

BIOBaseline
Informatiebeveiliging
Overheidcentrum informatiebeveiliging
en privacybescherming

Rijksoverheid

Vereniging van
Nederlandse Gemeenten

Interprovinciaal Overleg

UNIE VAN
WATERSCHAPPEN

Huisvesting Informatievoorzieningen

BIO Thema-uitwerking

Oktober 2021 [versie 2.1 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-GelijkDelen 4.0 Internationaal (CC BY-SA 4.0) verleend. Voor meer informatie zie: <https://creativecommons.org/licenses/by-sa/4.0/deed.nl>.



| | |
|---------------|---|
| Titel | BIO Thema-uitwerking Huisvesting Informatievoorzieningen |
| Datum | Oktober 2021 |
| Versie | 2.1 definitief |
| Opdrachtgever | Directeur CIP |
| Regime | Becommentarieerde praktijk |
| Auteurs | Wiekram Tewarie (UWV) en Jaap van der Veen (CIP) |
| Reviewers | Versie 1.0: Professionals uit het CIP-netwerk en het CIP-kernteam Versie 2.0: CIP-kernteam Versie 2.1: 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.

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

| | | |
|-------|---|----|
| 1 | Inleiding | 5 |
| 1.1 | Huisvesting IV | 6 |
| 1.2 | Scope en begrenzing huisvesting IV | 7 |
| 1.3 | Aanpak BIO Thema-uitwerking Huisvesting IV | 8 |
| 2 | Huisvesting IV-objecten | 9 |
| 2.1 | Schematische weergave huisvesting IV-objecten | 9 |
| 2.2 | Beleidsdomein | 9 |
| 2.3 | Uitvoeringsdomein | 9 |
| 2.4 | Control-domein | 10 |
| 2.5 | Organisatie huisvesting IV-objecten | 10 |
| 3 | Beleidsdomein | 11 |
| 3.1 | Doelstelling | 11 |
| 3.2 | Risico's | 11 |
| 3.3 | Objecten, controls en maatregelen | 11 |
| 3.3.1 | B.01 Huisvesting IV-beleid | 12 |
| 3.3.2 | B.02 Wet- en regelgeving | 13 |
| 3.3.3 | B.03 Eigenaarschap | 13 |
| 3.3.4 | B.04 Certificering | 14 |
| 3.3.5 | B.05 Contractmanagement | 15 |
| 3.3.6 | B.06 Service Level Management | 16 |
| 3.3.7 | B.07 In- en externe bedreigingen | 16 |
| 3.3.8 | B.08 Training en bewustwording | 17 |
| 3.3.9 | B.09 Organisatiestructuur huisvesting IV | 18 |
| 4 | Uitvoeringsdomein | 19 |
| 4.1 | Doelstelling | 19 |
| 4.2 | Risico's | 19 |
| 4.3 | Objecten, controls en maatregelen | 19 |
| 4.3.1 | U.01 Richtlijn gebieden en ruimten | 20 |
| 4.3.2 | U.02 Bedrijfsmiddelen-inventaris | 21 |
| 4.3.3 | U.03 Fysieke zonering | 22 |
| 4.3.4 | U.04 Beveiligingsfaciliteiten | 23 |
| 4.3.5 | U.05 Nutsvoorziening | 24 |

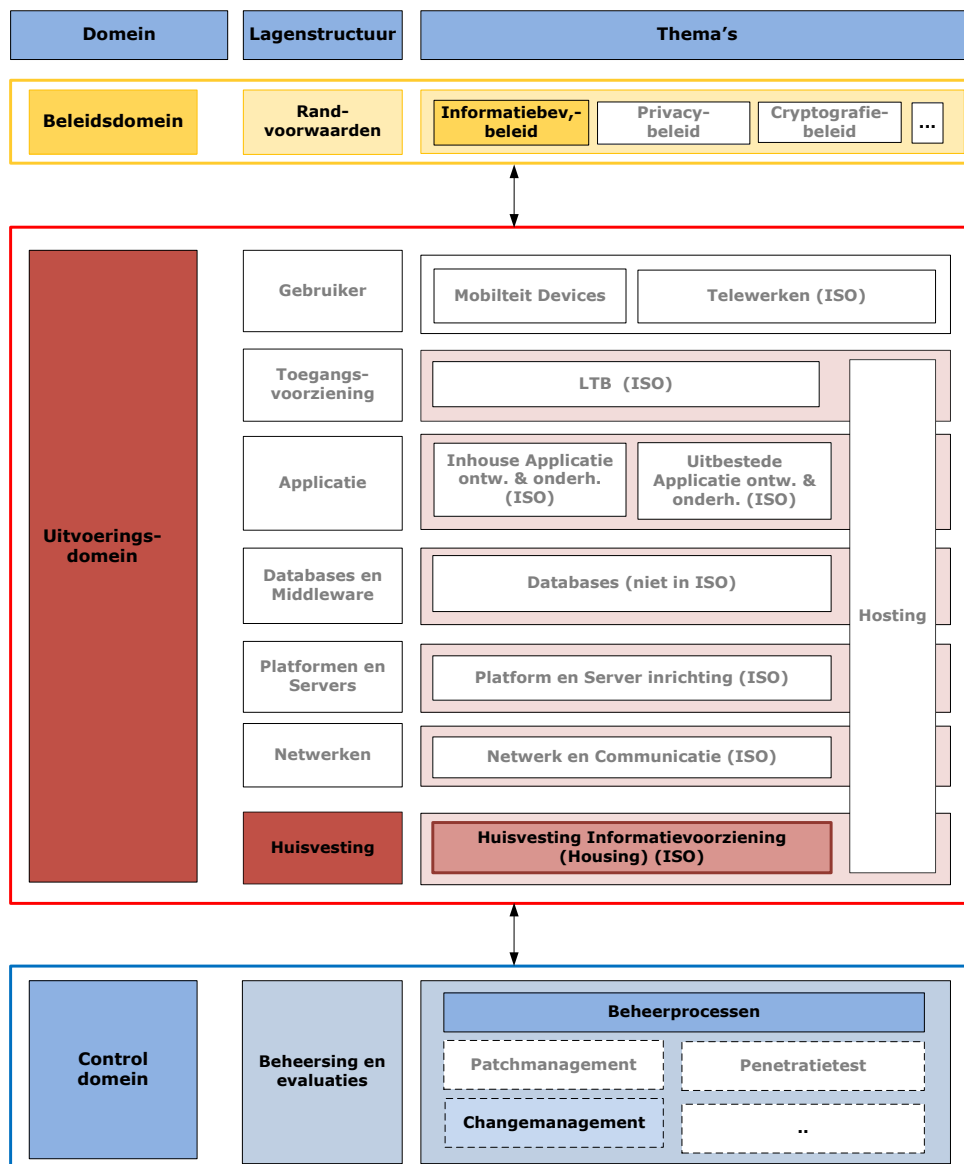


| | | |
|--------|--|----|
| 4.3.6 | U.06 Apparatuur-positionering | 25 |
| 4.3.7 | U.07 Apparatuur-onderhoud | 25 |
| 4.3.8 | U.08 Apparatuur-verwijdering | 26 |
| 4.3.9 | U.09 Bedrijfsmiddelenverwijdering | 27 |
| 4.3.10 | U.10 Laad- en loslocatie | 28 |
| 4.3.11 | U.11 Bekabeling | 29 |
| 4.3.12 | U.12 Huisvesting IV-architectuur | 29 |
| 5 | Control-domein | 31 |
| 5.1 | Doelstelling | 31 |
| 5.2 | Risico's | 31 |
| 5.3 | Objecten, controls en maatregelen | 31 |
| 5.3.1 | C.01 Controle-richtlijn huisvesting IV | 31 |
| 5.3.2 | C.02 Onderhoudsplan | 32 |
| 5.3.3 | C.03 Continuïteitsbeheer | 33 |
| 5.3.4 | C.04 Beheersorganisatie huisvesting IV | 34 |

1 Inleiding

Dit document bevat een referentiekader voor de BIO-Thema-uitwerking Huisvesting Informatievoorzieningen, hierna genoemd Huisvesting IV. Het is gebaseerd op de controls uit de Baseline Informatiebeveiliging Overheid (BIO). Voor die aspecten, waar de BIO onvoldoende praktische invulling geeft, zijn onder andere de volgende best practices geraadpleegd: NEN-EN-ISO/IEC 27002:2017 (hierna genoemd ISO 27002), The Standard of Good Practice (SoGP) 2018 en diverse van de National Institute of Standards and Technology (NIST).

