BIO Baseline Informatiebeveiliging Overheid

CIP centrum informatiebeveiliging en privacybescherming

Rijksoverheid

VNG Vereniging van Nederlandse Gemeenten

Interprovinciaal Overleg ipo

UNIE VAN WATERSCHAPPEN

Huisvesting Informatievoorzieningen

BIO Thema-uitwerking

Mei 2026 [versie 3.0 definitief]

BIO Thema-uitwerking Huisvesting Informatievoorzieningen

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.

Titel	BIO Thema-uitwerking Huisvesting Informatievoorzieningen
Datum	Mei 2026
Versie en status	3.0 def
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-kernteam

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	Mei 2026		CIP
1.1	Februari 2019		CIP
2.0	Januari 2021		CIP
2.1	Mei 2026		CIP
2.2	Maart 2023		CIP
2.3	November 2023	Tekstverbeteringen, BUC-afbeeldingen in tabelvorm, harde enters vervangen, doelstellingen en risico's geüniformeerd	CIP
3.0	Mei 2026	BIO2 v1.3 verwerkt	CIP

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.
- 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.

Voor een overzicht van alle gebruikte best practices, afkortingen en begrippen en een generieke toelichting op de opzet van de thema-uitwerkingen, zie de Structuurwijzer BIO Thema-uitwerkingen.

Inhoudsopgave

Leeswijzer 4

1 Inleiding 9

1.1 Opzet Huisvesting IV 10

1.2 Scope en begrenzing huisvesting IV 11

1.3 Aanpak BIO Thema-uitwerking Huisvesting IV 12

2 Huisvesting IV-objecten 13

2.1 Schematische weergave huisvesting IV-objecten 13

2.2 Beleidsdomein 13

2.3 Uitvoeringsdomein 13

2.4 Control-domein 14

2.5 Organisatie huisvesting IV-objecten 14

3 Beleidsdomein 15

3.1 Doelstelling 15

3.2 Risico’s 15

3.3 Objecten, controls en maatregelen 15

3.3.1 B.01 Huisvesting IV-beleid 15

Objectdefinitie 15

Objecttoelichting 16

3.3.2 B.02 Wet- en regelgeving 17

Objectdefinitie 17

Objecttoelichting 17

3.3.3 B.03 Eigenaarschap 17

Objectdefinitie 17

Objecttoelichting 17

3.3.4 B.04 Certificering 18

Objectdefinitie 18

Objecttoelichting 18

3.3.5 B.05 Contractmanagement 19

Objectdefinitie 19

Objecttoelichting 19

3.3.6 B.06 Service Level Management 20
Objectdefinitie 20
Objecttoelichting 20
3.3.7 B.07 In- en externe bedreigingen 20
Objectdefinitie 20
Objecttoelichting 20
3.3.8 B.08 Training en bewustwording 21
Objectdefinitie 21
Objecttoelichting 21
3.3.9 B.09 Organisatiestructuur huisvesting IV 22
Objectdefinitie 22
Objecttoelichting 22
4 Uitvoeringsdomein 23
4.1 Doelstelling 23
4.2 Risico's 23
4.3 Objecten, controls en maatregelen 23
4.3.1 U.01 Richtlijn gebieden en ruimten 24
Objectdefinitie 24
Objecttoelichting 24
4.3.2 U.02 Bedrijfsmiddelen-inventaris 24
Objectdefinitie 24
Objecttoelichting 25
4.3.3 U.03 Fysieke zonering 25
Objectdefinitie 25
Objecttoelichting 25
4.3.4 U.04 Beveiligingsfaciliteiten 26
Objectdefinitie 26
Objecttoelichting 26
4.3.5 U.05 Nutsvoorziening 27
Objectdefinitie 27
Objecttoelichting 27
4.3.6 U.06 Apparatuur-positionering 28

Objectdefinitie 28
Objecttoelichting 28
4.3.7 U.07 Apparatuur-onderhoud 28
Objectdefinitie 28
Objecttoelichting 28
4.3.8 U.08 Apparatuur-verwijdering 29
Objectdefinitie 29
Objecttoelichting 29
4.3.9 U.09 Opslagmedia beheren 30
Objectdefinitie 30
Objecttoelichting 30
4.3.10 U.10 Laad- en loslocatie 31
Objectdefinitie 31
Objecttoelichting 31
4.3.11 U.11 Bekabeling 32
Objectdefinitie 32
Objecttoelichting 32
4.3.12 U.12 Huisvesting IV-architectuur 33
Objectdefinitie 33
Objecttoelichting 33
5 Control-domein 34
5.1 Doelstelling 34
5.2 Risico’s 34
5.3 Objecten, controls en maatregelen 34
5.3.1 C.01 Controle-richtlijn huisvesting IV 34
Objectdefinitie 34
Objecttoelichting 35
5.3.2 C.02 Onderhoudsplan 35
Objectdefinitie 35
Objecttoelichting 35
5.3.3 C.03 Continuïteitsbeheer 36
Objectdefinitie 36

Objecttoelichting 36

5.3.4 C.04 Beheersorganisatie huisvesting IV 37

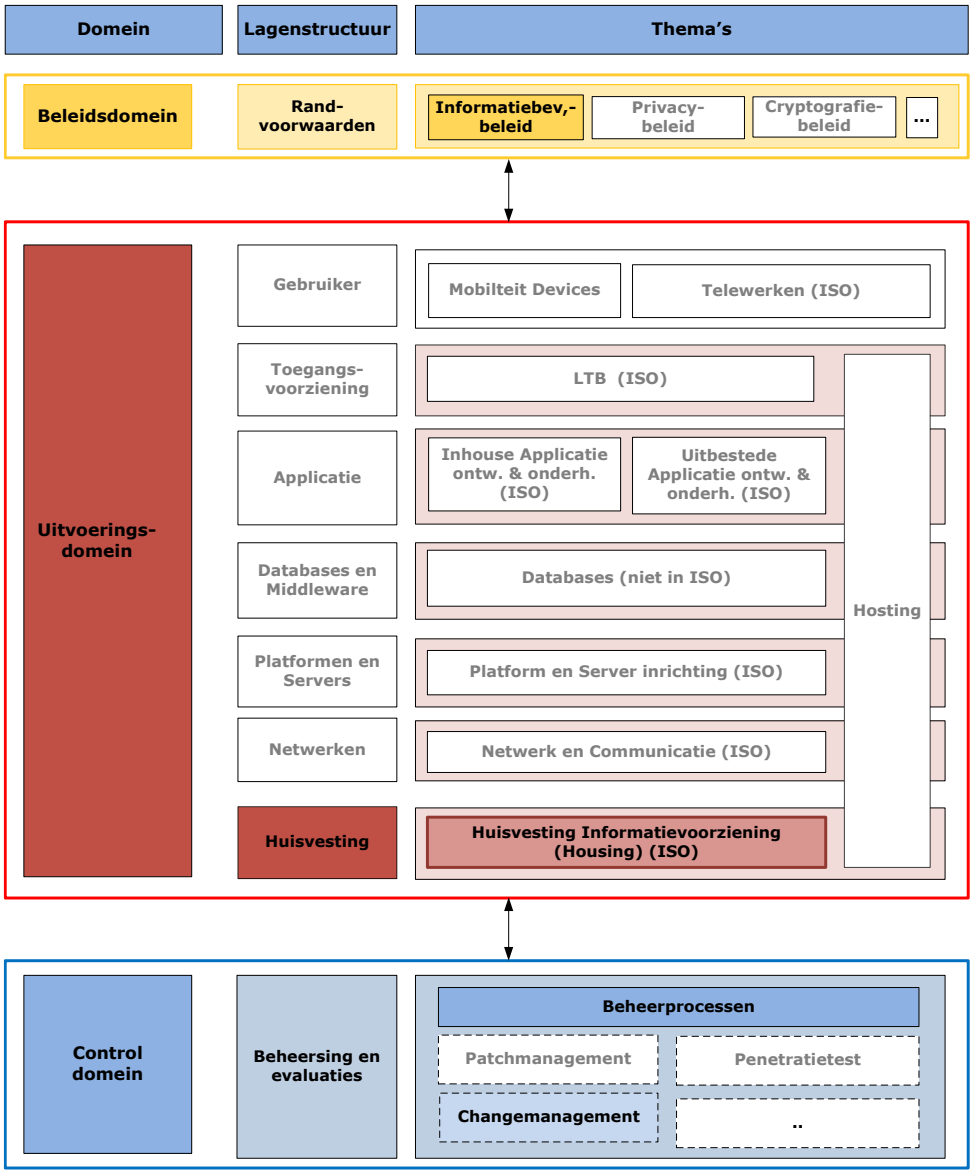
Objectdefinitie 37

Objecttoelichting 37

1 Inleiding

Dit document omvat een referentiekader voor het thema Huisvesting Informatievoorzieningen, hierna genoemd Huisvesting IV. Het bevat een set beveiligingsmaatregelen die zijn gerelateerd aan relevante onderwerpen (objecten) uit de Baseline Informatiebeveiliging Overheid (BIO2). Voor aspecten waarvan de BIO2 onvoldoende praktische invulling geeft, zijn onder andere de volgende best practices geraadpleegd: 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).

Afbeelding 1 geeft de relatie weer tussen de BIO Thema-uitwerking Huisvesting IV en onderwerpen die in de overige BIO Thema-uitwerkingen worden geraakt.

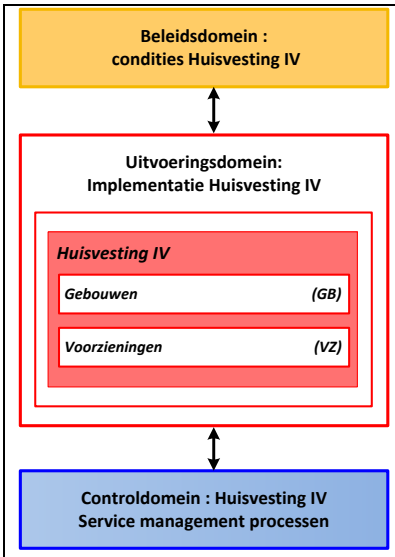


Afbeelding 1: Overzicht BIO-thema's en positie thema Huisvesting IV

1.1 Opzet Huisvesting IV

De inhoudelijke onderwerpen die besproken worden in deze BIO Thema-uitwerking (de objecten) zijn gestructureerd in een drietal domeinen: Beleid, Uitvoering en Control (BUC). Deze objecten vormen de onderwerpen die bij Huisvesting IV van belang zijn. Per domein zijn ze uitgewerkt in de vorm van controls en onderliggende maatregelen. De objecten en de bijbehorende maatregelen gelden zowel voor implementatie- als voor auditdoeleinden.

