TS2.2
Regels	2.	De regels voor cryptografie worden vastgelegd in een cryptografiebeleid. In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum Standaardisatie worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	BIO2: 8.24.01
Gebruik van cryptografie	3.	• Cryptografische beheersmaatregelen zijn opgenomen in de inventaris van de bedrijfsmiddelen; • Voor alle cryptografische beheersmaatregelen is vastgesteld waar ze worden ingezet, wie er voor verantwoordelijk is en hoe ze actueel worden gehouden.	BIO2: 8.24.02
	4.	De sterkte van de cryptografie wordt waar mogelijk gebaseerd op de actuele adviezen van het NCSC en de Unit Weerbaarheid van de AIVD.	BIO2: 8.24.04

3.3.5 *B.05 Beveiligingsorganisatie*

Objectdefinitie

Doelgerichte bundeling van kennis en vaardigheden tussen personen met taken, bevoegdheden en verantwoordelijkheden op het gebied van informatiebeveiliging.

Objecttoelichting

De beveiligingsorganisatie ziet toe op het naleven van het informatiebeveiligingsbeleid. Waar nodig grijpt de beveiligingsorganisatie in. Welke taken, verantwoordelijkheden, bevoegdheden en middelen een beveiligingsorganisatie hierin heeft, wordt vooraf expliciet benoemd en vastgesteld. Ook moet vaststaan hoe de rapportagelijnen zijn uitgestippeld.

Doelstelling	Het invullen, coördineren en borgen van het informatiebeveiligingsbeleid binnen de organisatie.		
Risico	Onvoldoende sturing en borging van het informatiebeveiligingsbeleid leidt tot ineffectieve uitvoering en verhoogde risico's op incidenten en niet-naleving.		
Control	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie. Het toewijzen van de rollen en verantwoordelijkheden die bij informatiebeveiliging horen, behoort te worden gedaan in overeenstemming met het beleid voor informatiebeveiliging en onderwerp specifieke beleidsregels.		ISO 27002:2022: 5.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Organisatorische positie	1.	De beveiligingsorganisatie heeft een formele positie binnen de gehele organisatie.	CIP-netwerk
Taken, verantwoordelijkheden en bevoegdheden (TVB)	2.	De organisatie heeft de verantwoordelijkheden voor het definiëren, coördineren en evalueren van de beveiligingsorganisatie beschreven en toegewezen aan specifieke functionarissen.	CIP-netwerk
	3.	De taken, verantwoordelijkheden en bevoegdheden zijn vastgelegd in bijvoorbeeld een autorisatiematrix.	CIP-netwerk
Functionarissen	4.	De belangrijkste functionarissen (stakeholders) voor de beveiligingsorganisatie zijn benoemd en de relaties tussen hen zijn met een organisatieschema inzichtelijk gemaakt.	CIP-netwerk
Rapportagelijnen	5.	De verantwoordings- en rapportagelijnen tussen de betrokken functionarissen zijn vastgesteld.	CIP-netwerk
	6.	Eigenaren behoren de resultaten te rapporteren aan de personen die onafhankelijke beoordelingen uitvoeren wanneer een onafhankelijke beoordeling plaatsvindt binnen hun verantwoordelijkheidsgebied.	ISO 27002:2022: 5.36

3.3.6 *B.06 Toegangsbeveiligingsarchitectuur*

Objectdefinitie

Modelmatige beschrijving van de technische en organisatorische samenhang van de onderdelen voor toegangsbeveiliging.

Objecttoelichting

De toegangsbeveiligingsarchitectuur is een blauwdruk waarmee wordt aangegeven op welke wijze gebruikers toegang krijgen tot applicaties en overige ICT-componenten. Typen gebruikers, beheerders, rollen en hun onderlinge verbanden worden hierbij vastgelegd volgens modellen als RBAC en ABAC.

Voor de toegang tot applicaties zijn in de toegangsbeveiligingsarchitectuur de volgende onderwerpen van belang:

- ontwerp van identiteits- en toegangsbeheer;
- inrichting toegangsbeheer;
- eisen en behoeften over gebruikersidentificatie en -authenticatie;
- gebruik van uniforme authenticatiemechanismen;
- gebruik van platformaccounts met beperkte rechten;
- audit van uitgedeelde autorisaties.

Doelstelling	Het verkrijgen van inzicht in de samenhang van en de relatie tussen de technische componenten die een rol spelen bij de inrichting en beheer van het toegangsvoorzieningsdomein.		
Risico	Onvoldoende inzicht in het toegangsvoorzieningsdomein leidt tot gebrekkige beheersing van autorisatie-inrichting en -beheer en verhoogde kans op onjuiste of onbevoegde toegang.		
Control	De organisatie behoort met organisatorische eisen en wensen de **technische inrichting** beschreven te hebben en behoort in een **toegangsbeveiligingsarchitectuur** te zijn vastgelegd.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Technische inrichting	1.	De technische inrichting van de toegangsbeveiliging is met organisatorische eisen vormgegeven aangaande: • de uniformiteit en flexibiliteit van authenticatiemechanismen; • de rechten voor beheeraccounts; • de identificatie- en authenticatiemechanismen om voldoende sterke wachtwoorden af te dwingen; • autorisatiemechanismen, waarbij gebruikers alleen toegang krijgen tot diensten (functies) waarvoor ze specifiek bevoegd zijn.	CIP-netwerk
Toegangs-beveiligings-architectuur	2.	De inrichting van het identiteits- en toegangsbeheer is vastgelegd in een toegangsbeveiligingsarchitectuur.	CIP-netwerk

4 Uitvoeringsdomein

4.1 Doelstelling

De doelstelling van het uitvoeringsdomein in deze BIO Thema-uitwerking is het zorgen dat de toegang tot terreinen, gebouwen, ruimten, applicaties en data is ingericht volgens de specifieke beleidsuitgangspunten van de organisatie (en/of organisatieonderdelen) en dat de werking voldoet aan de eisen die door de organisatie zijn gesteld met het (autorisatie)beleid.

4.2 Risico's

Wanneer een adequate toegangsbeveiliging tot terreinen, gebouwen, ruimten en informatiefaciliteiten ontbreekt, is het risico dat onbevoegden zich toegang kunnen verschaffen tot faciliteiten en data en/of dat gebruikers met te ruime bevoegdheden ongewenste acties kunnen uitvoeren.