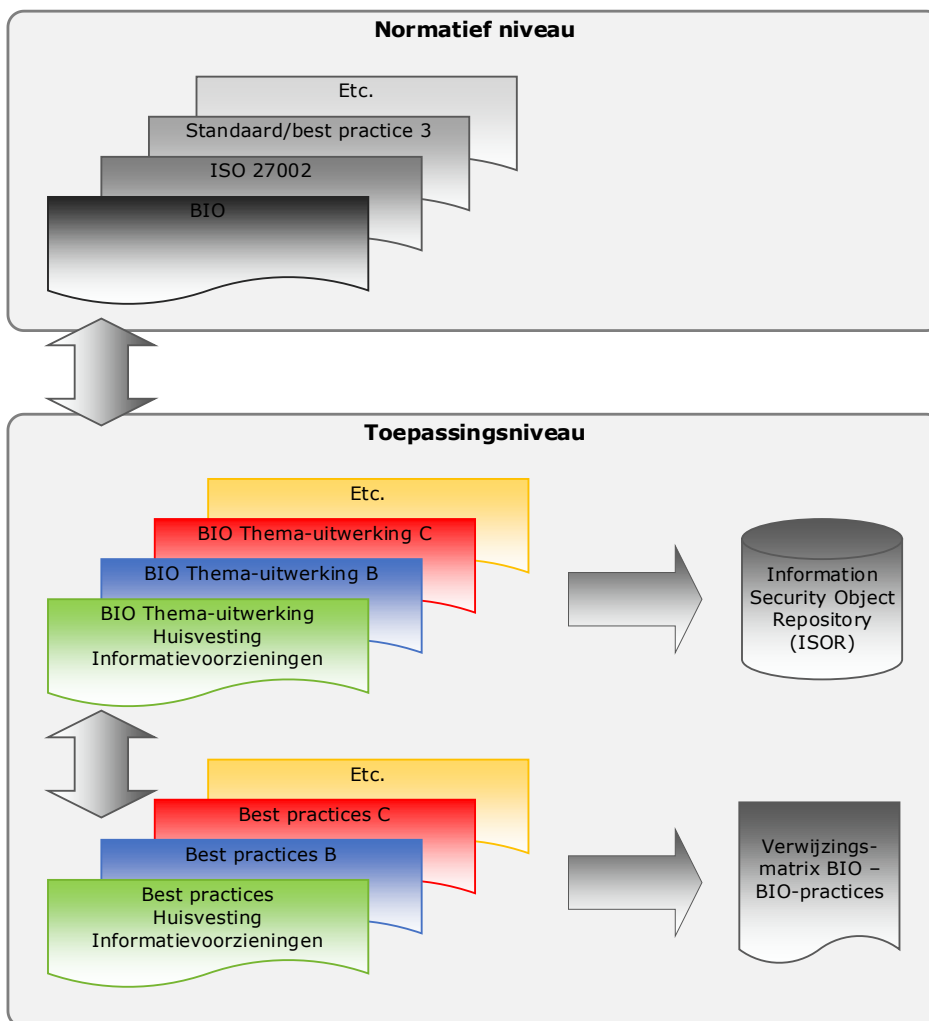
Afbeelding 1 geeft de relatie weer tussen de BIO Thema-uitwerking Huisvesting IV en overige BIO Thema-uitwerkingen.



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

1.1 Huisvesting IV

In dit document zijn een set beveiligingsmaatregelen voor de BIO Thema-uitwerking Huisvesting IV opgenomen. Deze beveiligingsmaatregelen zijn gerelateerd aan relevante onderwerpen (objecten) uit de BIO. Objecten die ontbreken in de BIO en die uit analyses voortvloeien, worden betrokken uit andere best practices, zoals de ISO 27002 en de SoGP. Voor noodzakelijke details bij specifieke maatregelen wordt verwezen naar operationele practices. De relatie tussen deze documenten wordt in afbeelding 2 weergegeven.



Afbeelding 2: Relatie BIO Thema-uitwerking Huisvesting IV met aanpalende documenten

De objecten en de bijbehorende maatregelen gelden zowel voor implementatie- als voor auditdoeleinden. Samenvattend komt het erop neer dat de objecten en de bijbehorende maatregelen georganiseerd zijn in het beleids-, uitvoerings- en control-domein. Afbeelding 3 schetst de structuur waarin een relatie wordt gelegd tussen objecten binnen het beleids-, uitvoerings- en control-domein voor huisvesting IV.



Afbeelding 3: Relatie tussen objecten in het beleids-, uitvoerings- en control-domein

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. De opkomst van de IT-clouddiensten betekent veranderingen in de aanschaf van IT-diensten en de daarvoor benodigde huisvesting.

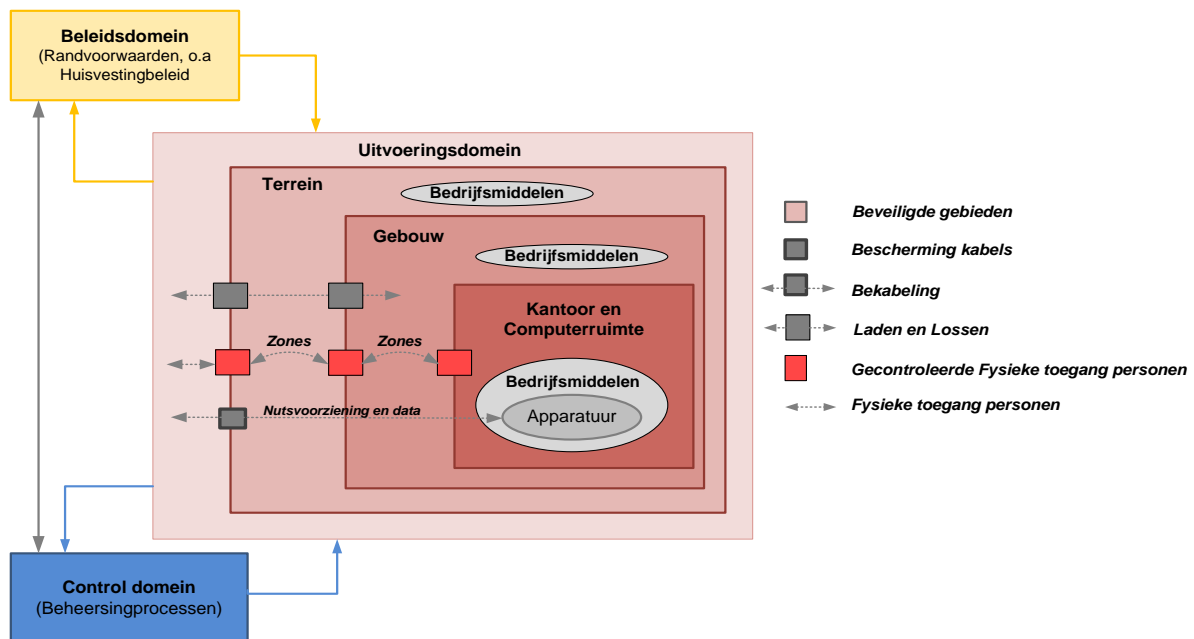
Het management van de doelorganisatie blijft verantwoordelijk voor het gehele bedrijfsproces en onderliggende IT-ondersteuning. Daarom worden er besluiten genomen op basis van: functionaliteit, wet- en regelgeving (beveiliging) en kosten. Dit heeft invloed op de keuze welke type huisvesting IV past bij de organisatie.