Afbeelding 2 schetst de structuur waarin een relatie wordt gelegd tussen objecten binnen het beleids-, uitvoerings- en control-domein voor huisvesting IV.



Het beleidsdomein bevat randvoorwaardelijke elementen.

Het uitvoeringsdomein bevat operationele elementen.

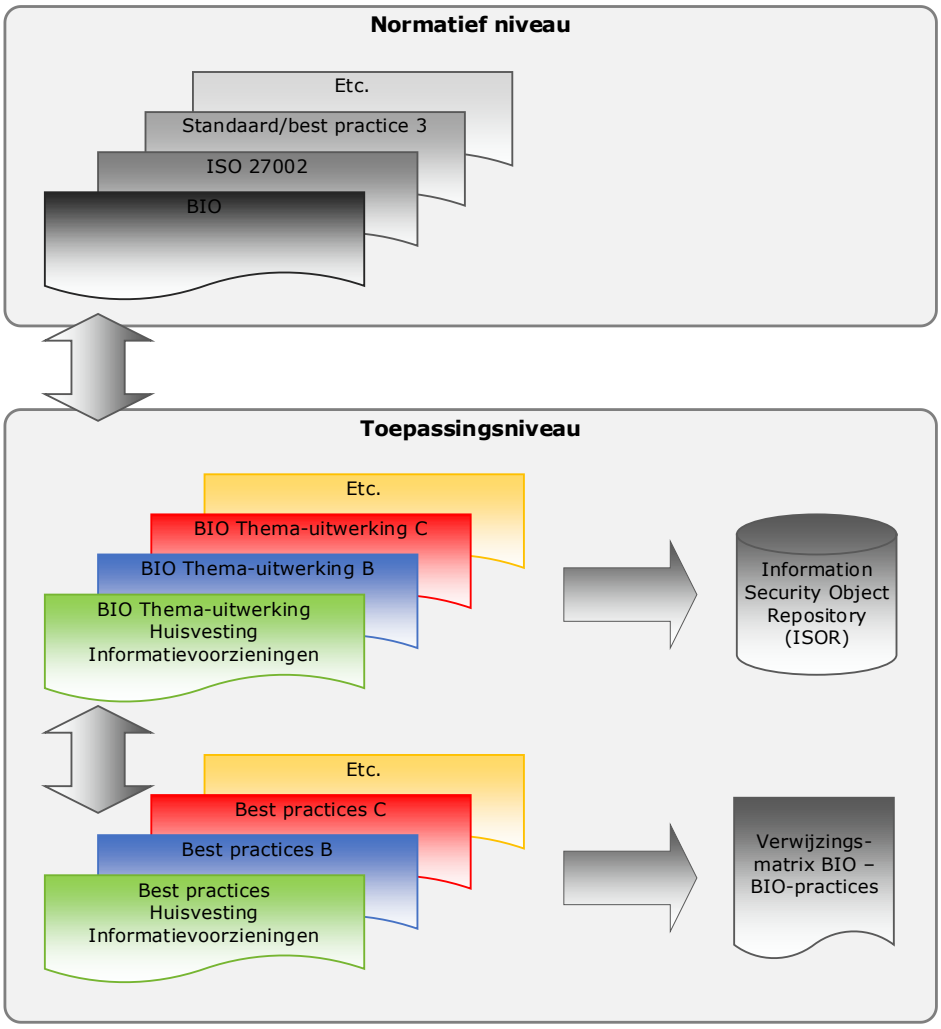
Het control-domein bevat elementen die met het beleid de beheersing waarborgen van het uitvoeringsdomein. Deze elementen zorgen voor de instandhouding van een beveiligings- of serviceniveau. In dit domein wordt ervoor gezorgd dat:

- tijdig beheersende, corrigerende of verbeteracties op de operationele aspecten worden uitgevoerd;
- rapportages gemaakt worden over de stand van zaken voor het hogere management.

Met deze driedeling is de toewijzing van maatregelen vanuit de normen (objecten) zodanig georganiseerd, dat alle noodzakelijke acties bij juiste functionarissen worden geadresseerd.

Afbeelding 2: Relatie tussen objecten in het beleids-, uitvoerings- en control-domein

De relatie tussen deze BIO Thema-uitwerking en de aanpalende documenten is weergegeven in afbeelding 3.



Afbeelding 3: Relatie BIO Thema-uitwerking Huisvesting IV met aanpalende documenten

1.2 Scope en begrenzing huisvesting IV

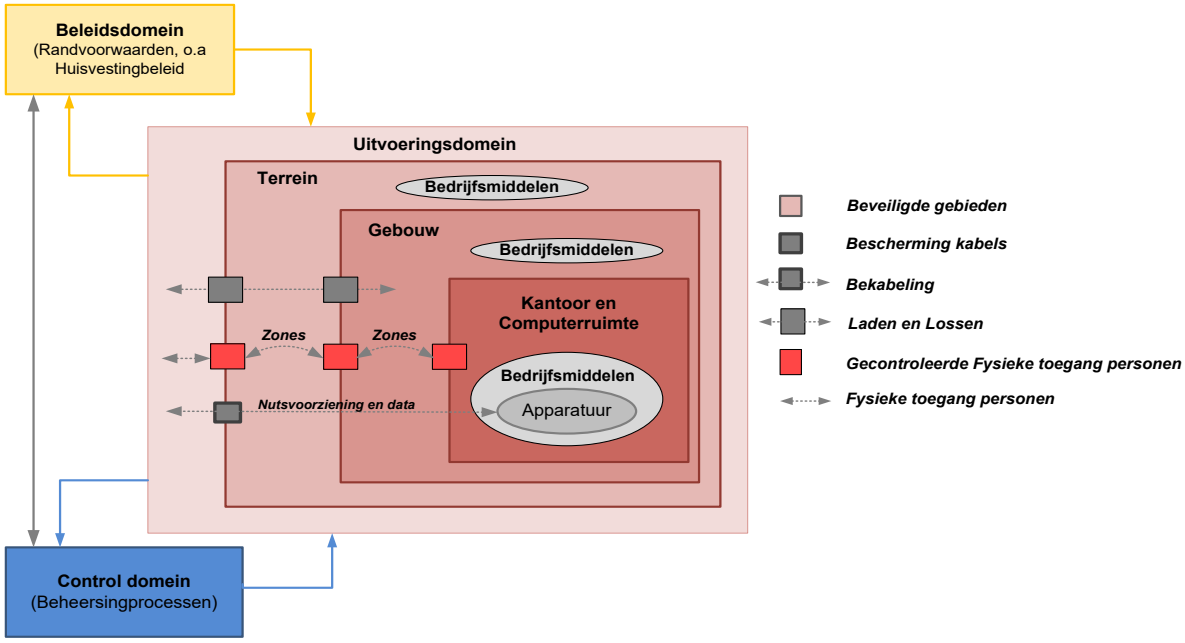
De te stellen eisen aan huisvesting IV worden vooral bepaald door de fysieke bescherming van de apparatuur die gebruikt wordt voor verwerking, transport en opslag van data. Maar ook de vorm waarin huisvesting IV wordt afgenomen speelt een rol. We onderkennen de volgende opties:

1. Fysieke huisvesting
   Bij deze traditionele huisvesting is het rekencentrum ondergebracht binnen één fysieke locatie onder beheer van de doelorganisatie.
2. Modulaire huisvesting
   Bij deze huisvestingsvorm is het rekencentrum ondergebracht in mobiele bouwblokken, die flexibel 'gestapeld' kunnen worden tot de benodigde capaciteit bereikt is (vrachtcontainers).
3. Virtuele huisvesting
   Bij deze vorm is het rekencentrum ondergebracht in een (private of publieke) cloud. Bij deze vorm van huisvesting valt slechts een beperkt deel van de bedrijfsmiddelen onder het technisch

beheer en de bestuurlijke invloed van de doelorganisatie. Men neemt een dienst af en stelt eisen. Hoe groot de invloed van de doelorganisatie is, hangt af van inrichtingskeuzes, maar vooral van de te leveren diensten door leveranciers, zoals Infrastructure as a Service (IaaS), Platform as a Service (PaaS) of Software as a Service (SaaS).

Afhankelijk van de gemaakte inrichtingskeuze voor huisvesting IV zijn normen voor de huisvesting in meer of mindere mate van toepassing.

Dit document beschrijft optie 1 'Fysieke huisvesting' en daarbij de objecten voor huisvesting IV die gerelateerd zijn aan terreinen, gebouwen, ruimten en middelen, zoals aangegeven in afbeelding 4. Vanuit het huisvestingsbeleid (zie hoofdstuk 3 Beleidsdomein) worden de inrichting en beveiliging van de resources binnen het uitvoeringsdomein aangestuurd en met beheersing op de uitvoering wordt grip verkregen op de naleving van de gestelde beveiligingseisen (zie het control-domein).