4.3 Objecten, controls en maatregelen

Binnen het uitvoeringsdomein worden specifieke inrichtings- en beveiligingsobjecten over toegangsbeveiliging beschreven. Per object is een control gedefinieerd en zijn conformiteitsindicatoren uitgewerkt. Binnen het uitvoeringsdomein worden de in tabel 2 vermelde objecten uitgewerkt. De rood gemarkeerde objecten komen voor in de BIO. De wit gemarkeerde zijn betrokken uit andere best practices.

Intentie	Functie	Gedrag	Structuur
U.01 Registratieprocedure ((Operationeel) beleid)	U.04 Autorisatieproces (proces)	U.08 Geheime authenticatie-informatie (interactie)	U.10 Autorisatievoorzieningen (faciliteit)
U.02 Toegangsverleningsprocedure ((Operationeel) beleid)	U.05 Wachtwoordenbeheer (proces)	U.09 Autorisatie (interactie)	/
U.03 Inlogprocedure ((Operationeel) beleid)	U.06 Speciale toegangsrechtenbeheer (proces)	/	/
/	U.07 Functiescheiding (taakvereiste)	/	/
/	U.11 Fysieke toegangsbeveiliging (Beschermingsfunctie)	/	/

Tabel 2: Uitvoeringsobjecten met -basiselementen voor logische toegangsbeveiliging per invalshoek

4.3.1 *U.01 Registratieprocedure*

Objectdefinitie

Vastgelegde manier van handelen voor het registreren van gebruikers.

Objecttoelichting

De oorspronkelijke titel in de BIO is 'Registratie en afmelden van gebruikers'. Het onderwerp 'Registratie en afmelden van gebruikers' duidt op het daadwerkelijk registreren en afmelden van gebruikers. De inhoud van de norm legt feitelijk de nadruk op procedures die bij het registreren en afmelden noodzakelijk zijn. Vandaar dat bij dit object gekozen is voor de titel 'Registratieprocedure'. Deze procedure beschrijft de gecontroleerde toegang voor bevoegde gebruikers vanaf het moment van intake en registratie tot en met de beëindiging. Het beschrijft dus de gehele levenscyclus van de gebruikerstoegang. Een onderdeel van de procedure is dat er gebruikers geregistreerd worden.

Het registreren van gebruikers geldt zowel bij logische als bij fysieke beveiliging. De noodzakelijke fysieke beveiligingsprocedure is gericht op zowel interne als externe medewerkers.

Bij uitbestede diensten geldt dat de provider zowel de logische als de fysieke beveiligingsmaatregelen treft voor de beveiliging van de ICT-dienstverlening aan de klant.

Doelstelling	Het zorgen voor een gecontroleerde toegang voor bevoegde gebruikers en voorkomen van onbevoegde toegang tot informatiesystemen.		
Risico	Als toegangsbeveiliging niet effectief is ingericht, wordt de betrouwbaarheid van registratiesystemen aangetast en bestaat de kans dat onbevoegden wijzigingen kunnen aanbrengen in informatiesystemen.		
Control	De volledige levenscyclus van **identiteiten** (personen en systemen) behoort te worden beheerd.		BIO2: 5.16 ISO 27002:2022: 5.16
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Identiteiten	1.	Er is een sluitende formele registratie-, wijzigings- en afmeldprocedure voor het beheren van gebruikersidentificaties.	BIO2: 5.16.01 ISO 27002:2022: 5.16
	2.	Het gebruiken van groepsaccounts is niet toegestaan, tenzij de proceseigenaar dit motiveert, vastlegt en afstemt met de CISO.	BIO2: 5.16.02 ISO 27002:2022: 5.16
	3.	De aanvraag van autorisaties op het gebruik van informatiesystemen en de toegewezen autorisatieniveaus worden geregistreerd, gecontroleerd en goedgekeurd.	ISO 27002:2022: 5.16
	4.	Gebruikers worden met juiste functierollen (en autorisatieprofielen) geautoriseerd voor het gebruik van applicaties (need-to-know- en need-to-have-principes).	CIP-netwerk
	5.	Een bevoegdhedenmatrix is beschikbaar waarmee gebruikers slechts die object- en/of systeemprivileges toegekend krijgen die zij nodig hebben voor de uitoefening van hun taken.	CIP-netwerk

4.3.2 *U.02 Toegangsverleningsprocedure*

Objectdefinitie

Vastgelegde manier van handelen voor het verlenen, beoordelen, aanpassen en verwijderen van toegang tot bedrijfsmiddelen.

Objecttoelichting

De toegangsverleningsprocedure beschrijft de verantwoordelijkheden bij de toekenning van toegangsrechten en omvat de toewijzing, aanpassing en intrekking van zowel logische als fysieke toegangsrechten, voor alle gebruikers.

Doelstelling	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen..		
Risico	Als niet is vastgelegd en goedgekeurd wie welke handelingen mag verrichten, bestaat het risico dat onbevoegden toegang krijgen tot informatie en bedrijfsmiddelen of dat bevoegden hun taken niet correct kunnen uitvoeren.		
Control	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.		BIO2: 5.18 ISO 27002:2022: 5.18
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Toegangsrechten	1.	De procedure voor het toewijzen of intrekken van fysieke en logische toegangsrechten aan de geauthenticeerde identiteit van een entiteit omvat: • autorisatie van de eigenaar van informatie of een informatiesysteem of het management; • toepassing van functiescheiding, waaronder het scheiden van de rollen van goedkeuring en implementatie van toegangsrechten; • toegangsrechten worden tijdig ingetrokken wanneer iemand geen toegang meer nodig heeft; • toegangsrechten aanpassen van gebruikers die van rol of functie zijn veranderd; • een registratie van het toekennen en wijzigingen in de logische en fysieke toegangsrechten van gebruikers.	ISO 27002:2022: 5.18
	2.	Het maken en aanpassen van accounts met bijzondere rechten wordt gemonitord. Indien deze wijzigingen ongeautoriseerd zijn, is dit een informatiebeveiligingsincident en wordt als zodanig vastgelegd en afgehandeld.	BIO2: 5.18.01
	3.	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. Een risicoafweging bepaalt of dit sneller moet.	BIO2: 5.18.02

4.3.3 *U.03 Inlogprocedure*

Objectdefinitie

Vastgelegde manier van handelen voor het verkrijgen van de toegang tot een systeem, een netwerk of een afgeschermd deel van een website.