De volgende 3 opties zijn mogelijk:

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](#)) wordt 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 4: Overzicht fysieke huisvesting IV

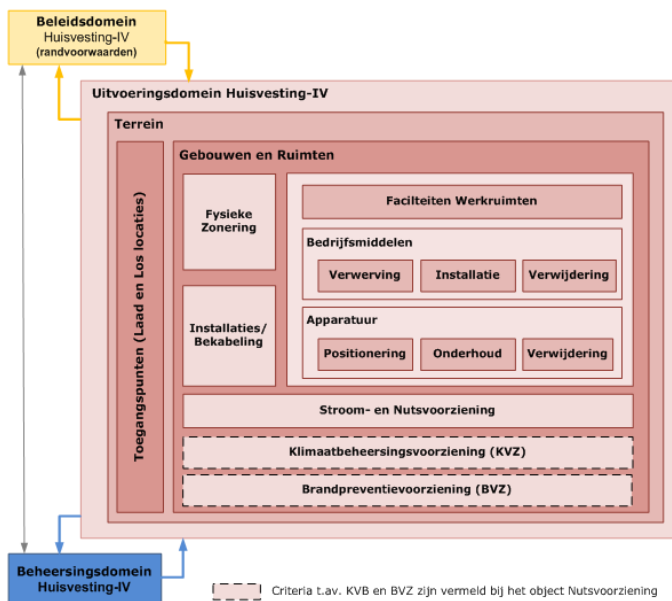
1.3 Aanpak BIO Thema-uitwerking Huisvesting IV

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 hostingdiensten. De essentiële objecten van huisvesting IV worden in afbeelding 5 weergegeven. De elementen worden toegelicht in het beleids-, uitvoerings- en control-domein.



Afbeelding 5: Schematische weergave huisvesting IV-objecten

2.2 Beleidsdomein

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

2.3 Uitvoeringsdomein

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

- **Terrein**
Terrein betreft de locaties van huisvesting IV.
- **Gebouwen, faciliteiten en werkruimten**
Gebouwen, faciliteiten en werkruimten zijn de aan huisvesting IV-georiënteerde objecten. Ze zorgen voor het fysieke bestaan van huisvesting IV. Onder het fysieke bestaan vallen ook de terreinen en de zonering (in ruimten) van gebouwen.
- **Voorzieningen**
Voorzieningen zijn gerelateerd aan de fysiek georiënteerde objecten voor huisvesting IV. Dit is gericht op bedrijfsmiddelen en nutsvoorzieningen (zoals gas, elektra, water maar ook brandblussers etc.). Er zijn 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. Met andere woorden, dit zijn zowel fysieke als elektronisch en informatietechnologie-gerelateerde objecten voor de te leveren huisvesting IV-diensten.

2.4 Control-domein

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

2.5 Organisatie huisvesting IV-objecten

De geïdentificeerde huisvesting IV-objecten zijn met het beleids-, uitvoerings- en control-domein georganiseerd. Hiermee worden deze aspecten in een juiste contextuele samenhang gepositioneerd. De betekenis die aan de lagen wordt toegekend, zijn:

1. Beleidsdomein
Binnen dit domein bevinden zich conditionele elementen over 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 reguleringen en beperkingen.
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 standhouden van de activiteiten in relatie tot huisvesting IV en of deze wel naar wens verlopen.

Objecten worden inclusief omschrijving opgeslagen in de objectenbibliotheek ISOR. ISOR staat voor Information Security Object Repository. Enkele van de objecten zijn uniek voor de BIO. Objecten die aanvullend aan de ISO 27002 voor de beveiliging nodig geacht worden van een bepaald toepassingsgebied zijn met de SIVA-methodiek bepaald. Deze relateren zo mogelijk aan standaarden als de SoGP.

3 Beleidsdomein

3.1 Doelstelling

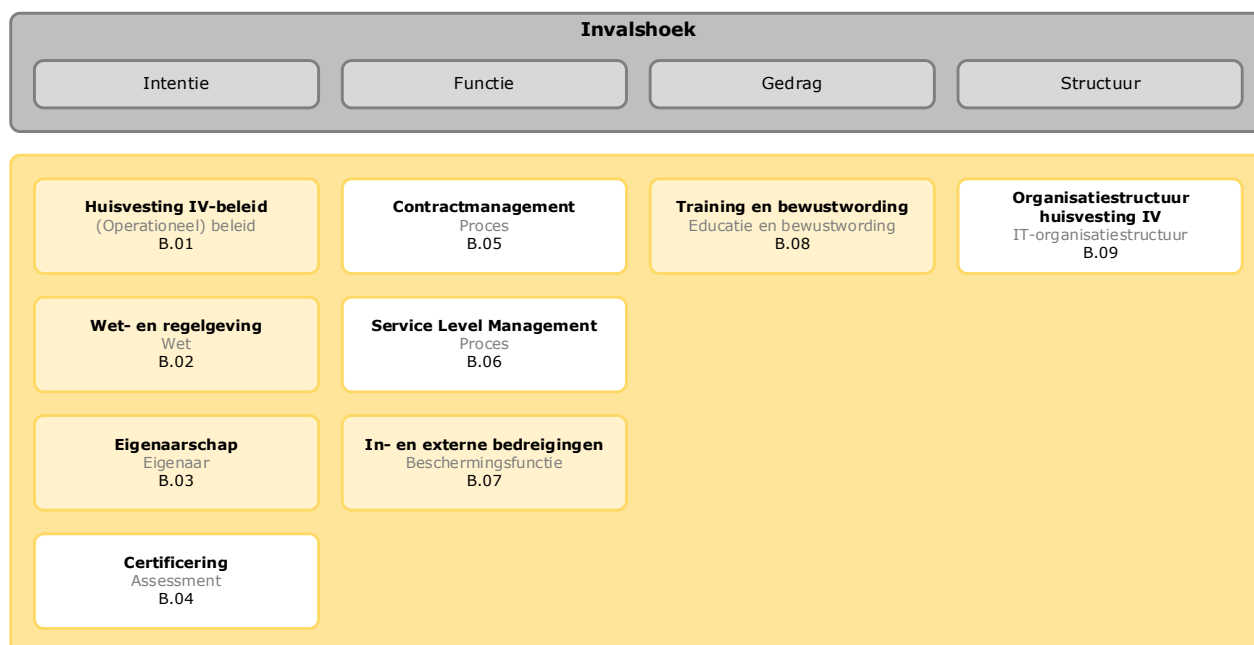
De doelstelling van huisvesting IV in het beleidsdomein is om randvoorwaarden en condities te bieden, zodat huisvesting IV adequaat kan functioneren. Hiermee kan de juiste ondersteuning worden geleverd voor het bereiken van de afgesproken doelstellingen. In dit hoofdstuk worden de objecten en daaraan 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, dan ontstaat het risico dat onvoldoende sturing wordt gegeven aan de veilige inrichting van huisvesting IV, met als gevolg 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 conformiteitindicatoren uitgewerkt. Deze conformiteitindicatoren representeren een vast te stellen set van maatregelen. De objecten die binnen dit domein een rol spelen, zijn in afbeelding 6 vermeld. Van de geel gemarkeerde objecten komen de controls uit de BIO.