Afbeelding 2: Overzicht fysieke huisvesting IV

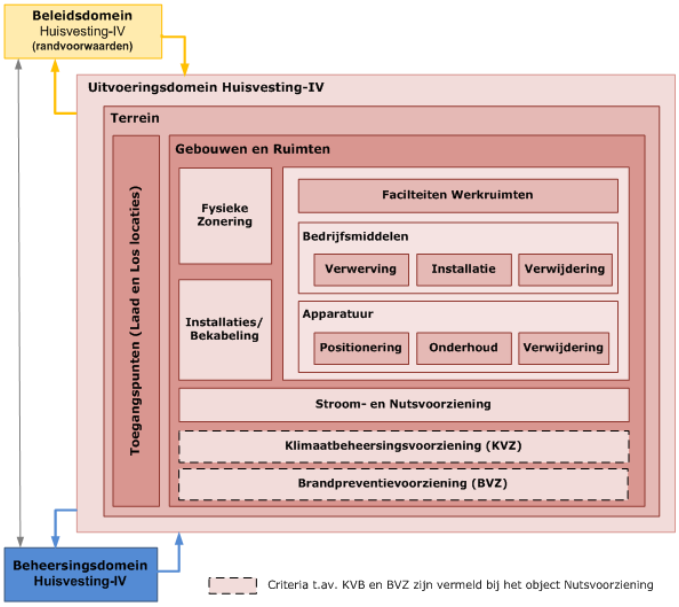
1.3 Aanpak BIO Thema-uitwerking Huisvesting IV

Het toelichtingsdocument schetst de standaardmethodiek waarmee BIO Thema-uitwerkingen worden opgesteld. Een uitgebreide uitwerking van de methodiek is beschreven in het document 'SIVA en toepassingssystematiek'.

2 Huisvesting IV-objecten

2.1 Schematische weergave huisvesting IV-objecten

Huisvesting IV omvat een geheel van objecten voor het leveren van betrouwbare housingdiensten. De essentiële objecten van huisvesting IV worden weergegeven in afbeelding 5. De elementen worden toegelicht in het beleids-, uitvoerings- en control-domein.



Afbeelding 3: Schematische weergave huisvesting IV-objecten

2.2 Beleidsdomein

Het beleidsdomein bevat randvoorwaarden voor huisvesting IV. Objecten die als randvoorwaarden gelden voor de gehele huisvesting IV zijn: beleid, wet- en regelgeving, contracten, organisatiestructuur e.d.

2.3 Uitvoeringsdomein

Het uitvoeringsdomein van huisvesting IV bevat een scala aan componenten die grofweg zijn onder te verdelen in:

- Terrein
  Terrein betreft de locaties van huisvesting IV.
- Gebouwen, faciliteiten en werkruimten
  Dit zijn de objecten waaruit huisvesting IV fysiek bestaat. Hieronder vallen ook de terreinen en de zonering binnen (ruimten van) gebouwen.
- Voorzieningen
  Voorzieningen zijn gerelateerd aan de gebouwen, faciliteiten en werkruimten. Het gaat om bedrijfsmiddelen en nutsvoorzieningen, zoals gas, elektra, water, maar ook brandblussers etc. Daarnaast zijn er bedrijfsmiddelen en specifieke IT-middelen ingezet waarmee huisvesting IV-diensten worden geleverd. Deze middelen zijn continu onderhevig aan veranderingen en

vernieuwingen. Voor een optimale dienstverlening moeten deze middelen onderhouden en/of gecontroleerd worden.

2.4 Control-domein

Het control-domein van huisvesting IV bevat beoordelingsrichtlijnen en procedures. De beoordelingsrichtlijnen zijn vastgesteld voor het evalueren van vastgestelde randvoorwaarden en uitvoeringscomponenten.

2.5 Organisatie huisvesting IV-objecten

Zoals eerder vermeld zijn de beveiligingsobjecten in context geplaatst in de drie verschillende domeinen: beleid, uitvoering en control. De betekenis die aan deze lagen wordt toegekend is als volgt:

1. Beleidsdomein
   Binnen dit domein bevinden zich conditionele elementen betreffende huisvesting IV. Hier zijn eisen opgenomen over geboden en verboden, zoals het huisvesting IV-beleid, de te hanteren wet- en regelgeving en andere vormen van regulering en beperking.
2. Uitvoeringsdomein
   Binnen dit domein bevinden zich:
   - elementen die gerelateerd zijn aan operationele activiteiten van huisvesting IV;
   - elementen die aangeven hoe deze activiteiten georganiseerd moeten zijn;
   - elementen die gerelateerd zijn aan beveiligingsaspecten die bij de activiteiten in acht moeten worden genomen.
3. Control-domein
   Binnen dit domein bevinden zich elementen die zorgdragen voor de beheersing en/of het in stand houden van de activiteiten in relatie tot huisvesting IV en die controleren of deze wel naar wens verlopen.

Objecten worden inclusief omschrijving opgeslagen in de objectenbibliotheek ISOR. ISOR staat voor Information Security Object Repository.

3 Beleidsdomein

3.1 Doelstelling

De doelstelling van het beleidsdomein is het bieden van randvoorwaarden en condities voor het adequaat functioneren van huisvesting IV. In dit hoofdstuk worden de objecten en daaraan gerelateerde normen opgenomen, die het mogelijk maken huisvesting IV-omgevingen op een veilige manier te laten functioneren. De objecten in dit beleidsdomein bieden de organisatie kaders op basis waarvan de beveiliging van huisvesting IV moet plaatsvinden.

3.2 Risico's

Als een door het management uitgevaardigd beleid over huisvesting IV ontbreekt, is het risico dat er onvoldoende sturing wordt gegeven aan de veilige inrichting van huisvesting IV. Het gevolg is bijvoorbeeld schade aan bedrijfsmiddelen en ongeautoriseerde toegang tot gegevens.

3.3 Objecten, controls en maatregelen

Binnen het beleidsdomein worden maatregelen opgenomen die gerelateerd zijn aan bepaalde beveiligingsobjecten. Per object worden conformiteitsindicatoren uitgewerkt. Deze conformiteitsindicatoren representeren een vast te stellen set van maatregelen. De objecten die binnen dit domein een rol spelen, zijn vermeld in tabel 1. De geel gemarkeerde controls komen uit de BIO2. De witte controls komen niet voor in de BIO maar zijn wel noodzakelijk voor deze BIO Thema-uitwerking.

Intentie	Functie	Gedrag	Structuur
B.01 Huisvesting IV-beleid ((Operationeel) beleid)	B.05 Contractmanagement (Proces)	B.08 Training en bewustwording (Educatie en bewustwording)	B.09 Organisatiestructuur huisvesting IV (IT-organisatiestructuur)
B.02 Wet- en regelgeving (Wet)	B.06 Service Level Management (Proces)	/	/
B.03 Eigenaarschap (Eigenaar)	B.07 In- en externe bedreigingen (Beschermingsfunctie)	/	/
B.04 Certificering (Assessment)	/	/	/

Tabel 1: Beleidsobjecten met basiselementen voor huisvesting IV per invalshoek

3.3.1 *B.01 Huisvesting IV-beleid*

Objectdefinitie

Resultaat van een besluitvorming over hoe om te gaan met de aanschaf, inrichting en gebruik van huisvesting IV.

Objecttoelichting

Net als bij het informatiebeveiligingsbeleid geldt ook voor andere beleidstypen dat deze twee aspecten kennen: proces en inhoud. Deze twee aspecten zijn beschreven bij het generieke object 'Informatiebeveiligingsbeleid'. Er wordt hier volstaan met een korte samenvatting.

Een huisvesting IV-beleidsdocument beschrijft een specifiek beleid dat het overkoepelende informatiebeveiligingsbeleid ondersteunt. Omdat het huisvestingsbeleid mede bepaald wordt door externe factoren, zoals wet- en regelgeving, is periodieke review nodig om vast te stellen of het huisvestingsbeleid nog voldoet. Het volstaat dus niet om alleen bij ontwikkelingen binnen de organisatie zelf te kijken of het beleid kan of moet worden aangepast. Door dit proces cyclisch in te richten wordt bereikt dat het huisvestingsbeleid, de ontwikkelingen en de uitvoering steeds op elkaar zijn afgestemd.

Doelstelling	Het zorgen voor een duidelijke richting en focus voor huisvesting IV. Betrokkenen weten welke doelen, doelstellingen en waarden voor huisvesting IV worden nageleefd.		
Risico	Medewerkers raken gedesoriënteerd. Ze hebben moeite met het begrijpen van de huisvesting IV-doelstellingen. Productiviteit en prestaties verminderen. Huisvesting IV voldoet (verwijtbaar) niet aan de actuele en gangbare beveiligingspraktijk. Juridische gevolgen, sancties en reputatieschade kunnen volgen.		
Control	Ten behoeve van het huisvesting IV-beleid behoort een reeks onderwerpspecifieke **beleidsregels** te worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, te worden beoordeeld.		ISO 27002:2022: 5.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Huisvesting IV-beleid	1.	De organisatie heeft een huisvesting IV-beleid opgesteld dat: • de doelstellingen en principes van informatiebeveiliging bevat, afgestemd op de huisvesting-context; • is goedgekeurd door het management; • specifieke verantwoordelijkheden en rollen voor informatiebeveiliging beschrijft; • processen bevat voor het ontwikkelen, vaststellen, goedkeuren, communiceren, implementeren, evalueren en actualiseren van het beleid.	ISO 27002:2022: 5.1
Beleidsregels	2.	Beleidsregels over het huisvesting IV-beleid behandelen eisen die voortkomen uit: • de strategische doelstellingen en randvoorwaarden van de organisatie; • wet- en regelgeving, normen en contractuele verplichtingen; • de huidige en verwachte bedreigingen en risico's voor informatiebeveiliging; • de classificatie en waarde van de te beschermen informatie en systemen.	ISO 27002:2022: 5.1

	3.	Beleidsregels zijn gerelateerd aan specifieke onderwerpen over huisvesting IV, zoals: • fysieke beveiligingszone; • fysieke toegangsbeveiliging.	ISO 27002:2022: 7.1, 7.2

3.3.2 *B.02 Wet- en regelgeving*

Objectdefinitie

Geheel van geldende nationale en internationale wetten en regelgeving dat van toepassing is op huisvesting IV.

Objecttoelichting

Er zijn verschillende wettelijke kaders waaraan de huisvestingsorganisatie moet voldoen, zoals de Algemene Verordening Gegevensbescherming (AVG). Het is een vereiste dat de huisvestingsorganisatie deze kaders in haar beleid geïntegreerd heeft.