Objecttoelichting

De inlogprocedure omvat de technische procedure waarbij het toegangsbeheersysteem controleert of aan de vereiste inlogeisen wordt voldaan.

Doelstelling	Het voorkomen van onbevoegde toegang tot systemen en toepassingen.		
Risico	Onvoldoende bescherming tegen onbevoegde toegang leidt tot risico's op datamisbruik, dataverlies en verstoring van beschikbaarheid.		
Control	Er behoren **beveiligde authenticatietechnologieen en -procedures** te worden geïmplementeerd op basis van **beperkingen van de toegang** tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.		BIO2: 8.5 ISO 27002:2022: 8.5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
beveiligde authenticatie technologieën en -procedures	1.	• de sterkte van authenticatiemechanismen wordt afgestemd op de classificatie van de informatie waartoe toegang wordt verleend. • de procedure om in een systeem in te loggen wordt zodanig ontworpen dat het risico op onbevoegde toegang zo klein mogelijk wordt gemaakt.	ISO 27002:2022: 8.5
beperkingen van de toegang	2.	Ingeval krachtige verificatie en authenticatie van de identiteit is vereist, behoren andere authenticatiemethoden dan wachtwoorden te worden gebruikt, zoals digitale certificaten, chipkaarten, tokens of biometrische middelen.	ISO 27002:2022: 8.5
	3.	Voor toegang tot essentiële informatiesystemen wordt multifactorauthenticatie (MFA) toegepast, gebaseerd op een combinatie van meerdere factoren (bijv. kennis, bezit en biometrie).	ISO 27002:2022: 8.5
	4.	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden en voor hoelang de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	BIO2: 8.5.01

4.3.4 *U.04 Wachtwoordenbeheer*

Objectdefinitie

Instandhoudingsproces voor de uitgifte en het onderhoud van wachtwoorden.

Objecttoelichting

Een wachtwoord is een geheim woord dat alleen de bezitter kent en waarmee hij zich toegang verschaft tot een locatie of een informatiesysteem.

Wachtwoordenbeheer betreft het samenstel van activiteiten voor het uitgeven, (doen) vernieuwen en blokkeren van wachtwoorden, waarbij ook de kwaliteit van de wachtwoorden wordt geborgd.

De control en maatregelen van dit object zijn gericht op het authentiseren van personen. Voor het authentiseren van systemen die andere systemen/bedrijfsobjecten e.d. benaderen, zijn soms stringentere eisen noodzakelijk.

Doelstelling	Het zorgen dat alleen de beoogde geauthentiseerde personen toegang tot (vooraf bepaalde) bedrijfsobjecten krijgen.

Risico	Onvoldoende borging van authenticatie en autorisatie leidt tot ongeautoriseerde toegang en een verhoogde kans op schade aan bedrijfsbelangen.		
Control	De toewijzing en het beheer van **authenticatie-informatie** behoort te worden beheerst door middel van een **beheerproces** waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.		BIO2: 5.17 ISO 27002:2022: 5.17
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
authenticatie-informatie	1.	Multi-factorauthenticatie (MFA) wordt toegepast bij 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. MFA wordt toegepast in deze twee vormen: 1. Wachtwoordloze toegang, zoals een pincode in combinatie met een hardware token of persoonlijk uniek certificaat (passkey). 2. Wachtwoordtoegang in combinatie met minimaal een tweede factor. Indien MFA niet mogelijk is voor deze accounts, neem andere mitigerende maatregelen. Betrek de CISO hierbij en laat ze goedkeuren door de proceseigenaar. Combineer waar mogelijk en veilig, MFA met federatieve authenticatievoorzieningen zoals Single Sign On en een Stepping Stone-oplossing.	BIO2: 5.17.01
	2.	De organisatie biedt aan alle medewerkers een wachtwoordmanager of vergelijkbare oplossing aan.	BIO2: 5.17.02
	3.	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	BIO2: 5.17.03

4.3.5 *U.05 Speciale toegangsrechtenbeheer*

Objectdefinitie

Instandhoudingsproces voor de uitgifte en het onderhoud van speciale toegangsrechten.

Objecttoelichting

Beheerders hebben vaak speciale systeembevoegdheden nodig om hun beheeractiviteiten uit te voeren. De activiteiten die met zulke bevoegdheden kunnen worden uitgevoerd, kunnen diep ingrijpen in het systeem. Daarom moet hier voorzichtig mee worden omgegaan en zijn hiervoor procedurele maatregelen noodzakelijk: het speciale toegangsrechtenbeheer.

Speciale toegangsrechtenbeheer betreft het samenstel van activiteiten voor de uitgifte, het beheer en de bewaking van speciale systeembevoegdheden van ICT-beheerders.

Doelstelling	Het voorkomen van misbruik en oneigenlijk gebruik van bedrijfsobjecten.
Risico	Als misbruik en oneigenlijk gebruik van bedrijfsobjecten niet wordt voorkomen, bestaat het risico dat onbevoegden of ongeautoriseerde handelingen plaatsvinden, wat kan leiden tot schade aan bedrijfsbelangen.

Control	Het **toewijzen** en het gebruik van **speciale toegangsrechten** behoren te worden beperkt en **beheerd**.		BIO2: 8.2 ISO 27002:2022 8.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Toewijzen	1.	Het toewijzen van speciale toegangsrechten behoort te worden beheerst door een autorisatieprocedure die in overeenstemming is met het beleid voor toegangsbeveiliging..	ISO 27002:2022 8.2
Speciale toegangs-rechten	2.	• gebruikers die speciale toegangsrechten nodig hebben worden voor elk systeem of proces geïdentificeerd; • gebruikers hebben toegang tot speciale toegangsrechten voor zover dat voor de uitoefening van hun taak noodzakelijk is (need-to-know en need-to-use); • het gebruik van identiteiten met speciale toegangsrechten wordt beperkt tot het uitvoeren van beheerfuncties en deze identiteiten worden niet gebruiken voor de dagelijkse algemene taken.	ISO 27002:2022 8.2
Beheerst	3.	De toegewezen of gebruikte speciale bevoegdheden worden in opzet, bestaan en werking minimaal ieder kwartaal beoordeeld.	BIO2: 8.02.01 ISO 27002:2022 8.2

4.3.6 *U.06 Functiescheiding*

Objectdefinitie

Scheiding van taken en verantwoordelijkheden over meerdere functionarissen, die - wanneer ze in één hand zouden liggen - risico's op fraude of misbruik zouden meenemen.