Afbeelding 6: Overzicht objecten voor huisvesting IV in het beleidsdomein

3.3.1 B.01 Huisvesting IV-beleid

Objectdefinitie

Betreft het 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 bewerkstelligen dat huisvesting IV de diensten leveren waarmee de organisatie haar doelstellingen kan realiseren. | |
| Risico | Schade door onvoldoende sturingsmogelijkheden voor een effectieve en betrouwbare inrichting van huisvesting IV en het daarmee geleverde niveau van dienstverlening. Aansprakelijkheid voor beveiligingsincidenten, doordat huisvesting IV (verwijtbaar) niet voldoet aan de actuele en gangbare beveiligingspraktijk. | |
| Control | Ten behoeve van het huisvesting IV-beleid behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. | BIO 2019: 5.1.1 |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van |
| Huisvesting IV-beleid | 1. De organisatie heeft een huisvesting IV-beleid opgesteld dat: <ul style="list-style-type: none"> • doelstellingen en principes van de huisvesting IV-beveiliging bevat; • specifieke verantwoordelijkheden en rollen bevat; • processen voor het behandelen van afwijkingen en afzonderingen bevat; • procesmatig tot stand komt, bijvoorbeeld: voorbereiden, ontwikkelen, vaststellen/goedkeuren, communiceren, implementeren, evalueren en aanpassen. | ISO 27002 2017: 5.1.1 |
| Beleidsregels | 2. Beleidsregels over het huisvesting IV-beleid behandelen eisen die voortkomen uit: <ul style="list-style-type: none"> • Bedrijfsstrategie • Wet- en regelgeving • Huidige en verwachte bedreigingen op huisvesting IV | ISO 27002 2017: 5.1.1 |

| | | | |
|--|----|---|-----------------------|
| | 3. | Beleidsregels zijn gerelateerd aan specifieke onderwerpen over huisvesting IV, zoals: <ul style="list-style-type: none"> • Fysieke beveiligingszone • Fysieke toegangsbeveiligingspersoneel | ISO 27002 2017: 5.1.1 |
|--|----|---|-----------------------|

3.3.2 B.02 Wet- en regelgeving

Objectdefinitie

Omvat de geldende nationale en internationale wetten en regelgeving die van toepassing is op huisvesting IV.

Objecttoelichting

Er zijn verschillende wettelijke kaders waar de huisvestingsorganisatie aan 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 enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen en enige beveiligingseisen. | |
| Risico | Schade door wettelijke aansprakelijkheid. | |
| 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. | |
| | | BIO 2019: 18.1.1 |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van |
| Wettelijke statutaire, regelgevende, contractuele eisen | 1. | De verantwoordelijke voor de huisvesting IV-organisatie stelt vast welke wetgeving van toepassing is voor huisvesting IV. |
| | 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. |
| | | ISO 27002 2017: 18.1.1 |
| | | CIP-netwerk |

3.3.3 B.03 Eigenaarschap

Objectdefinitie

Betreft het toewijzen 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. Om te borgen dat de juiste acties voor de bedrijfsmiddelen worden ondernomen, moet de organisatie de bedrijfsmiddelen toewijzen aan eigenaren en daarbij de taken en verantwoordelijkheden vastleggen.

| | | | |
|--|---|---|------------------------------|
| Doelstelling | Het bewerkstelligen dat er een verantwoordelijke is voor alle informatie en bedrijfsmiddelen om deze actueel te houden dan wel ervoor te zorgen dat noodzakelijke acties worden ondernomen. | | |
| Risico | Schade door achterstallig onderhoud en niet functioneren van bedrijfsmiddelen. | | |
| Control | Huisvesting IV-bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben. | BIO 2019: 8.1.2 | |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van | |
| Eigenaar | 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 2017: 8.1.2 |
| | 2. | Het eigenaarschap van een huisvesting IV-bedrijfsmiddel wordt toegekend bij het ontstaan en of bij de verwerving van het middel. | ISO 27002 2017: 8.1.2 |
| | 3. | De eigenaar van het huisvesting IV-bedrijfsmiddel is verantwoordelijk voor het juiste beheer gedurende de gehele levenscyclus ervan. | ISO 27002 2017: 8.1.2 |
| | 4. | De eigenaar van het bedrijfsmiddel zorgt ervoor dat: <ul style="list-style-type: none"> • bedrijfsmiddelen geïnventariseerd worden; • bedrijfsmiddelen passend worden geclassificeerd; • toegangsbeperkingen en classificatie van belangrijke bedrijfsmiddelen worden gedefinieerd en periodiek beoordeeld; • bedrijfsmiddelen met juiste procedures worden verwijderd of vernietigd. | ISO 27002 2017: 8.1.2a t/m d |

3.3.4 B.04 Certificering

Objectdefinitie

Betreft een 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 willen 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 bewerkstelligen dat de rekencentra aan het door de opdrachtgever beoogde beveiligingsniveau voldoet. | |
| Risico | Continuïteits- of datalekschade door een gebrekkig volwassenheidsniveau van huisvesting IV. | |
| 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 software en systemen. | BIO 2019: 14.2.1.1 |
| | 2. | Huisvesting IV die ingezet wordt voor de organisatie is minimaal ISO 27001 (Managementsystemen voor informatiebeveiliging) en ISO 50001 (Energiebeheer) gecertificeerd. | CIP-netwerk |

3.3.5 B.05 Contractmanagement

Objectdefinitie

Betreft de besturing en het beheer van de overeenkomsten tussen de klant en leverancier.

Objecttoelichting

Wanneer de ontwikkeling en/of het beheer over de gehele of een deel van huisvesting IV wordt uitbesteed, moeten de functionele en beveiligingseisen in een overeenkomst tussen beide partijen worden vastgelegd, zoals in een contract en/of Service Level Agreement (SLA). Deze overeenkomst moet garanderen dat er geen misverstanden bestaan tussen de beide partijen.

| Doelstelling | Het zorgen dat huisvesting IV voldoet aan vooraf ontworpen eigenschappen, waaronder het beveiligingsniveau. | | |
|---|--|---|------------------------------------|
| Risico | Schade door gebrek aan toetsmiddelen voor de huisvesting IV-organisatie om vast te stellen of de voorzieningen juist zijn en of deze aan het juiste beveiligingsniveau voldoen. | | |
| Control | Huisvesting IV die worden verworven, behoren 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 |
| | 2. | Het verwerven van huisvesting IV vindt uitsluitend plaats met een overeenkomst of andere formele afspraak. | CIP-netwerk |
| Overeenkomsten | 3. | De bij Service Level Agreements (SLA'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 SLA'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

Betreft de besturing en het beheer van 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 van de huisvesting IV-diensten door de leverancier. De overeenkomst tussen de leverancier en de klant over deze afspraken wordt geformaliseerd met een Service Level Managementproces.

| | | | |
|--|---|--|-------------------------------|
| Doelstelling | Het bewerkstelligen dat de huisvesting IV-services conform afspraken geleverd worden (leveren wat je hebt beloofd). | | |
| Risico | Onjuiste of verkeerde levering van services leidt tot klantontevredenheid. | | |
| Control | Het management van huisvesting IV behoort diensten te leveren conform een dienstenniveau-overeenkomst (Service Level Agreement). | | CIP-netwerk |
| Conformiteitsindicator, nummer en maatregel | | | Afgeleid/afkomstig van |
| Service Level Agreement | 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

Omvat besluitvorming over weerbaarheid tegen potentiële, fysieke schadelijke invloeden van binnenuit of buitenaf.

Objecttoelichting

Naast beveiligingsvoorzieningen, ter voorkoming van interne bedreigingen, moet de organisatie ook voorzieningen treffen die huisvesting IV beschermen tegen externe bedreigingen, zoals calamiteiten die veroorzaakt worden door de natuur of door menselijk handelen.

