Communicatievoorzieningen

BIO Thema-uitwerking

Mei 2026 [versie 3.0 definitief]

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



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

BIO Thema-uitwerking Communicatievoorzieningen

Titel	BIO Thema-uitwerking Communicatievoorzieningen
Datum	Mei 2026
Versie en status	3.0
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	CIP-kernteamleden
Reviewers	CIP-kernteamleden

Considerans

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

Wijzigingsbeheer

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

Versie	Datum	Wijziging	Door
1.0	Februari 2019		CIP
2.0	Februari 2021		CIP
2.1	Oktober 2021		CIP
2.2	Maart 2023		CIP
2.3	November 2023	Tekstverbeteringen, BUC-afbeeldingen in tabelvorm, harde enters vervangen, doelstellingen en risico's geüniformeerd, BIO2.0-opmaat verwerkt).	CIP
3.0	Mei 2026	BIO2 1.3 verwerkt	

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 3

1 Inleiding 7

1.1 Opzet BIO Thema-uitwerking 7

1.2 Context communicatievoorzieningen 7

1.3 Scope en begrenzing communicatievoorzieningen 9

1.4 Globale relaties tussen beveiligingsobjecten 10

2 Beveiligingsobjecten Communicatievoorzieningen 11

2.1 Drie onderzoeksvragen 11

2.2 Organisatie van applicatieontwikkelingsobjecten 11

3 Beleidsdomein 12

3.1 Doelstelling 12

3.2 Risico's 12

3.3 Objecten, controls en maatregelen 12

3.3.1 B.01 Beleid, procedures en overeenkomsten voor informatietransport 12

Objectdefinitie 12

Objecttoelichting 12

3.3.2 B.02 Cryptografiebeleid voor communicatie 14

Objectdefinitie 14

Objecttoelichting 14

3.3.3 B.03 Organisatiestructuur netwerkbeheer 15

Objectdefinitie 15

Objecttoelichting 15

4 Uitvoeringsdomein 16

4.1 Doelstelling 16

4.2 Risico's 16

4.3 Objecten, controls en maatregelen 16

4.3.1 U.01 Richtlijn voor netwerkbeveiliging 17

Objectdefinitie 17

Objecttoelichting 17

4.3.2 U.02 Beveiligde inlogprocedure 18

Objectdefinitie 18
Objecttoelichting 18
4.3.3 U.03 Netwerkbeveiligingsbeheer 19
Objectdefinitie 19
Objecttoelichting 19
4.3.4 U.04 Vertrouwelijkheids- of geheimhoudingsovereenkomst 20
Objectdefinitie 20
Objecttoelichting 20
4.3.5 U.05 Beveiliging netwerkdiensten 21
Objectdefinitie 21
Objecttoelichting 21
4.3.6 U.06 Zonering en filtering 23
Objectdefinitie 23
Objecttoelichting 23
4.3.7 U.07 Elektronische berichten 23
Objectdefinitie 23
Objecttoelichting 23
4.3.8 U.08 Gateways en firewalls 25
Objectdefinitie 25
Objecttoelichting 25
4.3.9 U.09 Virtual Private Network 26
Objectdefinitie 26
Objecttoelichting 26
4.3.10 U.10 Cryptografische services 26
Objectdefinitie 26
Objecttoelichting 26
4.3.11 U.11 Draadloze toegang 27
Objectdefinitie 27
Objecttoelichting 28
4.3.12 U.12 Netwerkconnectie 28
Objectdefinitie 28
Objecttoelichting 28

4.3.13 U.13 Netwerkauthenticatie 29
Objectdefinitie 29
Objecttoelichting 29
4.3.14 U.14 Netwerkbeheeractiviteiten 29
Objectdefinitie 29
Objecttoelichting 30
4.3.15 U.15 Logging en monitoring 30
Objectdefinitie 30
Objecttoelichting 31
4.3.16 U.16 Netwerkbeveiligingsarchitectuur 32
Objectdefinitie 32
Objecttoelichting 32
5 Control-domein 33
5.1 Doelstelling 33
5.2 Risico's 33
5.3 Objecten, controls en maatregelen 33
5.3.1 C.01 Naleving richtlijn netwerkbeveiliging en evaluaties 34
Objectdefinitie 34
Objecttoelichting 34
5.3.2 C.02 Compliance-toets netwerkbeveiliging 34
Objectdefinitie 34
Objecttoelichting 34
5.3.3 C.03 Evalueren robuustheid netwerkbeveiliging 35
Objectdefinitie 35
Objecttoelichting 35
5.3.4 C.04 Evalueren netwerkgebeurtenissen (monitoring) 36
Objectdefinitie 36
Objecttoelichting 36
5.3.5 C.05 Beheersorganisatie netwerkbeveiliging 37
Objectdefinitie 37
Objecttoelichting 37

1 Inleiding

Voor u ligt de BIO Thema-uitwerking Communicatievoorzieningen, door het CIP opgesteld om overheidsorganisaties een beeld te geven van de meest relevante onderwerpen die een rol spelen bij de beveiliging van communicatievoorzieningen. Het is geënt op controls uit de Baseline Informatiebeveiliging Overheid (BIO2) 2026, NEN-EN-ISO/IEC 27002:2022 (hierna genoemd ISO 27002), implementatiestandaarden-reeks ISO 27033, The Standard of Good Practice (SoGP) 2018 en tevens op best practices van de Bundesamt für Sicherheit in der Informationstechnik (BSI).