Objecttoelichting

In het autorisatieproces gaat het om taken van verschillende typen eindgebruikers en taken van beheerders. Het toegangsbeleid dient regels en voorschriften te geven voor de organisatorische en technische inrichting van de toegang tot ICT-voorzieningen, zoals applicatie (gebruikers) en ICT-componenten (beheerders).

Het toegangsvoorzieningsbeleid beschrijft onder andere de manier waarop de organisatie omgaat met identiteits- en toegangsbeheer. De nodige eisen worden gesteld aan functiescheiding om een effectief en consistent gebruikersbeheer, identificatie, authenticatie en toegangscontrolemechanismen voor heel de organisatie te waarborgen.

Doelstelling	Het zorgen dat: • de gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van bedrijfsmiddelen van de organisatie wordt verminderd; • niemand een gehele procescyclus kan beïnvloeden.	
Risico	Onvoldoende scheiding van taken leidt tot verhoogde kans op fraude, mogelijk misbruik van bedrijfsmiddelen en kans op ongeautoriseerde wijziging of vernietiging van informatie.	
Control	Conflicterende **taken** en conflicterende **verantwoordelijkheden** behoren te worden **gescheiden**.	BIO2: 5.3 ISO 27002:2022 5.3
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Taken	1.	Een scheiding is aangebracht tussen beheertaken en (overige) gebruikstaken.	CIP-netwerk
Verantwoor-delijkheden	2.	Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig zijn toegewezen aan één specifieke (beheerders)rol.	CIP-netwerk
Gescheiden	3.	Een risicoafweging bepaalt waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	CIP-netwerk
	4.	Rollen, taken en verantwoordelijkheden zijn vastgesteld volgens gewenste functiescheidingen.	CIP-netwerk

4.3.7 *U.07 Autorisatie*

Objectdefinitie

Proces voor het toekennen van rechten aan gebruikers.

Objecttoelichting

Gekozen is voor de objectnaam 'Autorisatie', omdat dit beter aansluit op de toegangsmechanismen (identificatie, authenticatie en autorisatie) dan de BIO-titel 'Beperking toegang tot informatie'.

Na het identificatie- en authenticatieproces krijgen gebruikers en beheerders (verdere) specifieke toegang tot informatiesystemen voor gebruiks- respectievelijk beheerdoeleinden. Toegang (en de beperking daarvan) wordt gecreëerd met rollen en toegangsprofielen die voortkomen uit het toegangsbeleid.

Doelstelling	Het voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.		
Risico	Als onbevoegde toegang tot informatie in toepassingssystemen niet wordt voorkomen, bestaat het risico dat ongewenste wijzigingen in informatiesystemen worden aangebracht.		
Control	De toegang tot **informatie** en andere gerelateerde bedrijfsmiddelen behoren te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.		BIO2: 8.3 ISO 27002:2022: 8.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Informatie	1.	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	BIO2: 8.03.01 ISO 27002:2022: 8.3
	2.	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	BIO2: 8.03.02
	3.	Het toegangsbeveiligingsbeleid geeft onder andere aan dat toegang tot informatie en tot functies van toepassingssystemen wordt beperkt met juiste rollen en verantwoordelijkheden.	CIP-netwerk

4.3.8 *U.08 Autorisatievoorzieningen*

Objectdefinitie

Middelen waarmee aan gebruikers fysieke en logische toegang kan worden verleend.

Objecttoelichting

Om autorisatiebeheer efficiënt en effectief te kunnen inrichten, zijn technische autorisatievoorzieningen zoals een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten noodzakelijk.

Doelstelling	Het effectief, efficiënt en veilig kunnen uitvoeren van autorisatiebeheer.		
Risico	Door vervuiling in het autorisatiebeheer die onvoldoende of niet tijdig wordt gesignaleerd, bestaat het risico dat onbevoegden toegang krijgen tot gegevens.		
Control	Voor autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische **autorisatievoorzieningen** beschikbaar zijn, zoals: een **personeelsregistratiesysteem**, een **autorisatiebeheersysteem** en **autorisatiefaciliteiten**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Autorisatie-voorzieningen	1.	Door een verantwoordelijke is formeel vastgesteld welke ondersteunende middelen worden ingezet binnen het autorisatiebeheer.	CIP-netwerk
Personeels-registratie systeem	2.	Alle interne en externe gebruikers worden vóór de toegangsverlening tot de applicatieomgeving opgenomen in het personeelsinformatiesysteem.	CIP-netwerk
Autorisatie-beheer-systeem	3.	Alle natuurlijke personen die gebruik maken van applicaties worden geregistreerd.	CIP-netwerk
Autorisatie-faciliteiten	4.	Iedere applicatie die valt onder het autorisatiebeheerproces heeft functionaliteiten om autorisaties toe te kennen, in te zien en te beheren.	CIP-netwerk

4.3.9 *U.09 Fysieke toegangsbeveiliging*

Objectdefinitie

Geheel van processen en middelen om gebruikers veilig en gecontroleerd toegang te verlenen tot terreinen, gebouwen en ruimten.

Objecttoelichting

Fysieke beveiliging kan worden bereikt door het opwerpen van allerlei fysieke barrières rond het bedrijfsterrein en rond de IT-voorzieningen. Elke barrière creëert zo een beveiligde zone waarmee de totale beveiliging wordt versterkt.

Binnen de organisatie moeten beveiligingsniveaus en beveiligde zones worden gebruikt om gebieden die IT-voorzieningen bevatten te beschermen. Een beveiligde zone is een gebied binnen een barrière, zoals

muren of hekken, die alleen met een toegangspas of via een bemande receptiebalie geopend kan worden. De locatie en benodigde sterkte van de barrières worden onder andere bepaald op basis van de resultaten van de risicoanalyse.

Als systemen worden ingezet bij het fysieke toegangsbeheer, voor bijvoorbeeld de aansturing van sloten, gelden onverminderd alle controls die van toepassing zijn op de toegangsverlening tot informatiesystemen en wordt ook het proces analoog ingericht.