Natuurlijke calamiteiten kunnen onder andere zijn storm, overstromingen, brand veroorzaakt door bliksem en/of schade aan gebouwen door een aardbeving. Calamiteiten kunnen ook worden veroorzaakt door foute handelingen van medewerkers, zoals het niet onderbrengen van kopieën van kritische data op verschillende locaties of kunnen ontstaan door ontwerpfouten of het nalaten van het treffen van beveiligingsmaatregelen.

| | | | |
|---|---|---|-------------------------------|
| Doelstelling | Het bewerkstelligen van de weerbaarheid van huisvesting IV en het voorkomen van verstoringen in huisvesting IV. | | |
| Risico | Niet-beschikbaar zijn van informatiesystemen en data, waardoor de aangesloten organisaties schade ondervinden in hun bedrijfsvoeringen. | | |
| Control | Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast. | | BIO 2019: 11.1.4 |
| Conformiteitsindicator, nummer en maatregel | | | Afgeleid/afkomstig van |
| Natuurrampen , kwaadwillige aanvallen of ongelukken | 1. | De organisatie heeft geïnventariseerd welke data en apparatuur bedrijfskritisch zijn. | BIO 2019: 11.1.4.1 |
| | 2. | Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging. | BIO 2019: 11.1.4.1 |
| | 3. | Bij huisvesting van bedrijfsmiddelen wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen. | BIO 2019: 11.1.4.2 |
| | 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

Betreft een 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 bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers: <ul style="list-style-type: none"> • zich bewust zijn van bedreigingen en gevaren van huisvesting IV; • continu op de hoogte zijn van het vigerende huisvesting IV-beleid; • continu bewust blijven van relevante maatregelen. | |
| Risico | Schade door onbewust en/of onbekwaam fout handelen van medewerkers. | |
| 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. | BIO 2019: 7.2.2 |

| Conformiteitsindicator, nummer en maatregel | | | Afgeleid/afkomstig van |
|--|----|---|--|
| Bewustzijns- opleiding en - training en bijscholing | 1. | Binnen huisvesting IV nemen alle medewerkers regelmatig deel aan beveiligingsbewustwording (bijvoorbeeld I-bewustzijn) en trainingsprogramma's of nemen deel 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

Betreft de 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 | Schade doordat de huisvesting IV-organisatie niet effectieve tot uitvoering komt. | | |
| 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

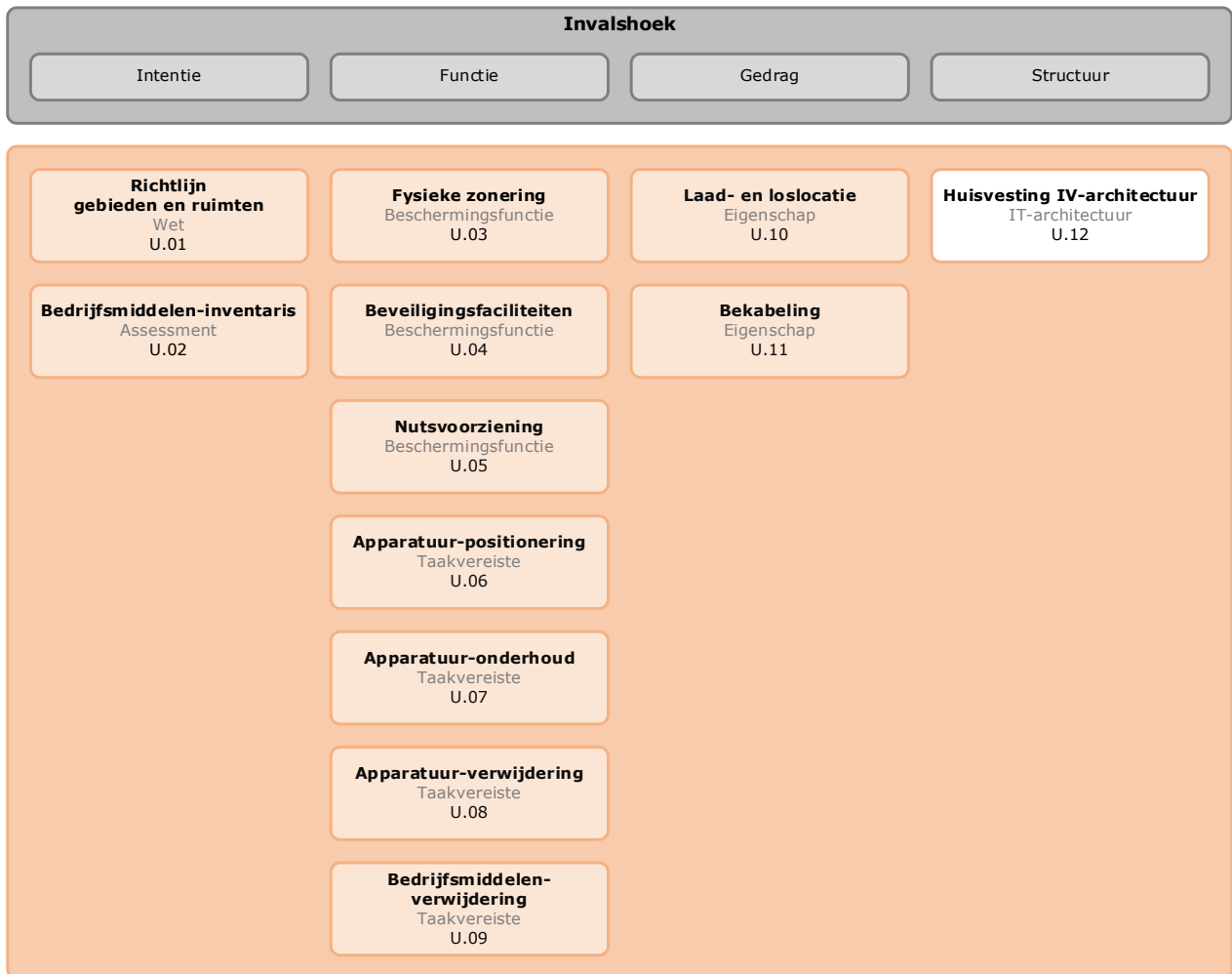
Het doel van het uitvoeringsdomein voor Huisvesting IV is het waarborgen dat de fysieke toegang tot functionaliteit is ingericht overeenkomstig specifieke beleidsuitgangspunten van de bedrijfsonderdelen en dat de beveiliging van de huisvesting als geheel in bestaan en werking voldoet aan de eisen die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

4.2 Risico's

Als naleving van de specifieke normen, omgezet in eisen voor de inrichting en exploitatie van de rekencentra niet wordt gerealiseerd, dan 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. Per object zijn de conformiteitsindicatoren en de desbetreffende implementatie-elementen uitgewerkt. De onderwerpen die uit de BIO binnen dit domein een rol spelen zijn huisvesting IV, inrichting en dienstverlening. Afbeelding 7 toont het resultaat van de SIVA-methodiek voor relevante objecten voor huisvesting IV. De wit ingekleurde objecten ontbreken als control in de BIO maar zijn van belang voor deze thema-uitwerking. Om deze reden zijn aanvullende objecten uit andere baselines opgenomen.



Afbeelding 7: Overzicht objecten voor huisvesting IV in het uitvoeringsdomein

4.3.1 U.01 Richtlijn gebieden en ruimten

Objectdefinitie

Betreft 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. Hiervoor moeten richtlijnen worden vervaardigd en toegepast en ook moeten voorzieningen worden getroffen, zie verder het onderwerp 'Voorzieningen'.

| | |
|--------------|--|
| Doelstelling | Het bewerkstelligen van de juiste coördinatie van activiteiten binnen de beveiligde ruimten. |
|--------------|--|

| | | | |
|--|---|---|-------------------------------|
| Risico | Ongewenste wijzigingen aanbrengen aan het functioneren van bedrijfsmiddelen door onbevoegde personen, waardoor de bedrijfsvoering verstoord wordt en schade ontstaat. | | |
| Control | Voor het werken in beveiligde gebieden behoren richtlijnen te worden ontwikkeld en toegepast. ¹ | | BIO 2019: 11.1.5 |
| Conformiteitsindicator, nummer en maatregel | | | Afgeleid/afkomstig van |
| Richtlijnen | 1. | Personeel behoort alleen dankzij 'need-to-know' bekend te zijn met het bestaan van of de activiteiten binnen een beveiligd gebied. | ISO 27002 2017: 11.1.5a |
| | 2. | Zonder toezicht wordt niet gewerkt in beveiligde gebieden. Dit is zowel om veiligheidsredenen als om geen gelegenheid te bieden voor kwaadaardige activiteiten. | ISO 27002 2017: 11.1.5b |
| | 3. | Leegstaande beveiligde ruimten behoren fysiek afgesloten en periodiek geïnspecteerd te zijn. | ISO 27002 2017: 11.1.5c |
| | 4. | Tenzij goedgekeurd wordt beeld- en geluidsopnameapparatuur, zoals in mobiele apparatuur niet toegelaten in de beveiligde ruimten. | ISO 27002 2017: 11.1.5d |
| | 5. | Bezoekers van kritieke faciliteiten: <ul style="list-style-type: none"> • 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-inventaris²

Objectdefinitie

Betreft de 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/of informatie over deze voorzieningen te inventariseren en te registreren zodat de juiste informatie beschikbaar is, wanneer gebeurtenissen daarom vragen.

| | |
|--------------|---|
| Doelstelling | Het bewerkstelligen dat een adequate informatie beschikbaar is wanneer het noodzakelijk is. |
|--------------|---|

¹ Omdat de criteria over richtlijn gaan, is het woord 'procedures' in de BIO vervangen door 'richtlijnen'.