Doelstelling	Het voorkomen van schendingen van wetgeving, wettelijke en regelgevende of contractuele verplichtingen en van beveiligingseisen.		
Risico	De organisatie wordt wettelijk aansprakelijk gesteld.		
Control	Alle relevante **wettelijke statutaire, regelgevende, contractuele eisen** en de aanpak van de huisvesting IV-organisatie om aan deze eisen te voldoen behoren voor elke huisvestingsdienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.		ISO 27002:2022: 5.31
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Wettelijke statutaire, regelgevende, contractuele eisen	1.	De organisatie identificeert, beoordeelt en documenteert welke wettelijke, statutaire, regelgevende en contractuele eisen van toepassing zijn op de huisvesting IV. De verantwoordelijke voor de huisvesting IV stelt vast hoe deze eisen worden nageleefd binnen de huisvesting en legt dit vast.	ISO 27002:2022: 5.31
	2.	Het huisvesting IV-beleid waarover de huisvesting IV-organisatie en de klant overeenstemming hebben bereikt, is mede gerelateerd aan alle relevante en specifiek geldende wet- en regelgeving en contractuele verplichtingen.	CIP-netwerk

3.3.3 *B.03 Eigenaarschap*

Objectdefinitie

De toewijzing van de verantwoordelijkheid voor bedrijfsmiddelen voor huisvesting IV.

Objecttoelichting

Binnen huisvesting IV worden verschillende bedrijfsmiddelen toegepast. Voor een betrouwbare dienstverlening door huisvesting IV aan de klanten moeten deze bedrijfsmiddelen continu onderhouden of vernieuwd worden. Ook moeten deze middelen blijvend aan de actuele beveiligingseisen voldoen.

Voor het nemen van de juiste acties voor bedrijfsmiddelen, moet de organisatie de bedrijfsmiddelen toewijzen aan eigenaren. Taken en verantwoordelijkheden moeten worden vastgelegd.

Doelstelling	Van elk bedrijfsmiddel is duidelijk wie in de organisatie verantwoordelijk is voor het actueel houden van de informatie daarover en voor het ondernemen van de noodzakelijke acties.		
Risico	Achterstallig onderhoud veroorzaakt schade. Bedrijfsmiddelen functioneren niet.		
Control	Er behoort een inventarislijst van informatie en andere gerelateerde Huisvesting IV-bedrijfsmiddelen, met inbegrip van de **eigenaren**, te worden opgesteld en onderhouden.		ISO 27002:2022: 5.9 BIO2: 5.09
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Eigenaren	1.	Personen of afdelingen, die door de directie verantwoordelijk zijn gesteld voor de levenscyclus van een huisvesting IV-bedrijfsmiddel, zijn als eigenaar benoemd.	ISO 27002:2022: 5.9
	2.	Het eigenaarschap van een huisvesting IV-bedrijfsmiddel wordt toegekend bij het ontstaan en bij de verwerving van het middel.	ISO 27002:2022: 5.9
	3.	De eigenaar van het huisvesting IV-bedrijfsmiddel is verantwoordelijk voor het juiste beheer gedurende de gehele levenscyclus ervan.	ISO 27002:2022: 5.9
	4.	De eigenaar van het bedrijfsmiddel zorgt ervoor dat: • bedrijfsmiddelen worden geïnventariseerd; • bedrijfsmiddelen passend worden geclassificeerd; • de classificatie en risico's van bedrijfsmiddelen periodiek worden beoordeeld; • passende toegangsbeperkingen en beveiligingsmaatregelen worden gedefinieerd en gehandhaafd; • bedrijfsmiddelen bij einde van de levenscyclus op een veilige wijze worden verwijderd, vernietigd of hergebruikt.	ISO 27002:2022: 5.9, 5,10, 5,12

3.3.4 *B.04 Certificering*

Objectdefinitie

Bewijs, afgegeven door een erkende organisatie, waarmee bevestigd wordt dat huisvesting IV voldoet aan vooraf vastgestelde eisen.

Objecttoelichting

Certificering vindt plaats door een certificatie-instelling. Zo bestaan er bijvoorbeeld verschillende ISO-certificaten die door geaccrediteerde certificatie-instellingen worden afgegeven. Klanten eisen steeds vaker dat het certificaat is behaald voordat zij zaken doen met de betreffende IV-dienstverlener. Om een ISO-certificaat te kunnen behalen, dient aantoonbaar aan een aantal eisen te zijn voldaan. Om aan een ISO-norm te kunnen voldoen, moeten bijvoorbeeld de werkprocessen in de organisatie inzichtelijk zijn gemaakt en dienen ze beheersbaar en bestuurbaar te zijn.

Doelstelling	Het zorgen dat de rekencentra aan het door de opdrachtgever beoogde beveiligingsniveau voldoen.
Risico	Er ontstaat continuïteits- of datalekschade.

Control	Huisvesting IV van de leverancier behoort gecertificeerd te zijn conform de **gangbare standaarden**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gangbare standaarden	1.	De gangbare principes rondom 'Security by design' zijn uitgangspunt voor de ontwikkeling van Huisvesting IV.	CIP-netwerk
	2.	Huisvesting IV die ingezet wordt voor de organisatie is minimaal ISO 27001 (Managementsystemen voor informatiebeveiliging) en ISO 50001 (Energiemanagement) gecertificeerd.	CIP-netwerk

3.3.5 *B.05 Contractmanagement*

Objectdefinitie

Besturing en het beheer van de overeenkomsten tussen de klant en leverancier.

Objecttoelichting

Wanneer (delen van) de ontwikkeling en/of het beheer van huisvesting IV worden uitbesteed, moeten de functionele en beveiligingseisen in een overeenkomst tussen beide partijen worden vastgelegd, zoals in een contract en/of dienstenniveau-overeenkomst (DNO). Deze overeenkomst moet garanderen dat er geen misverstanden bestaan tussen de beide partijen.

Doelstelling	Het zorgen dat huisvesting IV voldoet aan vooraf afgesproken eigenschappen, waaronder het beveiligingsniveau.		
Risico	Er is gebrek aan toetsmiddelen voor de huisvesting IV-organisatie. Er ontstaat schade.		
Control	Huisvesting IV behoort te voldoen aan **kwalitatieve en kwantitatieve eisen** die zijn vastgelegd in **overeenkomsten** met de betreffende leveranciers.		NCSC 2015: B.05 NCSC 2015: C.10
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Kwalitatieve en kwantitatieve eisen	1.	De eisen en specificaties voor huisvesting IV zijn onderdeel van het eisenpakket dat is opgesteld bij de verwerving van de voorzieningen.	NCSC 2015: B.05
Overeen-komsten	2.	Het verwerven van huisvesting IV vindt uitsluitend plaats op basis van een overeenkomst of andere formele afspraak.	CIP-netwerk
	3.	De bij DNO's en Dossier Afspraken en Procedures (DAP's) betrokken rollen Contractmanagement en Service Level Management zijn vastgelegd.	CIP-netwerk
	4.	Afspraken met en activiteiten van leveranciers zijn contractueel vastgelegd in DNO's en DAP's.	CIP-netwerk
	5.	De levering van voorzieningen wordt periodiek geëvalueerd door een onafhankelijke partij.	CIP-netwerk

3.3.6 *B.06 Service Level Management*

Objectdefinitie

Beheersing van het nakomen van de afspraken tussen klant en leverancier over het te leveren serviceniveau.

Objecttoelichting

Service Level Management omvat de afspraken over het definiëren, meten, bewaken en verbeteren van de te leveren kwaliteit en beveiliging van de huisvesting IV-diensten door de leverancier, alsmede het sturen op het nakomen van deze afspraken.

Doelstelling	Het zorgen dat de huisvesting IV-services volgens afspraken geleverd worden.		
Risico	Het serviceniveau en de beveiliging van de huisvesting IV is ontoereikend voor de informatiesystemen die daarvan afhankelijk zijn.		
Control	Het management van huisvesting IV behoort diensten te leveren volgens een **dienstenniveau-overeenkomst** (DNO).		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
dienstenniveau-overeenkomst	1.	De huisvesting IV-organisatie heeft de te leveren diensten en bijbehorende dienstenniveaus beschreven.	CIP-netwerk
	2.	Deze dienstenniveaus zijn in lijn met het huisvesting IV-beveiligingsbeleid.	CIP-netwerk
	3.	De dienstenniveaus zijn onder andere gericht op de aspecten: beschikbaarheid, openstelling, vertrouwelijkheid (zonering) en herstel (disaster recovery).	CIP-netwerk

3.3.7 *B.07 In- en externe bedreigingen*

Objectdefinitie

Weerbaarheid tegen potentiële, fysieke schadelijke invloeden van binnenuit of buitenaf.

Objecttoelichting

Ter bescherming van de Huisvesting IV moet de organisatie voorzieningen treffen tegen zowel interne als externe bedreigingen.

Voorbeelden van interne bedreigingen zijn: foutieve handelingen van medewerkers, zoals het niet onderbrengen van kopieën van kritische data op verschillende locaties, ontwerpfouten of het nalaten van het treffen van beveiligingsmaatregelen.

Externe bedreigingen zijn calamiteiten die veroorzaakt worden door de natuur of door kwaadwillenden. Denk daarbij aan schade door storm, vernieling, overstroming of brand.

Doelstelling	Het zorgen voor een weerbare huisvesting IV. Het voorkomen van verstoringen in huisvesting IV.

Risico	Informatiesystemen en data zijn niet beschikbaar. De aangesloten organisaties ondervinden schade in hun bedrijfsvoeringen.		
Control	Er behoort bescherming tegen fysieke en **omgevingsdreigingen**, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, te worden ontworpen en geïmplementeerd.		ISO 27002:2022: 7.5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Omgevingsdreigingen	1.	De organisatie heeft geïnventariseerd welke data, systemen en apparatuur bedrijfskritisch zijn en welke impact een verstoring hiervan zou hebben.	ISO 27002:2022: 7.5
	2.	Op basis van een expliciete risicoafweging zijn passende beveiligingsmaatregelen genomen om bedrijfskritische data, systemen en apparatuur te beschermen tegen natuurrampen, kwaadwillige aanvallen en ongevallen.	ISO 27002:2022: 7.5
	3.	Bij de huisvesting van bedrijfs kritische middelen wordt rekening gehouden met de kans op en de gevolgen van rampen die worden veroorzaakt door natuur, menselijk handelen of technische storingen.	ISO 27002:2022: 7.5
	4.	De aanwezige brandblusapparatuur wordt jaarlijks op geschiktheid gekeurd door de brandweer of een hiertoe erkend keuringsinstituut.	CIP-netwerk

3.3.8 *B.08 Training en bewustwording*

Objectdefinitie

Formeel proces voor opleiding en het vormen van bewustzijn bij medewerkers over veilig gedrag.