Doelstelling	Het zorgen dat alleen bevoegd personeel toegang krijgt en dat geen schade aan gebouwen of verstoring van informatie plaatsvindt.		
Risico	Als fysieke toegangsbeveiliging niet waarborgt dat alleen bevoegd personeel toegang krijgt, bestaat het risico dat onbevoegden schade toebrengen aan de computerruimte en verstoringen veroorzaken in informatie en systemen.		
Control	**Beveiligde zones** behoren te worden beschermd door **passende toegangsbeveiligings-maatregelen en toegangspunten**.		BIO2: 7.2 ISO 27002:2022: 7.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligde zones	1.	Toegang tot beveiligingszones (terreinen, gebouwen en ruimten) waar zich resources bevinden, is slechts toegankelijk voor personen die hiervoor geautoriseerd zijn.	CIP-netwerk
Passende toegang-beveiligings-maatregelen en toegangspunten	2.	De aankomst- en vertrektijden van bezoekers worden geregistreerd in een fysiek of elektronisch logboek.	ISO 27002:2022: 7.2
	3.	Alle medewerkers, contractanten en andere externen dragen een bepaalde vorm van zichtbare identificatie en stellen onmiddellijk het beveiligingspersoneel op de hoogte als zij bezoekers zonder begeleiding en personen die geen zichtbare identificatie dragen, tegenkomen.	ISO 27002:2022: 7.2
	4.	In geval van concrete beveiligingsrisico's worden waarschuwingen, volgens onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	BIO2: 7.02.01
	5.	Aan personeel van leveranciers die ondersteunende diensten verlenen wordt alleen indien noodzakelijk, beperkte toegang te worden verleend tot beveiligde gebieden of faciliteiten die vertrouwelijke informatie verwerken. Deze toegang behoort te zijn gebaseerd op autorisatie en te worden gemonitord.	ISO 27002:2022: 7.2

5 Control-domein

5.1 Doelstelling

De doelstelling van het control-domein in deze thema-uitwerking is te zorgen dat en/of vast te stellen of:

- de toegangsbeveiliging afdoende is ingericht voor het leveren van het gewenste niveau van autorisaties;
- het juiste beveiligingsniveau van de toegangsvoorziening wordt gegarandeerd.

Dit houdt onder meer in dat binnen de organisatie een adequate beheersingsorganisatie moet zijn ingericht waarin beheerprocessen zijn vormgegeven.

5.2 Risico's

Als de noodzakelijke maatregelen in het control-domein ontbreken, dan is het risico dat de autorisatieomgeving niet voldoet aan de beoogde organisatorische- en beveiligingsvoorwaarden. Ook kan niet worden vastgesteld of de gewenste maatregelen worden nageleefd.

5.3 Objecten, controls en maatregelen

Het beoordelen van de logische en fysieke toegangsrechten richt zich op het naleven van de verplichtingen die voortkomen uit wet- en regelgeving en door de organisatie zelf gekozen standaarden en richtlijnen. Vanuit beveiligingsoptiek is het van belang om periodiek, namens de directie, vast te stellen of het registratiesysteem betrouwbaar is.

Binnen dit specifieke control-domein zijn de objecten in tabel 4 van belang bij het beoordelen van gebruikersautorisatie. De blauw gemarkeerde objecten komen voor in de BIO. De wit gemarkeerde objecten zijn betrokken uit andere best practices.

Intentie	Functie	Gedrag	Structuur
C.01 Beoordelingsprocedure ((Operationeel) beleid)	C.02 Beoordeling toegangsrechten (Proces)	C.03 Logging en monitoring (Event/historie)	C.04 Beheersorganisatie toegangsbeveiliging (IT-organisatiestructuur)

Tabel 3: Control-objecten met basiselementen voor toegangsbeveiliging per invalshoek

5.3.1 *C.01 Beoordelingsprocedure*

Objectdefinitie

Vastgelegde manier van handelen voor de evaluatie van de mate waarin beheeractiviteiten voldoen aan de vooraf gestelde eisen.

Objecttoelichting

De inrichting van de toegangsbeveiliging moet beheerst worden. Een bepaalde functionaris met specifieke bevoegdheden dient hiervoor periodiek controle-activiteiten uit te voeren. Om te borgen dat deze controle-activiteiten voldoen aan de gestelde eisen, dienen ze ondersteund te worden met procedures en instructies.

Doelstelling	Het bieden van ondersteuning bij het uitvoeren van formele controle-activiteiten.		
Risico	Als controle-activiteiten niet worden ondersteund met procedures en instructies, bestaat het risico dat niet kan worden vastgesteld of deze gestructureerd en consistent plaatsvinden, waardoor tekortkomingen in toegangsbeveiliging onopgemerkt blijven.		
Control	Om het gebruik van toegangsbeveiligingsvoorzieningen te (kunnen) controleren, behoren er **procedures** te zijn vastgesteld.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procedures	1.	De organisatie beschikt over procedures voor het controleren van toegangsbeveiligingssystemen en -registraties (log-data).	CIP-netwerk
	2.	De organisatie beschikt over een beschrijving van de relevante controleprocessen.	CIP-netwerk
	3.	De procedures hebben betrekking op controleprocessen die volgens een vastgestelde cyclus zijn ingericht, zoals: registratie, statusmeting, bewaking (monitoring), analyse, rapportage en evaluatie.	CIP-netwerk
	4.	De procedures schrijven voor dat de resultaten van controle-activiteiten aan het management gerapporteerd moeten worden om de juiste acties te laten initiëren.	CIP-netwerk

5.3.2 *C.02 Beoordeling toegangsrechten*

Objectdefinitie

Evaluatie van de mate waarin de actuele toegangsrechten nog valide zijn.

Objecttoelichting

Beoordeling toegangsrechten behelst het proces voor het evalueren van toegangsrechten op validiteit en actualiteit.

Het is nodig om de (logische en fysieke) toegangsrechten van gebruikers regelmatig te beoordelen om de toegang tot gegevens en informatiediensten doeltreffend te kunnen beheersen. De toekenningen en wijzigingen van toegangsrechten dienen daarom periodiek gecontroleerd te worden. Hiertoe dienen maatregelen te worden getroffen in de vorm van:

- het voeren van controle-activiteiten op de registratie van toegangsrechten;
- het uitbrengen van rapportages aan het management.