² De control uit de BIO is ten opzichte van de ISO 27001 veranderd.

| | | | |
|--|--|--|-----------------------|
| Risico | 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. | | |
| BIO 2019: 8.1.1 | | | |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van | |
| Inventaris | 1. | Voor elk van de geïdentificeerde bedrijfsmiddelen is het eigenaarschap toegekend (zie paragraaf 8.1.2 van de ISO 27002) en de classificatie van het bedrijfsmiddel is geïdentificeerd (zie paragraaf 8.2 van de ISO 27002). | ISO 27002 2017: 8.1.1 |
| | 2. | De huisvesting IV-organisatie identificeert de bedrijfsmiddelen, die voor huisvesting IV relevant zijn in de levenscyclus van informatie en documenteert het belang daarvan, waarbij: <ul style="list-style-type: none"> de levenscyclus van informatie (aanmaak, verwerking, opslag, overdracht, verwijdering en vernietiging) omvat; de documentatie onderhouden wordt in speciale of bestaande inventarislijsten indien van toepassing. | ISO 27002 2017: 8.1.1 |
| | 3. | De inventarislijst van de bedrijfsmiddelen is nauwkeurig, actueel, consistent en conform andere inventarisoverzichten. | ISO 27002 2017: 8.1.1 |
| | 4. | De huisvesting IV-organisatie heeft inventarisoverzichten, waarvoor geldt: <ul style="list-style-type: none"> inventarisoverzichten van bedrijfsmiddelen helpen zeker te stellen dat doeltreffende bescherming plaatsvindt; inventarisoverzichten kunnen vereist zijn voor: financieel (beheer van bedrijfsmiddelen), verzekeringen, gezondheid en veiligheidsredenen e.d. | ISO 27002 2017: 8.1.1 |

4.3.3 U.03 Fysieke zonerings

Objectdefinitie

Betreft de fysieke scheiding en gecontroleerde doorgang tussen terreinen, gebouwen en ruimten.

Objecttoelichting

Bij het indelen in beveiligde zones (zonerings) gaat het enerzijds om het scheiden van verantwoordelijkheidsgebieden en anderzijds het mogelijk maken van gecontroleerde doorgang tussen de gedefinieerde gebieden. Voor huisvesting IV gaat het om fysieke 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 | Niet kunnen voorkomen dat bedreigingen in het ene verantwoordelijkheidsgebied schade veroorzaken in een ander verantwoordelijkheidsgebied. |

| | | | |
|--|---|---|-------------------------------|
| Control | Fysieke beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten. | | BIO 2019: 11.1.1 |
| Conformiteitsindicator, nummer en maatregel | | | Afgeleid/afkomstig van |
| Beveiligingszones | 1. | Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van de volgende standaarden : <ul style="list-style-type: none"> • Kader Rijkstoegangsbeleid 2010 • Normenkader Beveiliging Rijkskantoren (NkBR) 2016 • Beveiligingsvoorschrift Rijksdienst (BVR) 2013 | BIO 2019: 11.1.1.1 |
| | 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 2017: 11.1.1a |
| | 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 2017: 11.1.1g |
| | 4. | Alle medewerkers dragen zichtbaar een identificatiemiddel en informeren beveiligingspersoneel als zij in de niet publieke ruimten personen zonder begeleiding en zonder zichtbaar identificatiemiddel tegenkomen. | ISO 27002 2017: 11.1.2d |
| | 5. | Elke fysieke toegang wordt gecontroleerd en fysiek of elektronisch in een logboek vastgelegd. | ISO 27002 2017: 11.1.2c |

4.3.4 U.04 Beveiligingsfaciliteiten

Objectdefinitie

Betreft de 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 | Toegang verschaffen tot ruimten en schade aanrichten aan de eigendommen van de organisatie door niet-geautoriseerden. | |
| Control | Voor het beveiligen van ruimten behoren faciliteiten te worden ontworpen en toegepast ³ . | BIO 2019: 11.1.3 |

³ Voor de uitwerking van de BIO Thema-uitwerking huisvesting IV is de control geherformuleerd.

| Conformiteitsindicator, nummer en maatregel | | | Afgeleid/afkomstig van |
|---|----|--|-------------------------|
| Faciliteiten | 1. | Belangrijke faciliteiten zijn zo gelegen dat ze niet voor iedereen toegankelijk zijn. | ISO 27002 2017: 11.1.3 |
| | 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 2017: 11.1.3c |
| | 3. | Adresboeken en interne telefoonboeken waarin locaties worden aangeduid met faciliteiten die vertrouwelijke informatie verwerken, zijn niet vrij toegankelijk voor onbevoegden. | ISO 27002 2017: 11.1.3d |
| | 4. | Sleutelbeheer is ingericht op basis van een sleutelplan (zie ook het Normenkader Beveiliging Rijkskantoren (NKBR) 2016 paragraaf 5.4). | BIO 2019: 11.1.3.1 |

4.3.5 U.05 Nutsvoorziening

Objectdefinitie

Betreft een product die door een nutsbedrijf geleverd worden.

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 | Niet beschikbaar zijn van de gehuisveste informatievoorzieningen. | | |
| Control | Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen. | BIO 2019: 11.2.2 | |
| Conformiteitsindicator, nummer en maatregel | | | Afgeleid/afkomstig van |
| Nutsvoorzieningen | 1. | Nutsvoorzieningen: <ul style="list-style-type: none"> • zijn conform de technische beschrijving van de fabrikant en de lokale wettelijke eisen; • worden regelmatig onderzocht, om te beoordelen of hun capaciteit toereikend is voor de groei van het bedrijf en de interactie met andere nutsvoorzieningen; • worden regelmatig geïnspecteerd en getest, om te waarborgen dat ze correct functioneren; • zijn zo nodig voorzien van een alarmsysteem, om disfunctioneren op te sporen; • beschikken voor zover nodig over meervoudige voeding met een verschillende fysieke route. | ISO 27002 2017: 11.2.2a t/m e |

| | | | |
|--|----|---|------------------------|
| | 2. | Noodverlichting en (nood)communicatiemiddelen zijn aanwezig. | ISO 27002 2017: 11.2.2 |
| | 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 2017: 11.2.2 |
| | 4. | Voor de netwerkverbinding(en) is redundantie verkregen via meerdere routes en vanaf meer dan één aanbieder. | ISO 27002 2017: 11.2.2 |

4.3.6 U.06 Apparatuur-positionering

Objectdefinitie

Betreft het veilig plaatsen 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 en onderbreking van bedrijfsmiddelen wordt voorkomen.

| | | | |
|--|---|---|-------------------------------|
| Doelstelling | Het voorkomen van verlies, schade, diefstal en/of compromitering van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten. | | |
| Risico | Verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten. | | |
| Control | Apparatuur behoort zo te worden geplaatst en beschermd , dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind. | | BIO 2019: 11.2.1 |
| 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 2017: 11.2.1 |
| | 2. | Apparatuur wordt beschermd tegen bedreiging (zoals overspanningen, blikseminslag, diefstal, weglekken van informatie door elektromagnetische straling) van buitenaf. | ISO 27002 2017: 11.2.1 |