Objecttoelichting

Huisvesting IV kent verschillende organisatorische, procedurele en technische beveiligingsvoorzieningen. Deze voorzieningen zijn onderhevig aan veranderingen. De medewerkers die betrokken zijn bij huisvesting IV dienen doorlopend getraind te worden hoe daarmee om te gaan en hoe te handelen in specifieke situaties en gebeurtenissen. Hiermee wordt een cultuur gecreëerd waarin medewerkers bewust zijn van de gevaren die huisvesting IV bedreigen.

Doelstelling	Het zorgen dat alle werknemers, ingehuurd personeel en externe gebruikers: • zich bewust zijn van bedreigingen en gevaren van huisvesting IV; • continue op de hoogte zijn van het vigerende huisvesting IV-beleid; • continu bewust blijven van relevante maatregelen.	
Risico	Medewerkers handelen onbewust en/of onbekwaam fout. Dit zorgt voor schade.	
Control	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende **bewustzijnsopleiding en -training** te krijgen **en** regelmatige **bijscholing** van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	ISO 27002:2022: 6.3 BIO2: 6.03
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Bewustzijns-opleiding en -training en bijscholing	1.	Binnen huisvesting IV nemen alle medewerkers regelmatig deel aan trainingsprogramma's over beveiligingsbewustwording of aan workshops hierover.	SoGP 2018: PM2.1.1 SoGP 2018: PM2.3
	2.	Aan de medewerkers wordt regelmatig training (e-learning) aangeboden en zij worden regelmatig op de hoogte gesteld van de ontwikkelingen rond rekencentrumbeveiliging met brochures en nieuwsberichten.	SoGP 2018: PM2.2 SoGP 2018: PM2.3

3.3.9 *B.09 Organisatiestructuur huisvesting IV*

Objectdefinitie

Structuur waarin personen met taken, verantwoordelijkheden en bevoegdheden voor huisvesting IV samenwerken.

Objecttoelichting

Om huisvesting IV volgens de eisen te kunnen invullen, moeten verantwoordelijkheden worden toegewezen. Functionarissen moeten de juiste positie hebben in de organisatie en toezien op het naleven van het huisvesting IV-beleid en wet- en regelgeving. Waar nodig moeten zij gepaste acties (laten) uitvoeren. Taken, verantwoordelijkheden en bevoegdheden moeten expliciet zijn benoemd en vastgesteld.

Doelstelling	Het invullen, coördineren en borgen van huisvesting IV.		
Risico	De huisvesting IV-organisatie komt niet effectief tot uitvoering. Er ontstaat schade.		
Control	De huisvesting IV-organisatie behoort voor de te realiseren huisvesting IV een adequate **organisatiestructuur** in te richten en de aan **functionarissen** toe te wijzen **taken, verantwoordelijkheden en bevoegdheden** vast te stellen.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Organisatie-structuur	1.	Binnen de huisvestingsorganisatie hebben de verantwoordelijken voor huisvesting IV een formele positie.	CIP-netwerk
	2.	Voor huisvesting IV is een organisatieschema beschikbaar.	CIP-netwerk
Functionaris-sen	3.	Het organisatieschema toont de rollen/functionarissen binnen de huisvesting IV-organisatie.	CIP-netwerk
Taken, verantwoorde-lijkheden en bevoegdheden	4.	De taken, verantwoordelijkheden en bevoegdheden van de functionarissen binnen huisvesting IV zijn expliciet vastgelegd en belegd.	NCSC 2015: C.01.08

4 Uitvoeringsdomein

4.1 Doelstelling

Het doel van het uitvoeringsdomein voor Huisvesting IV is het waarborgen dat de fysieke toegang tot functionaliteiten is ingericht overeenkomstig specifieke beleidsuitgangspunten van de bedrijfsonderdelen en dat de beveiliging van de huisvesting als geheel in bestaan en werking voldoet aan de eisen die door de organisatie zijn gesteld.

4.2 Risico's

Als de eisen voor de inrichting en exploitatie van de rekencentra niet worden nageleefd, ontstaan continuïteits-, vertrouwelijkheids- en integriteitsrisico's, zoals uitval van bedrijfsfuncties, datalekken en verminking van cruciale persoonsinformatie of bedrijfsgegevens.

4.3 Objecten, controls en maatregelen

Binnen het uitvoeringsdomein zijn specifieke inrichtings- en beveiligingsobjecten voor huisvesting IV beschreven. Elk object is uitgewerkt in een control met conformiteitsindicatoren. Tabel 2 toont de objecten die gebruik maken van de SIVA-methodiek zijn vastgesteld voor huisvesting IV. De rode objecten komen uit de BIO2. Het (enige) witte object komt niet voor in de BIO maar is hier wel van belang.

Intentie	Functie	Gedrag	Structuur
U.01 Richtlijn gebieden en ruimten (Wet)	U.03 Fysieke zonering (Beschermingsfunctie)	U.10 Laad- en loslocatie (Eigenschap)	U.12 Huisvesting IV-architectuur (IT-architectuur)
U.02 Bedrijfsmiddelen-inventaris (Assessment)	U.04 Beveiligingsfaciliteiten (Beschermingsfunctie)	U.11 Bekabeling (Eigenschap)	/
/	U.05 Nutsvoorziening (Beschermingsfunctie)	/	/
/	U.06 Apparatuur-positionering (Taakvereiste)	/	/
/	U.07 Apparatuur-onderhoud (Taakvereiste)	/	/
/	U.08 Apparatuur-verwijdering (Taakvereiste)	/	/
/	U.09 Opslagmedia beheren (Taakvereiste)	/	/

Tabel 2: Uitvoeringsobjecten met basiselementen voor huisvesting IV per invalshoek

4.3.1 *U.01 Richtlijn gebieden en ruimten*

Objectdefinitie

Systematisch ontwikkelde aanbevelingen voor gebieden en werkruimten die als beveiligingszones gehanteerd worden.

Objecttoelichting

Huisvesting IV heeft betrekking op afgebakende terreinen en gebouwen (gebieden) die verschillende werkruimten bevatten. Deze gebieden en werkruimten moeten, afhankelijk van het type activiteiten en de informatie die binnen deze ruimten worden verwerkt, worden beveiligd. Richtlijnen voor activiteiten, gedrag, procedures, controles e.d. zijn nodig en moeten worden toegepast.

Doelstelling	Veilig en gecontroleerd gedrag in - en beheer van - beveiligde ruimten.		
Risico	Onbevoegde personen brengen ongewenste wijzigingen aan. De bedrijfsvoering wordt verstoord. Er ontstaat schade.		
Control	Voor het werken in beveiligde zones behoren **beveiligingsmaatregelen** te worden ontwikkeld en geïmplementeerd.		ISO 27002:2022: 7.6
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
beveiligings maatregelen	1.	Het personeel met de bevoegdheid 'need-to-know' is alleen bekend met het bestaan van de activiteiten in een beveiligde zone.	ISO 27002:2022: 7.6
	2.	In het belang van de veiligheid en ter beperking van de kans op kwaadaardige activiteiten, wordt in de beveiligde gebieden alleen gewerkt onder toezicht.	ISO 27002:2022: 7.6
	3.	Leegstaande beveiligde ruimten behoren fysiek afgesloten en periodiek geïnspecteerd te zijn.	ISO 27002:2022: 7.6
	4.	Tenzij goedgekeurd, wordt beeld- en geluidsopnameapparatuur, zoals in mobiele apparatuur, niet toegelaten in de beveiligde ruimten.	ISO 27002:2022: 7.6
	5.	Bezoekers van kritieke faciliteiten: • worden slechts toegang geboden voor vastgestelde doeleinden; • worden continu aan toezicht onderworpen; • worden gemonitord bij aankomst en vertrek; • krijgen instructie over de beveiliging van de omgeving en van de noodprocedures en worden bewust gemaakt van de beveiligingsregels; • wordt verteld dat het gebruik van beeld- en geluidopnamemateriaal/apparatuur niet is toegestaan; • dragen verplicht een badge.	SoGP 2018: LC 2.1.8

4.3.2 *U.02 Bedrijfsmiddelen-inventaris*

Objectdefinitie

Registratie van alle tot het bedrijfsproces behorende middelen.

Objecttoelichting

In de huisvesting van de rekencentra zijn verschillende bedrijfsmiddelen, voorzieningen en hieraan gerelateerde componenten opgenomen, zoals glasvezel en bekabeling, back-upvoorzieningen, klimaatbeheersing, airconditioning en geavanceerde brandblussystemen. Het is van belang de componenten van deze voorzieningen zelf en de informatie over deze voorzieningen te inventariseren en te registreren, zodat de juiste informatie beschikbaar is wanneer nodig.