Doelstelling	Het vaststellen of: • de autorisaties juist zijn aangebracht in de applicaties; • de wijzigingen en verwijderingen juist zijn uitgevoerd; • de koppelingen tussen gebruikers en rollen tijdig zijn aangepast wanneer de inhoud van de functies of de eisen over functiescheiding, scheiding van handelingen en doelbinding daar aanleiding toe geven.		
Risico	Als afwijkingen in het autorisatieproces niet tijdig worden gesignaleerd, treedt mogelijk vervuiling op in autorisaties, waardoor onbevoegden informatie kunnen inzien en/of manipuleren.		
Control	**Toegangsrechten** voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, **beoordeeld**, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.		BIO2: 5.18 ISO 27002:2022: 5.18
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Toegangs-rechten	1.	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. Een risicoafweging bepaalt of dit sneller moet.	BIO2: 5.18.02
	2.	Toegangsrechten van gebruikers behoren na wijzigingen, zoals promotie, degradatie of beëindiging van het dienstverband, te worden beoordeeld.	ISO 27002:2022: 5.18
	3.	Autorisaties voor speciale toegangsrechten behoren frequenter te worden beoordeeld.	ISO 27002:2022: 5.18
	4.	De beoordelingsrapportage bevat verbetervoorstellen en wordt gecommuniceerd met de verantwoordelijken/eigenaren van de systemen waarin kwetsbaarheden en zwakheden zijn gevonden.	CIP-netwerk
	5.	Het maken en aanpassen van accounts met bijzondere rechten wordt gemonitord. Indien deze wijzigingen ongeautoriseerd zijn, is dit een informatiebeveiligingsincident en wordt als zodanig vastgelegd en afgehandeld.	ISO 27002:2022: 5.18
Beoordeeld	6.	Het beoordelen vindt plaats op basis van een formeel proces, waarin planning, uitvoering van scope, rapporteren en bespreken van verbetervoorstellen een plaats hebben.	CIP-netwerk
	7.	Een functionaris is verantwoordelijk voor het controleren van de organisatorische en de technische inrichting van toegangsbeveiliging.	CIP-netwerk

5.3.3 *C.03 Logging en monitoring*

Objectdefinitie

Vastlegging van aan informatiebeveiliging gerelateerde gebeurtenissen en het bewaken en onderkennen van afwijkingen op beleidsregels.

Objecttoelichting

De beoogde werking van toegangsbeveiliging behoort via logging en monitoring te worden bewaakt.

Logging betreft de registratie van handelingen van gebruikers en systemen in een registratiesysteem voor analyse- en controledoeleinden. Monitoring behelst het bewaken en onderkennen van ongeautoriseerde acties en het analyseren van de geregistreerde acties op onvolkomenheden.

Tevens dient periodiek getoetst te worden of actuele autorisaties nog overeenkomen met de werkelijke situaties. Verder moet het volgende worden beoordeeld:

- wijzigingen op autorisaties (vastgelegd in log-bestanden);
- afspraken die niet systeemtechnisch worden afgedwongen (vier ogen principe).

Doelstelling	Het mogelijk maken om: • eventuele schendingen van functionele en beveiligingseisen te detecteren en achteraf de juistheid van de uitgevoerde acties vast te stellen; • handelingen te herleiden naar individuele personen.		
Risico	Als logging, monitoring en vastlegging van handelingen onvoldoende zijn ingericht, kan niet worden vastgesteld wie welke handelingen heeft uitgevoerd en worden schendingen van functionele of beveiligingseisen niet tijdig herkend, waardoor passende corrigerende acties achterwege blijven.		
Control	Er behoren **logbestanden** waarin **activiteiten**, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en **geanalyseerd**.		BIO2: 8.15 ISO 27002:2022: 8.15
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Log-bestanden	1.	Een logregel bevat minimaal: • Actie: de gebeurtenis of handeling die heeft plaatsgevonden. • Object: waarop de gebeurtenis of handeling effect had (bijvoorbeeld welk bestand, proces of systeem). • Resultaat: het resultaat van de gebeurtenis of handeling. • 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 handeling plaatsvond.	BIO2: 8.15.01
	2.	Een logregel bevat nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden.	BIO2: 8.15.02
	3.	Er is een overzicht van logbestanden die worden gegenereerd.	BIO2: 8.15.03
	4.	De bewaartermijn van logbestanden en gegevens in het Security Incident en Event Monitoring (SIEM) worden risicogericht bepaald, rekening houdend met het scenario dat aanvallers langdurig binnen zijn.	BIO2: 8.15.04
	5.	Actieve netwerkcomponenten zijn voorzien van logging en monitoring van die logging om afwijkende gebeurtenissen te kunnen waarnemen en daarop te reageren.	BIO2: 8.16.04

Activiteiten	6.	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als informatiebeveiligingsincident via de procedure voor informatiebeveiligingsincidenten volgens beheersmaatregel 5.24.	BIO2: 8.15.05
	7.	Op basis van een expliciete risicoafweging bepaalt de organisatie de periodieke toetsing op het ongewijzigd bestaan van logbestanden gedurende de bewaartermijn. Toetsing wordt uitgevoerd door een onafhankelijke functionaris (ten opzichte van de uitvoering).	BIO2: 8.15.06
	8.	De informatieverwerkende omgeving wordt gemonitord met een detectie- en response-oplossing, waarmee aanvallen kunnen worden gedetecteerd en afwijkingen adequaat en tijdig worden behandeld.	BIO2: 8.16.03
	9.	Bij ontdekte nieuwe dreigingen (aanvallen) via overheidsmaatregel 8.16.3 worden deze binnen geldende juridische kaders verplicht gedeeld met de daarvoor aangewezen Computer Emergency Response Team (CERT).	BIO2: 8.16.01
Beoordeeld	10.	De SIEM en/of het SOC-monitoring-proces hebben eenduidige regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	BIO2: 8.16.02
	11.	Bij het verwerken van persoonsgegevens wordt, volgens het gestelde in de AVG, een verwerkingsregister bijgehouden.	CIP-netwerk
Bewaard	12.	De log-bestanden worden gedurende een overeengekomen periode bewaard voor toekomstig onderzoek en toegangscontrole.	CIP-netwerk

5.3.4 *C.04 Beheersorganisatie toegangsbeveiliging*

Objectdefinitie

Doelgerichte bundeling van kennis en vaardigheden tussen personen met taken, verantwoordelijkheden en bevoegdheden voor de beheersing van toegangsbeveiliging en de doorontwikkeling van het afsprakenstelsel.