4.3.7 U.07 Apparatuur-onderhoud

Objectdefinitie

Betreft de 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 waarborging dat apparatuur continue beschikbaar en integer is. |
|--------------|--|

| | | | |
|--|---|---|-------------------------|
| Risico | Schade door ongeautoriseerde toegang en onvoldoende beschikbaarheid van falende apparatuur. | | |
| Control | Apparatuur behoort op een correcte wijze te worden onderhouden. | | |
| BIO 2019: 11.2.4 | | | |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van | |
| Correcte wijze | 1. | Apparatuur wordt onderhouden volgens de door de leverancier aanbevolen intervallen voor servicebeurten en voorschriften. | ISO 27002 2017: 11.2.4a |
| | 2. | Reparaties en onderhoudsbeurten aan apparatuur worden alleen uitgevoerd door bevoegd onderhoudspersoneel. | ISO 27002 2017: 11.2.4b |
| | 3. | Reparaties van en onderhoud aan apparatuur (hardware) worden op locatie en door bevoegd personeel uitgevoerd, tenzij geen data (meer) op het apparaat aanwezig of toegankelijk is. | ISO 27002 2017: 11.2.4d |
| | 4. | Van alle vermeende en daadwerkelijke fouten en van al het preventieve en correctieve onderhoud worden registraties bijgehouden. | ISO 27002 2017: 11.2.4c |
| | 5. | Voldaan wordt aan alle onderhoudseisen die door verzekeringspolissen zijn opgelegd. | ISO 27002 2017: 11.2.4e |
| | 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 niet slecht functioneert. | ISO 27002 2017: 11.2.4f |

4.3.8 U.08 Apparatuur-verwijdering

Objectdefinitie

Betreft het 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 waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik van apparatuur zijn verwijderd of betrouwbaar veilig zijn overschreven. | | |
| Risico | In ongeautoriseerde handen komen van gevoelige gegevens en software. | | |
| Control | Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven . | BIO 2019: 11.2.7 | |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van | |
| Geverifieerd | 1. | Voorgaand aan verwijdering of hergebruik, behoort te worden gecontroleerd of apparatuur opslagmedia bevat. | ISO 27002 2017: 11.2.7 |

| | | |
|--|---|---|
| Verwijdering of betrouwbaar veilig zijn overschreven | <p>2. Het verwijderen van apparatuur vindt plaats met vastgestelde procedurestappen:</p> <ul style="list-style-type: none"> • Inleveren Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. • Verwijderen De beheerorganisatie zorgt voor een verantwoorde verwijdering van data, zodat geen data meer op het apparaat aanwezig of toegankelijk is. • Vernietigen Als verwijdering niet mogelijk is, wordt de data vernietigd. • Afvoeren De beheerorganisatie zorgt voor een verantwoorde afvoer. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd. | <p>ISO 27002 2017: 8.3.1b ISO 27002 2017: 8.3.2a en e ISO 27002 2017: 9.4.4</p> |
|--|---|---|

4.3.9 U.09 Bedrijfsmiddelenverwijdering

Objectdefinitie

Betreft het veilig en gecontroleerd verwijderen en afvoeren van bedrijfsmiddelen.

Objecttoelichting

Bedrijfsmiddelen zijn alle objecten waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en objecten, waarmee toegang tot gebouwen, ruimten en IT-voorzieningen kan worden verkregen. Verwijdering en afvoer van deze middelen dient nauwkeurig met vastgestelde procedures te worden uitgevoerd.

| | | | |
|--|---|--|-------------------------|
| Doelstelling | Het bewerkstelligen van een gecontroleerde verwijdering en afvoer van bedrijfsmiddelen. | | |
| Risico | Misbruik van bedrijfsmiddelen in de hand werken door het ontbreken van procedures voor de behandeling van bedrijfsmiddelen. | | |
| Control | Informatieverwerkende bedrijfsmiddelen , uitgezonderd daarvoor bestemde mobiele apparatuur, behoren niet van de locatie te worden verwijderd zonder voorafgaande goedkeuring. | BIO 2019: 11.2.5 | |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van | |
| Bedrijfsmiddelen | 1. | In het beveiligingsbeleid is geborgd dat het invoeren en afvoeren van bedrijfsmiddelen met een vaste procedure plaatsvindt. Onderdeel van deze procedure is een formeel toestemmingstraject. | CIP-netwerk |
| | 2. | Medewerkers en gebruikers van externe partijen, die bevoegd zijn om toe te staan dat bedrijfsmiddelen van de locatie worden meegenomen, worden geïdentificeerd. | ISO 27002 2017: 11.2.5a |
| | 3. | Aan de afwezigheid van bedrijfsmiddelen worden tijdsgrenzen gesteld en geverifieerd wordt dat ze tijdig worden teruggebracht. | ISO 27002 2017: 11.2.5b |
| | 4. | Voor zover nodig en gepast wordt het meenemen en de terugkeer van bedrijfsmiddelen geregistreerd. | ISO 27002 2017: 11.2.5c |

| | | | |
|--|----|---|-------------------------|
| | 5. | De identiteit, rol en connectie van iedereen die bedrijfsmiddelen hanteert of gebruikt, worden gedocumenteerd en deze documenten moeten samen met de apparatuur, informatie of software worden geretourneerd. | ISO 27002 2017: 11.2.5d |
|--|----|---|-------------------------|

4.3.10 U.10 Laad- en loslocatie

Objectdefinitie

Betreft een of meer specifieke toegangspunten voor het laden en lossen van goederen op terreinen en in gebouwen.

Objecttoelichting

De rekencentra kennen 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 huisvesting IV, zoals terreinen en gebouwen. | | |
| Risico | Toegang verschaffen tot beveiligingsruimten of zones van huisvesting IV door onbevoegden. | | |
| 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. | | BIO 2019: 11.1.6 |
| 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 2017: 11.1.6a |
| | 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 2017: 11.1.6b |
| | 4. | De buitendeuren van een laad- en loslocatie moeten beveiligd zijn als de binnendeuren open zijn. | ISO 27002 2017: 11.1.6c |
| | 5. | Inkomende materialen worden bij binnenkomst op de locatie geregistreerd volgens de procedures voor bedrijfsmiddelenbeheer. | ISO 27002 2017: 11.1.6e |
| | 6. | Inkomende en uitgaande zendingen worden, voor zover mogelijk, fysiek gescheiden. | ISO 27002 2017: 11.1.6f |
| | 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 2017: 11.1.6g |

4.3.11 U.11 Bekabeling

Objectdefinitie

Betreft middelen voor transport van energie en signalen.

Objecttoelichting

Binnen huisvesting IV is alle apparatuur verbonden met een bekabelingssysteem die in speciale kabelruimten is geïnstalleerd. Deze bekabelingsruimten kunnen doelwit worden van misbruik door bijvoorbeeld speciale af luisterapparatuur aan te sluiten. Het is daarom noodzakelijk om deze bekabelingsruimten te voorzien van specifieke beveiligingsmaatregelen.

| | | | |
|--|---|---|-------------------------------|
| Doelstelling | Het bewerkstelligen dat de bekabeling aan het aspect robuustheid voldoet. | | |
| Risico | Misbruik van het bekabelingssysteem. | | |
| Control | Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade. | | BIO 2019: 11.2.3 |
| Conformiteitsindicator, nummer en maatregel | | | Afgeleid/afkomstig van |
| Voedings- kabels | 1. | Kabels worden bij voorkeur ondergronds aangelegd. | ISO 27002 2017: 11.2.3a |
| | 2. | Huisvesting IV is ingericht met de volgende best practices: <ul style="list-style-type: none"> • 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 door onbevoegden. | ISO 27002 2017: 11.2.3 |

4.3.12 U.12 Huisvesting IV-architectuur

Objectdefinitie

Betreft een 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. Architectuur geeft ook 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 ontwerpbeslissingen (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 en inzicht geeft in de inrichting van de fysieke voorzieningen. | | |
| Risico | Gebrek aan inzicht in de positie en samenhang van beveiligingsmaatregelen maakt de kans groot dat bedreigingen over het hoofd worden gezien en schade ontstaat door ongeautoriseerde toegang en misbruik van bedrijfsmiddelen en gegevens. | | |
| 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 |
| Architectuurvoorschriften | 1. | De aanwezige architectuurvoorschriften voor de fysieke inrichting van huisvesting IV worden actief onderhouden. | CIP-netwerk |
| | 2. | De inrichting van huisvesting IV en bekabelingen zijn gedocumenteerd. | CIP-netwerk |
| Documentatie | 3. | Het document met de inrichting van huisvesting IV en de bekabeling: <ul style="list-style-type: none"> • 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