Doelstelling	Het zorgen dat adequate informatie beschikbaar is wanneer het noodzakelijk is.		
Risico	Er wordt niet tijdig actie ondernomen wanneer omstandigheden het vereisen.		
Control	Bedrijfsmiddelen die samenhangen met informatie en informatie-verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een **inventaris** te worden opgesteld en onderhouden.		ISO 27002:2022: 5.9
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Inventaris	1.	De organisatie identificeert bedrijfsmiddelen en onderhoudt een inventaris van alle informatie en andere gerelateerde bedrijfsmiddelen die relevant zijn voor de huisvesting IV.	ISO 27002:2022: 5.9
	2.	Voor elk geïnventariseerd bedrijfsmiddel wordt ten minste vastgelegd: • de levenscyclusfase(n) waarin het bedrijfsmiddel zich bevindt (aanmaak, verwerking, opslag, overdracht, verwijdering of vernietiging); • de eigenaar van het bedrijfsmiddel; • de classificatie van de informatie.	ISO 27002:2022: 5.9, 5,10, 5,12
	3.	De inventaris van bedrijfsmiddelen is actueel, consistent, nauwkeurig en wordt periodiek beoordeeld en bijgewerkt.	ISO 27002:2022: 5.9
	4.	De inventaris wordt zodanig opgesteld en onderhouden dat deze kan worden gebruikt voor onder andere risicobeoordelingen, financiële administratie, verzekeringen, beveiligingsmaatregelen en naleving van wet- en regelgeving.	ISO 27002:2022: 5.9

4.3.3 *U.03 Fysieke zonering*

Objectdefinitie

Fysieke scheiding en gecontroleerde doorgang tussen terreinen, gebouwen en ruimten.

Objecttoelichting

Bij het indelen in beveiligde zones (zonering) gaat het enerzijds om het scheiden van verantwoordelijkheidsgebieden en anderzijds om het mogelijk maken van gecontroleerde doorgang tussen de gedefinieerde gebieden. Voor huisvesting IV gaat het om barrières met de verschillende doorgangen daarin.

Doelstelling	Het voorkomen van onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie.		
Risico	Het niet kunnen voorkomen dat bedreigingen in het ene verantwoordelijkheidsgebied schade veroorzaken in een ander verantwoordelijkheidsgebied.		
Control	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door **beveiligingszones** te definiëren en te gebruiken.		ISO 27002:2022: 7.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-zones	1.	Voor het inrichten van beveiligingszones wordt rekening gehouden met relevante wet- en regelgeving, normen en standaarden.	ISO 27002:2022: 7.1
	2.	Beveiligingszones worden gedefinieerd waarbij de locatie en de sterkte van elke zone afhangen van de beveiligingseisen van de bedrijfsmiddelen die zich binnen de zone bevinden en van de resultaten van een risicobeoordeling.	ISO 27002:2022: 7.1
	3.	Informatieverwerkende faciliteiten die worden beheerd door de organisatie zijn fysiek of logisch gescheiden van informatieverwerkende faciliteiten die door externe partijen worden beheerd.	ISO 27002:2022: 7.1
	4.	Kritieke informatie of informatiesystemen zijn nooit via één beveiligde zone te bereiken.	BIO2: 7.01.02
	5.	Medewerkers en bezoekers dragen in beveiligde zones zichtbaar een geldig identificatiemiddel. Toegang tot niet-publieke ruimten is uitsluitend toegestaan met geldige identificatie en onder begeleiding van bevoegd personeel indien nodig.	ISO 27002:2022: 7.2
	6.	Alle fysieke toegangen tot beveiligde zones worden gecontroleerd. Toegangspogingen worden vastgelegd in een logboek of elektronisch systeem.	ISO 27002:2022: 7.2
	7.	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

4.3.4 *U.04 Beveiligingsfaciliteiten*

Objectdefinitie

Faciliteiten waarmee bedrijfsmiddelen binnen ruimten beveiligd worden.

Objecttoelichting

De rekencentra bevatten verschillende typen ruimten, zoals kantoren, bekabelingsruimten en serverruimten. Deze ruimten moeten conform de beveiligingsgraad van deze ruimten voorzien zijn van beveiligingsfaciliteiten.

Doelstelling	Het voorkomen van onbevoegde toegang tot ruimten.

Risico	Ongeautoriseerden hebben toegang tot beveiligde ruimten en veroorzaken schade aan de eigendommen van de organisatie.		
Control	Voor kantoren, ruimten en **faciliteiten** behoort fysieke beveiliging te worden ontworpen en geïmplementeerd.		ISO 27002:2022: 7.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Faciliteiten	1.	Essentiële faciliteiten zijn zo gelegen dat ze niet voor iedereen toegankelijk zijn.	ISO 27002:2022: 7.3
	2.	Faciliteiten zijn zo geconfigureerd dat wordt voorkomen dat vertrouwelijke informatie of activiteiten van buitenaf zichtbaar en hoorbaar zijn; voor zover van toepassing wordt ook elektromagnetische afscherming overwogen.	ISO 27002:2022: 7.3
	3.	Adresboeken en interne telefoonboeken waarin locaties worden aangeduid met faciliteiten die vertrouwelijke informatie verwerken, zijn niet vrij toegankelijk voor onbevoegden.	ISO 27002:2022: 7.3
	4.	Toegang tot sleutels, toegangspassen en andere middelen voor fysieke toegang tot beveiligde faciliteiten wordt beheerst via een sleutelplan of vergelijkbaar beheerproces.	ISO 27002:2022: 7.2, 7.3

4.3.5 *U.05 Nutsvoorziening*

Objectdefinitie

Product dat door een nutsbedrijf geleverd wordt.

Objecttoelichting

Een nutsvoorziening is een algemene voorziening, zoals elektriciteit, telecommunicatie, water, gas, riolering, ventilatie en airconditioning. Nutsvoorzieningen dienen zo te zijn geïnstalleerd of gerealiseerd dat onderbreking hiervan niet kan leiden tot verstoringen in de apparaten die zich binnen de huisvesting IV-organisatie bevinden.

Doelstelling	Het bewerkstelligen dat het disfunctioneren van nutsvoorzieningen geen negatieve invloed heeft op de beschikbaarheid van de huisvesting IV-dienstverlening.		
Risico	De gehuisveste IV is niet beschikbaar.		
Control	Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in **nutsvoorzieningen**.		ISO 27002:2022: 7.11
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Nutsvoor-zieningen	1.	Nutsvoorzieningen voldoen aan de technische specificaties van de fabrikant en aan de geldende wet- en regelgeving. Zij worden regelmatig geïnspecteerd, getest en onderhouden om te waarborgen dat zij betrouwbaar functioneren en voldoende capaciteit hebben.	ISO 27002:2022: 7.11

	2.	Er zijn noodvoorzieningen aanwezig voor verlichting en communicatie, zodat bij uitval van de primaire nutsvoorzieningen de veiligheid en operationele continuïteit gewaarborgd blijven.	ISO 27002:2022: 7.11
	3.	Nabij nooduitgangen en ruimten waar apparatuur aanwezig is, zijn noodschakelaars en knoppen waarmee stroom, water, gas of andere voorzieningen kunnen worden uitgeschakeld.	ISO 27002:2022: 7.11
	4.	Netwerkverbindingen zijn redundant uitgevoerd via meerdere routes en bij voorkeur via meer dan één leverancier.	ISO 27002:2022: 7.11

4.3.6 *U.06 Apparatuur-positionering*

Objectdefinitie

Veilige plaatsing van apparatuur binnen huisvesting IV.

Objecttoelichting

In huisvesting IV bevindt zich verschillende apparatuur. Deze apparatuur dient zo te zijn gepositioneerd en beschermd dat verlies, diefstal, compromittering en onderbreking van bedrijfsmiddelen wordt voorkomen.

Doelstelling	Het verkleinen van risico's van bedreigingen en gevaren van buitenaf en de kans op onbevoegde toegang.		
Risico	Verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.		
Control	Apparatuur behoort effectief te worden **geplaatst en beschermd**.		ISO 27002:2022: 7.8
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Geplaatst en beschermd	1.	Apparatuur en informatieverwerkende en opslagfaciliteiten worden zodanig geplaatst dat onbevoegden hier geen toegang toe hebben en beveiligd zijn tegen onbevoegde kennisname van gegevens.	ISO 27002:2022: 7.8
	2.	Apparatuur wordt beschermd tegen bedreiging (zoals overspanning, blikseminslag, diefstal en weglekken van informatie door elektromagnetische straling) van buitenaf.	ISO 27002:2022: 7.8

4.3.7 *U.07 Apparatuur-onderhoud*

Objectdefinitie

Instandhouding van apparatuur binnen huisvesting IV.

Objecttoelichting

Apparaten, zoals installaties en machines, moeten voor veilige toepassing periodiek en volgens de juiste procedures worden onderhouden door geautoriseerde medewerkers of leveranciers.

Doelstelling	Het zorgen dat apparatuur continu beschikbaar en integer is.

Risico	Ongeautoriseerde toegang zorgt voor schade door en onvoldoende beschikbaarheid van falende apparatuur.		
Control	Apparatuur behoort op de juiste wijze te worden **onderhouden** om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.		ISO 27002:2022: 7.13
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Onderhouden	1.	Apparatuur wordt in overeenstemming met de door de leverancier aanbevolen frequentie voor servicebeurten en voorschriften onderhouden.	ISO 27002:2022: 7.13.a
	2.	Reparaties en onderhoudsbeurten aan apparatuur worden alleen uitgevoerd door bevoegd onderhoudspersoneel, waarbij toezicht wordt gehouden op onderhoudspersoneel tijdens het uitvoeren van onderhoud ter plaatse.	ISO 27002:2022: 7.13.c,f
	3.	Passende beheersmaatregelen worden geïmplementeerd wanneer onderhoud van apparatuur is gepland, rekening houdend met of dit onderhoud wordt uitgevoerd door personeel ter plaatse of door extern personeel, waarbij het onderhoudspersoneel gehouden is aan een passende geheimhoudingsovereenkomst. De toegang voor onderhoud op afstand wordt op basis van autorisaties toegestaan en beveiligd.	ISO 27002:2022: 7.13.e,g
	4.	Van alle vermeende en daadwerkelijke fouten en van al het preventieve en correctieve onderhoud worden registraties bijgehouden.	ISO 27002:2022: 7.13.d
	5.	Voldaan wordt aan alle onderhoudseisen die door verzekeringspolissen zijn opgelegd.	ISO 27002:2022: 7.13.i
	6.	Voordat apparatuur na onderhoud weer in bedrijf wordt gesteld, wordt een inspectie uitgevoerd om te waarborgen dat niet met de apparatuur geknoeid is en dat deze naar behoren functioneert.	ISO 27002:2022: 7.13.j

4.3.8 *U.08 Apparatuur-verwijdering*

Objectdefinitie

Veilig en gecontroleerd verwijderen van apparatuur binnen huisvesting IV.