Objecttoelichting

Voor het adequaat beheersen en beheren van het toegangsbeveiligingssysteem dient een beheersorganisatiestructuur te zijn vastgesteld, waarin de verantwoordelijkheden voor de beheersprocessen met toereikende bevoegdheden zijn uitgedrukt en op het juiste niveau zijn gepositioneerd.

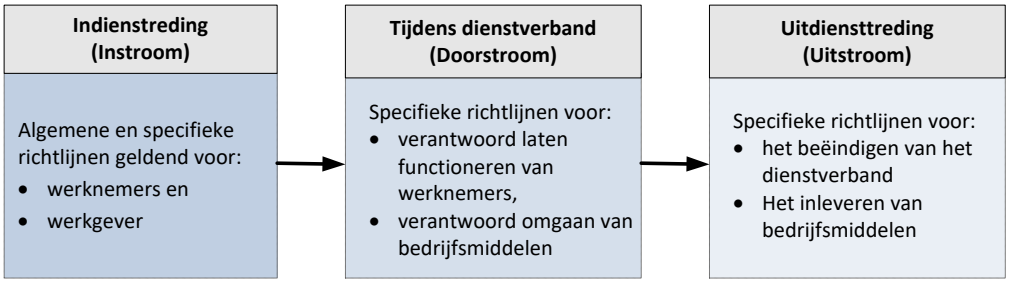
Doelstelling	Het invullen, coördineren en borgen van de beheersing van het toegangsbeveiligingssysteem.
Risico	Als de beheersorganisatiestructuur voor het toegangsbeveiligingssysteem niet duidelijk is vastgesteld en verantwoordelijkheden onvoldoende zijn belegd, bestaat het risico dat het systeem niet effectief wordt beheerd en tekortkomingen in de toegangsbeveiliging ontstaan.

Control	De eigenaar van het toegangsbeveiligingssysteem en de toegangsmiddelen dient een beheersingsorganisatie ingericht te hebben, waarin de **processtructuur**, de **taken, verantwoordelijkheden en bevoegdheden** van de betrokken **functionarissen** zijn vastgesteld.	CIP-netwerk
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**
Proces-structuur	1. De samenhang van de processen wordt met een processtructuur vastgelegd.	CIP-netwerk
Taken, verantwoor-delijkheden en bevoegd-heden	2. De taken, verantwoordelijkheden en bevoegdheden voor de uitvoering van de beheerwerkzaamheden zijn beschreven en de bijbehorende bevoegdheden zijn vastgelegd in een autorisatiematrix.	CIP-netwerk
Functiona-rissen	3. De belangrijkste functionarissen (stakeholders) voor de beheerorganisatie zijn benoemd en de relaties tussen hen zijn met een organisatieschema inzichtelijk gemaakt.	CIP-netwerk

Bijlage 1: Scenario voor toegangsbeveiliging

Hanteer, voor zowel interne als externe medewerkers, bij de inrichting en evaluatie van voorzieningen voor toegangsbeveiliging de volgende fasering (zie afbeelding 4):

- Indiensttreding (instroom)
  In deze fase gelden algemene en specifieke richtlijnen voor de taken en verantwoordelijkheden van de werkgever en de werknemer. De werkgever zal in deze fase, na een zorgvuldige selectieprocedure, de noodzakelijke zaken voor de werknemer moeten regelen.
- Tijdens dienstverband (doorstroom)
  In deze fase worden werknemers, afhankelijk van hun functie, via trainingen en opleidingen bewust gemaakt van het omgaan met bedrijfsmiddelen (onder andere bedrijfsgegevens) en geleerd hoe zij moeten omgaan met aspecten van informatiebeveiliging.
- Uitdiensttreding (uitstroom)
  In deze fase treft de werkgever de noodzakelijke maatregelen voor het beëindigen van het dienstverband. De werknemer zal de aan hem verstrekte bedrijfsmiddelen volgens afgesproken procedure moeten inleveren.



Afbeelding 4: Schematische weergave componenten toegangsbeveiliging in drielagenstructuur

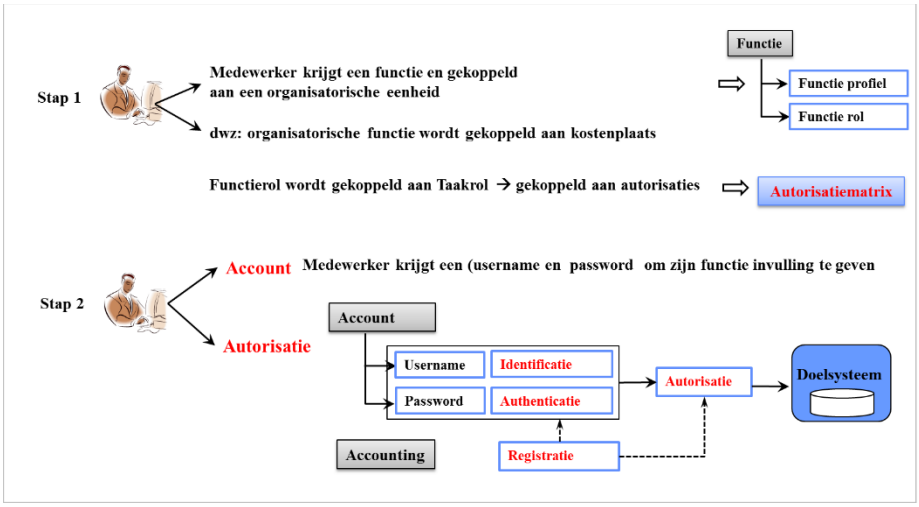
Indiensttreding nieuwe medewerkers

Met het verstrekken van de aanstellingsbeschikking komt een medewerker in dienst. Bij indiensttreding ontvangt de medewerker een toegangspas waarmee hij toegang krijgt tot het terrein, gebouw en de bij de functie horende ruimtes (fysieke toegangsbeveiliging). Naast de fysieke ruimtes krijgt de medewerker ook toegang tot logische ruimtes, oftewel: de persoonlijke en gemeenschappelijke gegevensverzamelingen en tot de algemene kantoorautomatiseringsomgeving, zoals de KA- of de Front-Office omgeving en specifieke applicaties. Voor de werkzaamheden binnen de specifieke applicaties kan hij weer algemene en specifieke rechten krijgen.