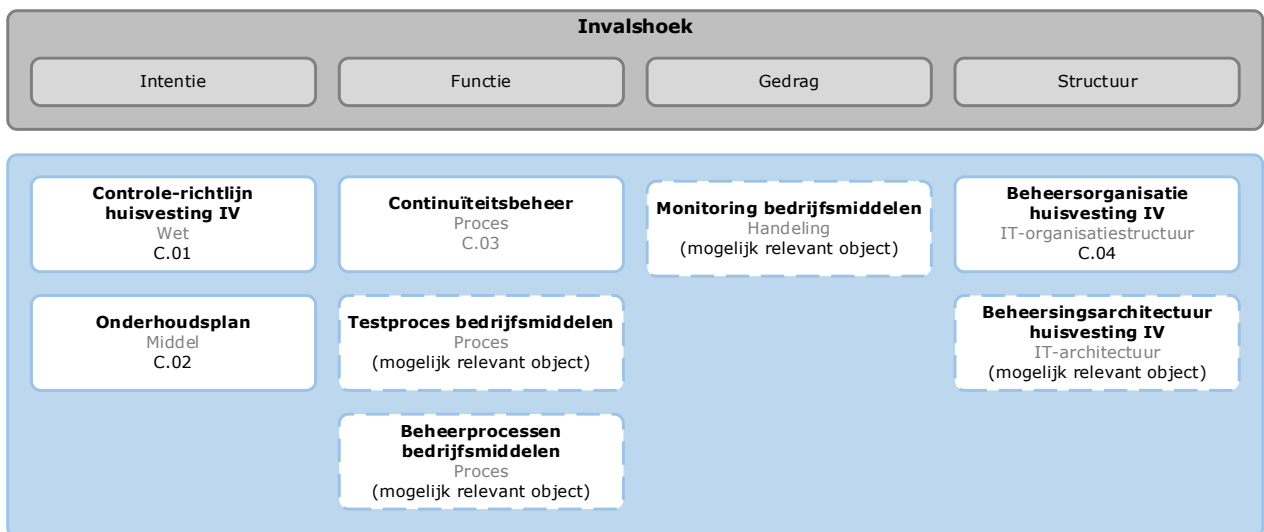
De doelstelling van het control-domein is ervoor te zorgen dat en/of vast te stellen of huisvesting IV afdoende is ingericht voor het leveren van het gewenste niveau van beveiliging. Dit houdt onder meer in dat binnen de organisatie een adequate beheerorganisatie moet zijn ingericht, waarin beheerprocessen zijn vormgegeven.

5.2 Risico's

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

5.3 Objecten, controls en maatregelen

Afbeelding 8 toont de objecten die voor huisvesting IV een rol spelen. De objecten die gestreept omlind zijn, worden mogelijk in de volgende versie uitgewerkt.



Afbeelding 8: Overzicht objecten voor huisvesting IV in het control-domein

5.3.1 C.01 Controle-richtlijn huisvesting IV

Objectdefinitie

Betreft systematisch ontwikkelde aanbevelingen voor het periodiek evalueren van het opgelegde beleid van huisvesting IV op de actualiteitswaarde.

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. De beheerorganisatiestructuur geeft de samenhang van de ingerichte processen weer.

| | | | |
|--|--|---|-------------|
| Doelstelling | Het effectief beheersen van de bedrijfsmiddelen binnen huisvesting IV. | | |
| Risico | Niet tijdig de juiste maatregelen kunnen treffen. | | |
| Control | Bedrijfsmiddelen behoren periodiek te worden gecontroleerd met 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

Betreft een beschrijving van activiteiten voor de instandhouding van huisvesting IV.

Objecttoelichting

De bedrijfsmiddelen dienen continue onderhouden te worden. Hiertoe dient de huisvesting IV-organisatie te beschikken over een onderhoudsplan.

| | | |
|--|--|-------------------------------|
| Doelstelling | Het zorgen dat vastgoed zoals gebouwen en ruimten van de rekencentra in een goede staat blijven en niet verwaarloosd worden en in verval raken. | |
| Risico | Ongeautoriseerde toegang in niet onderhouden gebouwen. | |
| 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 |

| | | | |
|----------------------|----|---|-------------|
| Onderhoudsplan | 1. | Voor kwetsbare voorzieningen (binnen en buiten het gebouw) zijn duidelijke onderhoudsbepalingen gesteld. | CIP-netwerk |
| Onderhoudsbepalingen | 2. | Het vastgoed (onder andere gebouwen) wordt op alle locaties van de huisvesting van de rekencentra onderhouden met een vastgesteld onderhoudsplan. | CIP-netwerk |

5.3.3 C.03 Continuïteitsbeheer

Objectdefinitie

Betreft een instandhoudingsproces voor alle activiteiten om de continuïteit van de te leveren huisvesting IV-diensten te waarborgen.

Objecttoelichting

Bedrijfscontinuïteit is het vermogen van de organisatie, om na een verstorend incident, producten of diensten te blijven leveren op acceptabele, vooraf vastgestelde niveaus.

Bedrijfscontinuïteitsmanagement (BCM) is het proces waarmee bedrijfscontinuïteit bereikt wordt en gaat over het voorbereiden van een organisatie op het afhandelen van versturende incidenten die anders zouden kunnen verhinderen haar doelstellingen te bereiken. Dit om de continuïteit binnen de afgesproken grenzen bij storingen en calamiteiten te waarborgen/het vereiste niveau van beschikbaarheid te kunnen waarborgen.

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 en netwerk op de lange termijn. In het control-domein gaat het om de vraag of voldoende maatregelen genomen zijn om te zorgen dat na een calamiteit huisvesting IV-services weer zo snel mogelijk hersteld kunnen worden.

Samengevat, continuïteitsbeheer:

- stelt plannen op, en onderhoudt deze, om voorbereid te zijn om na het zich voordoen van een calamiteit, zo snel mogelijk over te kunnen schakelen op noodvoorzieningen en daarna op een gestructureerde wijze terug te keren naar een (herbouwde) stabiele omgeving.
- heeft noodvoorzieningen achter de hand om de belangrijkste activiteiten zo snel mogelijk weer op te starten (uitwijk).
- is in staat om, na herstel van de oorspronkelijke omgeving, gestructureerd terug te gaan naar een situatie zoals die was voor het uitbreken van de calamiteit ('business as usual').

| | |
|--------------|---|
| Doelstelling | Het tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen. |
|--------------|---|

| | | | |
|--|--|--|--------------------|
| Risico | Onnodig lange uitval van bedrijfsactiviteiten na calamiteiten, waardoor bedrijfsdoelstellingen niet worden 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 . | | |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van | |
| Procesmatig | 1. | Het BCMS is: <ul style="list-style-type: none"> • 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 en 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 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 serviceverlening binnen de daartoe gestelde termijn voortgezet kan worden. | CIP-netwerk |
| | 6. | 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

Betreft een 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 uitgedrukt en op het juiste niveau zijn gepositioneerd.

| | |
|--------------|--|
| Doelstelling | Het invullen, coördineren en borgen van de beheersing van de huisvesting IV-dienstverlening. |
|--------------|--|

| | | | |
|--|---|--|-----------------------|
| Risico | Niet effectief ingerichte beheersorganisatie waardoor de huisvesting IV-dienstverlening niet optimaal verloopt. | | |
| 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. | | |
| Conformiteitsindicator, nummer en maatregel | | Afgeleid/afkomstig van | |
| Beheersorganisatie | 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 2017: 6.1.1 |
| | 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 |
| Processtructuur | 4. | De samenhang van de processen wordt met een processtructuur vastgelegd. | NCSC 2015: B.06.07 |