1.1 Opzet BIO Thema-uitwerking

De BIO Thema-uitwerking Communicatievoorzieningen brengt de voor communicatiebeveiliging relevante controls uit de BIO overzichtelijk bij elkaar. Relevante items die daarin ontbreken, zijn aangevuld met behulp van de bovengenoemde kaders. De NORA-patronen zijn gebruikt voor afbeeldingen en begeleidende teksten. NORA staat voor Nederlandse Overheid Referentie Architectuur. De implementatiestandaard ISO 27033, deel 1 t/m 6, is gerelateerd aan de ISO 27002 en is hier gebruikt als referentiekader voor overzicht en technische duiding van netwerkbeveiliging.

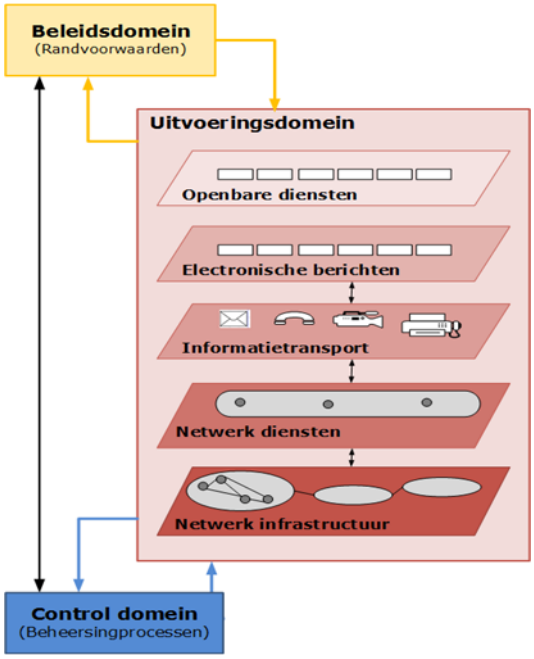
Deze thema-uitwerking volgt de standaardopzet voor BIO Thema-uitwerkingen:

- context en globale structuur van de thema-uitwerking (zie paragraaf 1.2);
- scope en begrenzing van de thema-uitwerking (zie paragraaf 1.3);
- globale relaties tussen de geïdentificeerde beveiligingsobjecten (zie paragraaf 1.4).

1.2 Context communicatievoorzieningen

De basis voor de uitwerking van de BIO Thema-uitwerking Communicatievoorzieningen is de BIO2. Deel 2 van de BIO2 bevat alle overheidsmaatregelen. Deze maatregelen zijn gekoppeld aan de beheersmaatregelen uit NEN-EN-ISO/IEC 27002:2022. Er bestaan beheersmaatregelen zonder overheidsmaatregelen. Als een dergelijke beheersmaatregel van toepassing is, wordt gebruik gemaakt van de bijbehorende implementatierichtlijn uit NEN-EN-ISO/IEC 27002. In de BIO2 en de NEN-EN-ISO/IEC 27002 worden verschillende typen communicatievoorzieningen genoemd, zoals geïllustreerd in afbeelding 1, te weten:

- Openbare diensten
  Het gebruik van openbare diensten, zoals: instant messaging en sociale media (vehikel).
- Elektronische berichten
  Informatie opgenomen in elektronische berichten (inhoud).
- Informatietransport
  Het transporteren van informatie via allerlei communicatiefaciliteiten, zoals: e-mail, telefoon, fax en video (inhoud).
- Netwerkdiensten
  Het leveren van aansluitingen, zoals: firewalls, gateways, detectiesystemen en technieken voor te beveiligen netwerkdiensten, zoals authenticatie (vehikel).
- Netwerk (infrastructuur)
  Dit betreft de fysieke en logische verbindingen (vehikel).