Achter de schermen worden heel wat stappen gezet om deze nieuwe medewerker daadwerkelijk in te voeren als een actieve functionaris. Hierbij zijn verschillende afdelingen betrokken:

- De Personeelsafdeling (of Human Resource Management) zorgt voor invoering van de nieuwe medewerker in het personeelsbestand.
- De Facilitaire dienst of Facilitair bedrijf zorgt voor een fysieke werkplek (bureau, stoel etc.) en maakt een toegangspas aan (= identificatiemiddel).
- De Gegevens-/Proceseigenaar zorgt voor een mandaatregister waaruit blijkt welke personen bevoegd zijn voor uitvoering van welke taken (autorisaties).
- De ICT-afdeling zorgt voor ICT-voorzieningen en de geautoriseerde toegang tot benodigde applicaties evenals het authenticatiemiddel (zoals een toegangspas).

Deze stappen staan niet los van elkaar. Zij dienen namelijk één gemeenschappelijk doel: het bieden van geautoriseerde toegang. Meerdere gegevens van de medewerker en meerdere acties vanuit de organisatie zijn daarbij nodig. Eenmaal in dienst, zal de medewerker kennis moeten nemen van de missie/visie van de organisatie en van haar informatiebeveiligingsbeleid. Afbeelding 5 geeft een beeld van de processtappen bij de indiensttreding (instroom) van een medewerker.

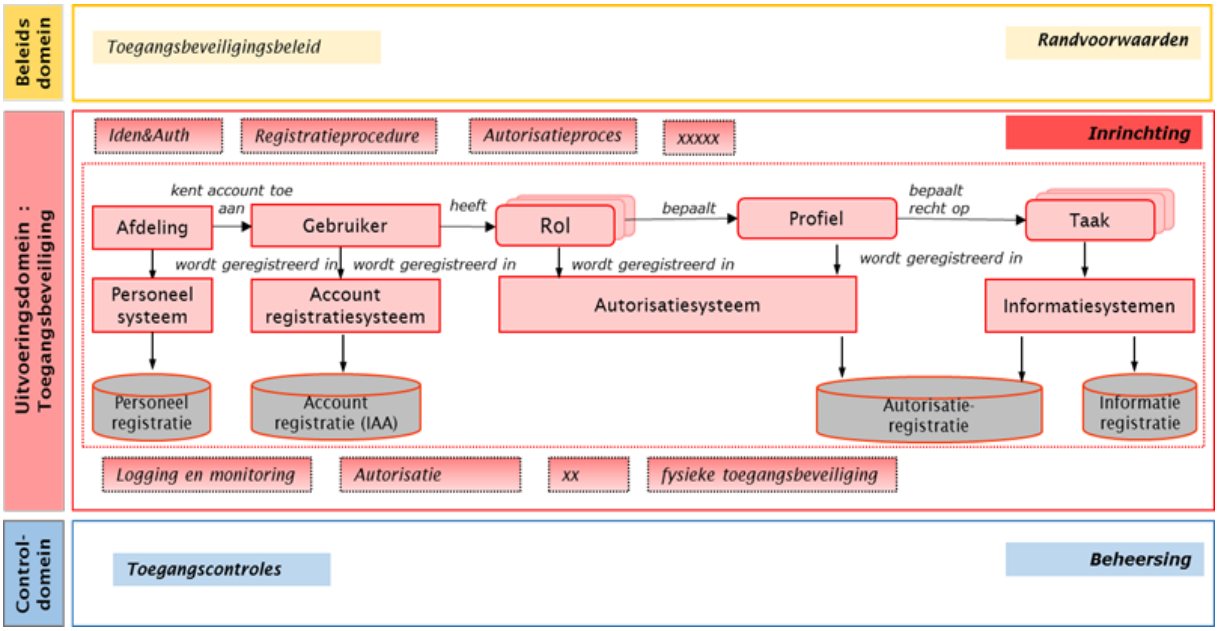


Afbeelding 5: Processtappen en acties bij indiensttreding van een medewerker

Nadat de processtappen en acties bij de indiensttreding van de medewerker zijn doorlopen, is de medewerker geïdentificeerd. De medewerker (gebruiker) bezit dan de nodige middelen, een fysiek toegangsbewijs voor toegang tot terreinen, gebouwen en ruimtes van de organisatie in de vorm van een toegangspas en een logisch toegangsbewijs in de vorm van een account voor toegang tot IV-faciliteiten. De gebruiker krijgt met zijn inloggegevens (identificatie/accountnaam en authenticatie) toegang tot applicaties.

Aan het account, het identificatiebewijs van de gebruiker, zijn toegangsrechten (autorisaties) gekoppeld. Autorisatie (profiel) komt tot stand met de rol van de gebruiker en geeft hem het recht bepaalde taken in de applicatie uit te voeren. Bij doorstroom kan er sprake zijn van wijzigingen van de toegangsgegevens (identificatie, authenticatie en autorisatie). Bij uitstroom is er sprake van blokkering van deze gegevens.

De persoonlijke gegevens van de gebruiker zijn opgeslagen in het personeelssysteem, de rol en het profiel zijn opgeslagen in het autorisatiesysteem. De profielen en de taken zijn op hun beurt weer opgeslagen in het informatiesysteem. Afbeelding 6 geeft hiervan een overzicht.



Afbeelding 6: Schematische weergave autorisatieproces in de domeinen

Tijdens het dienstverband

Tijdens het dienstverband heeft de medewerker (gebruiker) toegang tot de informatiesystemen met de bij de indiensttreding verkregen middelen en toegangsrechten. Voor het beheer van deze middelen moeten fysieke toegangssystemen, authenticatiesystemen en autorisatiesystemen zijn ingericht.

Tijdens het dienstverband kunnen werkzaamheden van medewerkers worden gewijzigd, kan de medewerker van functie/project wisselen of is er sprake van een (tijdelijke) overplaatsing. In al deze gevallen zullen de nodige wijzigingen in functieprofielen (autorisatie) en taakrollen in het registratiesysteem worden doorgevoerd.

Uitdiensttreding

Uiteindelijk zal een medewerker uit dienst treden. Alle toegangsrechten en autorisaties zullen direct na afloop van het dienstverband moeten worden verwijderd.