Objecttoelichting

Apparaten kunnen cruciale data bevatten. Het verwijderen van apparatuur moet daarom veilig met vastgestelde procedures plaatsvinden.

Doelstelling	Het zorgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik van apparatuur zijn verwijderd of betrouwbaar veilig zijn overschreven.
Risico	Ongeautoriseerden beschikken over gevoelige gegevens en software.

Control	Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden **gecontroleerd** om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan **verwijdering** of hergebruik zijn verwijderd **of betrouwbaar veilig zijn overschreven**.		ISO 27002:2022: 7.14
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gecontroleerd	1.	Voorafgaand aan verwijdering, hergebruik of afvoer van apparatuur of opslagmedia, wordt gecontroleerd of alle gevoelige informatie veilig is verwijderd of onherstelbaar gewist.	ISO 27002:2022: 7.14
Verwijdering of betrouwbaar veilig zijn overschreven	2.	Opslagmedia die vertrouwelijke informatie bevatten, worden niet met de standaard delete-functie gewist, maar fysiek vernietigd of onherstelbaar gewist met gevalideerde technieken.	ISO 27002:2022: 7.14
	3.	Bij het einde van een huurovereenkomst of bij verhuizing worden beveiligingsbeheersmaatregelen (zoals toegangscontrolesystemen, bewakingsapparatuur en andere fysieke beveiligingsmiddelen) verwijderd, tenzij deze in de nieuwe locatie kunnen worden hergebruikt of de huurovereenkomst anders vereist.	ISO 27002:2022: 7.14
	4.		

4.3.9 *U.09 Opslagmedia beheren*

Objectdefinitie

Opslagmedia (inclusief harde schijven, SSD's, USB-drives, tapes en andere dragers) worden gedurende hun volledige levenscyclus – van aanschaf tot verwijdering of vernietiging – beheerd en beveiligd.

Objecttoelichting

In de context van huisvesting IV waarborgt deze beheersmaatregel dat opslagmedia die informatie bevatten (zoals servers, back-upmedia, werkstations of apparatuur in technische ruimten) niet leiden tot ongeautoriseerde blootstelling van vertrouwelijke of gevoelige gegevens bij hergebruik, transport, verwijdering of afvoer. Verwijdering en afvoer van deze middelen dient nauwkeurig met vastgestelde procedures te worden uitgevoerd.

Doelstelling	Het zorgen voor een gecontroleerde verwijdering en afvoer van bedrijfsmiddelen.		
Risico	Bedrijfsmiddelen worden misbruikt door het ontbreken van procedures voor de behandeling van bedrijfsmiddelen.		
Control	**Opslagmedia** behoren te worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.		ISO 27002:2022: 7.10
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Bedrijfsmiddelen	1.	In het beveiligingsbeleid is geborgd dat het invoeren en afvoeren van bedrijfsmiddelen volgens een vaste procedure plaatsvindt. Onderdeel van deze procedure is een formeel toestemmingstraject.	ISO 27002:2022: 7.10

	2.	De organisatie heeft procedures vastgesteld voor het veilig hergebruiken en verwijderen van opslagmedia, afgestemd op de gevoeligheid en classificatie van de informatie die daarop is opgeslagen.	ISO 27002:2022: 7.10
	3.	Opslagmedia met vertrouwelijke informatie worden voorafgaand aan hergebruik binnen de organisatie op een beveiligde wijze gewist of geformatteerd.	ISO 27002:2022: 7.10
	4.	Opslagmedia die niet meer nodig zijn, worden op een veilige en onherstelbare wijze verwijderd of vernietigd. Bij de keuze voor een externe leverancier voor inzameling en vernietiging wordt zorgvuldig gecontroleerd of deze leverancier voldoende waarborgen en ervaring heeft.	ISO 27002:2022: 7.10
	5.	De verwijdering of vernietiging van opslagmedia wordt geregistreerd om een audittraject te waarborgen. Bij het verzamelen van grote hoeveelheden media wordt rekening gehouden met het aggregatie-effect.	ISO 27002:2022: 7.10
	6.	Er wordt gecontroleerd of alle data op het medium onherstelbaar verwijderd is. Hiervan wordt verslag gemaakt. Er wordt waar mogelijk gebruik gemaakt van producten waarvoor de Unit Weerbaarheid van het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een positief inzetadvies afgegeven heeft.	BIO2: 7.10.02

4.3.10 *U.10 Laad- en loslocatie*

Objectdefinitie

Specifiek toegangspunt voor het laden en lossen van goederen op terreinen en in gebouwen.

Objecttoelichting

De rekencentra kennen een of meerdere toegangspunten voor het laden en lossen. Deze toegangspunten kunnen potentiële zwakheden in de beveiliging van de rekencentra vormen. De laad- en lostoegangspunten moeten daarom van specifieke maatregelen zijn voorzien.

Doelstelling	Het voorkomen van onbevoegde toegang tot de laad- en loslocatie en andere ruimten.		
Risico	Diefstal van gegevensdragers en informatie, schade aan bedrijfsmiddelen en verstoringen van activiteiten.		
Control	**Toegangspunten,** zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van IT-voorzieningen.		ISO 27002:2022: 7.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Toegangs-punten	1.	Er is een procedure voor het omgaan met verdachte brieven en pakketten in postkamers en laad- en losruimten.	CIP-netwerk

	2.	Toegang tot een laad- en loslocatie van buiten het gebouw wordt beperkt tot geïdentificeerd en bevoegd personeel.	ISO 27002:2022: 7.2
	3.	De laad- en loslocaties zijn zo ontworpen dat goederen kunnen worden geladen en gelost zonder dat de leverancier toegang heeft tot andere delen van het gebouw.	ISO 27002:2022: 7.2
	4.	De buitendeuren van een laad- en loslocatie moeten beveiligd zijn als de binnendeuren open zijn.	ISO 27002:2022: 7.2
	5.	Inkomende materialen worden bij binnenkomst op de locatie geregistreerd volgens de procedures voor bedrijfsmiddelenbeheer.	ISO 27002:2022: 7.2
	6.	Inkomende en uitgaande zendingen worden, voor zover mogelijk, fysiek gescheiden.	ISO 27002:2022: 7.2
	7.	Inkomende materialen worden gecontroleerd op mogelijke aanwijzingen voor vervalsing tijdens het transport. Bij ontdekte vervalsing wordt dit direct aan het beveiligingspersoneel gemeld.	ISO 27002:2022: 7.2

4.3.11 *U.11 Bekabeling*

Objectdefinitie

Middelen voor transport van energie en telecommunicatie.

Objecttoelichting

Binnen huisvesting IV is alle apparatuur verbonden met een bekabelingssysteem dat in speciale kabelruimten is geïnstalleerd. Deze bekabelingsruimten kunnen doelwit worden van misbruik, zoals het aftappen met behulp van speciale afluisterapparatuur. Het is daarom noodzakelijk om deze bekabelingsruimten te voorzien van specifieke beveiligingsmaatregelen.

Doelstelling	Het zorgen dat de bekabeling robuust is.		
Risico	Het bekabelingssysteem wordt misbruikt.		
Control	**Voedingskabels** en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen onderschepping, interferentie of beschadiging.		ISO 27002:2022: 7.12
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Voedings-kabels	1.	Kabels worden zoveel mogelijk ondergronds of op een andere veilige wijze aangelegd om fysieke schade en ongeoorloofde toegang te voorkomen.	ISO 27002:2022: 7.12
	2.	Huisvesting IV is ingericht met de volgende best practices: • TIA-942: Telecommunication Infrastructure Standard for Data Centers • NEN-EN 50600: Europese normenreeks voor datacenters • NPR 5313: Richtlijn voor datacenters (2014)	CIP-netwerk
	3.	Voedings- en telecommunicatiekabels zijn beveiligd en niet toegankelijk voor onbevoegden.	ISO 27002:2022: 7.12

4.3.12 *U.12 Huisvesting IV-architectuur*

Objectdefinitie

Modelmatige beschrijving van de technische en organisatorische samenhang, waarin de relaties tussen de onderdelen van huisvesting IV zijn vastgelegd.

Objecttoelichting

De architectuur van huisvesting IV geeft overzicht en inzicht in de wijze waarop de gebieden en objecten zijn of dienen te worden beveiligd en biedt inzicht in de samenhang en de samenwerking van beveiligingsmaatregelen.

In de architectuur zijn gemaakte ontwerp- en inrichtingskeuzen gedocumenteerd, verantwoord en de gemaakte keuzen zijn onderbouwd. Tegelijkertijd speelt documentatie een (belangrijke) rol bij het bepalen van de impact van wijzigingen en het voorkomen van fouten. Documentatie moet dan ook na elke wijziging worden bijgewerkt en oude documentatie moet worden gearchiveerd.

Doelstelling	Het bieden van een huisvesting IV-landschap dat in samenhang beveiligd is. Het geeft inzicht in de inrichting van de fysieke voorzieningen.		
Risico	Geen goed zicht op de samenhang van beveiligingsmaatregelen, waardoor bedreigingen over het hoofd worden gezien en de kans op uitbuiting door kwaadwillenden toeneemt.		
Control	Voor het implementeren en onderhouden van huisvestingsvoorzieningen behoren **architectuurvoorschriften** en benodigde **documentatie** beschikbaar te zijn.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Architectuur-voorschriften	1.	De aanwezige architectuurvoorschriften voor de fysieke inrichting van huisvesting IV worden actief onderhouden.	CIP-netwerk
	2.	De inrichting van huisvesting IV en bekabelingen is gedocumenteerd.	CIP-netwerk
Documentatie	3.	Het document met de inrichting van huisvesting IV en de bekabeling: • heeft een eigenaar; • is voorzien van een datum en versienummer; • bevat een documenthistorie (wat is wanneer en door wie aangepast); • is actueel, juist en volledig; • is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.	CIP-netwerk

5 Control-domein

5.1 Doelstelling

Het doel van het control-domein voor deze BIO Thema-uitwerking is vast te stellen in hoeverre:

- de controls voldoende zijn ingericht en functioneren voor het leveren van het gewenste niveau van beveiliging van de huisvesting IV;
- de huisvesting IV en de bedrijfsmiddelen fysiek en technisch op het juiste niveau van onderhoud worden gehouden en de beveiliging ervan kan worden gegarandeerd.

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

5.2 Risico's

Door het ontbreken van noodzakelijke maatregelen binnen de huisvesting IV-organisatie bestaat het risico dat huisvesting IV niet aan de beoogde organisatorische en beveiligingsvoorwaarden voldoet en dat de governance van deze omgeving toereikend is ingericht. Daarnaast kan niet worden vastgesteld dat de gewenste maatregelen worden nageleefd.

5.3 Objecten, controls en maatregelen

Tabel 3 toont de objecten die voor huisvesting IV een rol spelen. De ongenummerde objecten worden later uitgewerkt. Dit zijn mogelijk relevante objecten.

Intentie	Functie	Gedrag	Structuur
C.01 Controle-richtlijn huisvesting IV (Wet)	C.03 Continuïteitsbeheer (Proces)	Monitoring bedrijfsmiddelen (Handeling)	C.04 Beheersorganisatie huisvesting IV (IT-organisatiestructuur)
C.02 Onderhoudsplan (Middel)	Testproces bedrijfsmiddelen (Proces)	/	Beheersingsarchitectuur huisvesting IV (IT-architectuur)
/	Beheerprocessen bedrijfsmiddelen (Proces)	/	/

Tabel 3: Control-objecten met basiselementen voor huisvesting IV per invalshoek

5.3.1 *C.01 Controle-richtlijn huisvesting IV*

Objectdefinitie

Systematisch ontwikkelde aanbevelingen voor het periodiek evalueren op nakoming van het opgelegde beleid van huisvesting IV.

Objecttoelichting

Binnen huisvesting IV bevinden zich verschillende bedrijfsmiddelen. Periodiek dient een functionaris met specifieke bevoegdheden controle-activiteiten op de bedrijfsmiddelen te verrichten. Hierdoor kunnen eventuele gebreken tijdig worden vastgesteld en de noodzakelijke maatregelen worden getroffen. Deze activiteiten moeten ondersteund worden met richtlijnen, procedures en instructies, anders bestaat het risico dat de resultaten van de controle-activiteiten niet voldoen aan de verwachte eisen.

Doelstelling	Het effectief beheersen van de bedrijfsmiddelen binnen huisvesting IV.		
Risico	De juiste maatregelen worden niet tijdig getroffen.		
Control	Bedrijfsmiddelen behoren periodiek te worden gecontroleerd op basis van formeel vastgestelde **richtlijnen** en geconstateerde bevindingen dienen tijdig aan het management te worden gerapporteerd.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Richtlijnen	1.	De huisvesting IV-organisatie beschikt over richtlijnen voor de controle van bedrijfsmiddelen.	CIP-netwerk
	2.	De huisvesting IV-organisatie beschikt over geautomatiseerde middelen voor een effectieve ondersteuning van de controle-activiteiten.	CIP-netwerk
	3.	De huisvesting IV-organisatie beschikt over richtlijnen voor het uitvoeren van een registratie, statusmeting, analyse, rapportage en evaluatie.	CIP-netwerk
	4.	De huisvesting IV-organisatie beschikt over richtlijnen voor het evalueren van de huisvesting IV-organisatie.	CIP-netwerk
	5.	De huisvesting IV-organisatie heeft de taken, verantwoordelijkheden en bevoegdheden van controlefunctionarissen vastgelegd.	CIP-netwerk

5.3.2 *C.02 Onderhoudsplan*

Objectdefinitie

Beschrijving van activiteiten voor de instandhouding van huisvesting IV.

Objecttoelichting

De bedrijfsmiddelen voor vastgoed, zoals gebouwen en ruimten van de rekencentra, dienen continu onderhouden te worden. Daarvoor beschikt de huisvesting IV-organisatie over een onderhoudsplan.

Doelstelling	Het zorgen dat huisvesting IV in een goede staat blijft, niet verwaarloosd wordt en niet in verval raakt.	
Risico	Er wordt ingebroken of ongeautoriseerde toegang verkregen, met gevaar van diefstal en beschadiging van eigendommen.	
Control	Voor iedere locatie van huisvesting IV behoort een **onderhoudsplan** te zijn opgesteld met een risicoafweging en **onderhoudsbepalingen**.	CIP-netwerk
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Onderhouds-plan	1.	Voor kwetsbare voorzieningen (binnen en buiten het gebouw) zijn duidelijke onderhoudsbepalingen gesteld.	CIP-netwerk
Onderhouds-bepalingen	2.	Voor alle locaties van de huisvesting IV is een vastgesteld onderhoudsplan aanwezig met relevante onderhoudsbepalingen.	CIP-netwerk

5.3.3 *C.03 Continuïteitsbeheer*

Objectdefinitie

Instandhoudingsproces dat alle activiteiten omvat ter waarborging van de continuïteit van de te leveren huisvesting IV-diensten.

Objecttoelichting

Bedrijfscontinuïteit is het vermogen van de organisatie om na een verstorend incident, de producten of diensten te blijven leveren op acceptabele, vooraf vastgestelde niveaus.
Bedrijfscontinuïteitsmanagement (BCM) is het proces waarmee bedrijfscontinuïteit bereikt wordt. BCM betreft het voorbereiden op de afhandeling van verstorende incidenten, op zodanige wijze dat het vereiste niveau van beschikbaarheid binnen afgesproken grenzen wordt gewaarborgd bij storingen en calamiteiten. BCM omvat continuïteitsplannen, noodvoorzieningen voor uitwijk en herstelprocedures voor herstel van de oorspronkelijke situatie.

Continuïteitsbeheer, ook bekend als een bedrijfscontinuïteitsmanagementsysteem (BCMS), is genormeerd en beschreven in de NEN-EN-ISO 22313: Managementsystemen voor bedrijfscontinuïteit (business continuity management systems).

In de context van huisvesting IV richt BCMS zich onder andere op de beschikbaarheid van data en bedrijfsfuncties vanuit applicaties en de onderliggende infrastructuur op de lange termijn. In het control-domein gaat het om de vraag of voldoende maatregelen genomen zijn voor een spoedig herstel van de IV-services na een calamiteit.

Doelstelling	Het tegengaan van de onderbreking van bedrijfsactiviteiten. Het beschermen van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen. Het zorgen voor een tijdig herstel.		
Risico	Er is onnodig lange uitval van bedrijfsactiviteiten na calamiteiten. Bedrijfsdoelstellingen worden niet gehaald.		
Control	Continuïteitbeheer behoort **procesmatig** voor de gehele organisatie te zijn ingericht, zodat na het plaatsvinden van een calamiteit de hosting services zo snel mogelijk worden **hersteld en voortgezet**.		NCSC 2015: C.10
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procesmatig	1.	Het BCMS is: • beschreven; • goedgekeurd door het management; • toegekend aan een verantwoordelijke functionaris. Het behandelt onder andere: planning, uitvoering van de scope, rapporteren en bespreken van verbetervoorstellen.	NCSC 2015: C.10.01

	2.	De beoordelingsrapportage bevat kwetsbaarheden en verbetervoorstellen die worden gecommuniceerd met verantwoordelijken/eigenaren van systemen waarin kwetsbaarheden en zwakheden gevonden zijn.	CIP-netwerk
Hersteld en voortgezet	3.	Een continuïteitsplan is opgesteld, met daarin activiteiten, rollen en verantwoordelijkheden, uit te voeren validaties, escalatiepaden en een signaleringsrapportage over continuïteit.	CIP-netwerk
	4.	De herstelprocessen en -procedures voor de huisvesting IV-organisatie zijn gedocumenteerd.	NCSC 2015: C10.02
	5.	Er is gezorgd voor afdoende uitwijkfaciliteiten, zodat bij calamiteiten de dienstverlening binnen de daartoe gestelde termijn voortgezet kan worden.	CIP-netwerk
	6.	Het gebruik van de uitwijkfaciliteit(en) en het draaiboek wordt periodiek op correctheid en doelmatigheid getest.	CIP-netwerk
	7.	De huisvesting IV-organisatie is verantwoordelijk voor het beheer, periodiek testen en controleren van uitwijkvoorzieningen.	CIP-netwerk

5.3.4 *C.04 Beheersorganisatie huisvesting IV*

Objectdefinitie

Doelgerichte bundeling van kennis en vaardigheden tussen personen met taken, verantwoordelijkheden en bevoegdheden voor het functionele en technische beheer van huisvesting IV.

Objecttoelichting

De verantwoordelijke stakeholder voor de beheersorganisatie van huisvesting IV behoort een organisatiestructuur vastgesteld te hebben, waarin de verantwoordelijkheden voor de beheersprocessen met toereikende bevoegdheden zijn vastgelegd en op het juiste niveau zijn gepositioneerd.

Doelstelling	Het invullen, coördineren en borgen van de beheersing van de huisvesting IV-dienstverlening.		
Risico	De beheersorganisatie is niet effectief ingericht. De huisvesting IV-dienstverlening verloopt niet optimaal.		
Control	De stakeholder van huisvesting IV behoort een **beheersorganisatie** te hebben ingericht waarin de **processtructuur**, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beheersorga-nisatie	1.	De belangrijkste functionarissen (stakeholders) voor de beheersorganisatie zijn benoemd en de relaties tussen hen zijn met een organisatieschema inzichtelijk gemaakt.	CIP-netwerk
	2.	De verantwoordelijkheden voor de beheersprocessen zijn aan een specifieke functionaris toegewezen en vastgelegd.	ISO 27002:2022: 5.2

	3.	De organisatie heeft de taken en verantwoordelijkheden voor de uitvoering van de beheerwerkzaamheden beschreven en de bijbehorende bevoegdheden vastgelegd in een autorisatiematrix.	CIP-netwerk
Proces-structuur	4.	De samenhang van de processen wordt met een processtructuur vastgelegd.	NCSC 2015: B.06.07