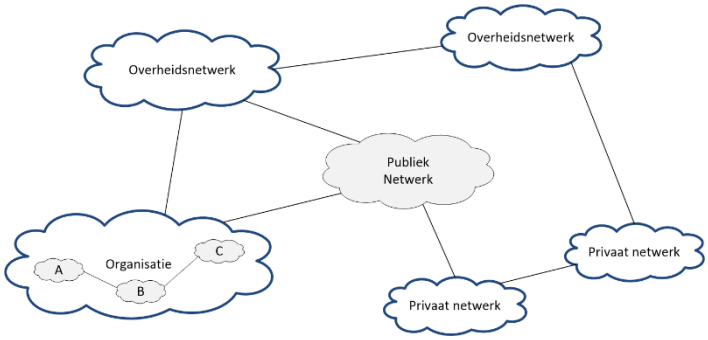


Afbeelding 1: Schematische weergave context communicatievoorzieningen

Iedere organisatie die digitaal communiceert met personen of andere organisaties in de omgeving, past deze communicatievoorzieningen toe en heeft een of meer koppelingen met de buitenwereld ingericht. De basis van deze communicatie is de netwerkinfrastructuur. De netwerkvoorzieningen omvatten zowel mobiele als vaste componenten.

Afbeelding 2 schetst de belangrijkste soorten van netwerkkoppelingen:

- tussen organisaties onderling
- tussen organisaties en publieke netwerken
- binnen organisaties



Afbeelding 2: Overzicht soorten netwerkkoppelingen

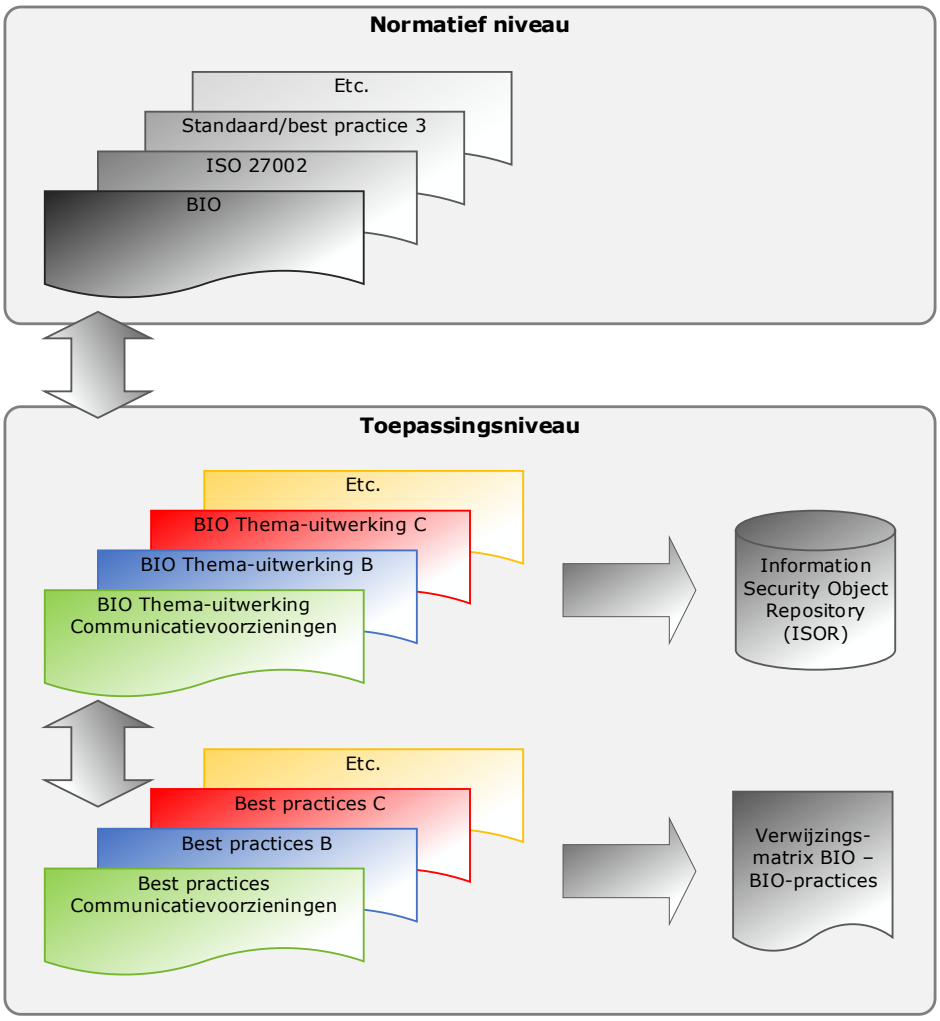
Het doel van deze netwerkkoppelingen is de uitwisseling van data tussen informatiedomeinen. Een informatiedomein is een fysiek of logisch platform met digitale informatieverwerking en of -opslag.

1.3 Scope en begrenzing communicatievoorzieningen

Deze BIO Thema-uitwerking omvat een set beveiligingsobjecten voor communicatievoorzieningen, zoals aangeduid in paragraaf 1.2.

Bepaalde typen communicatiefaciliteiten, zoals: Voice over IP (VoIP), intranet en extranet zijn in deze BIO Thema-uitwerking niet uitgewerkt. Ook wordt niet diepgaand ingegaan op typen verbindingen, zoals Virtual Private Network (VPN) en gateway-verbindingen en berichtfunctionaliteit, zoals instant messaging en e-mail.

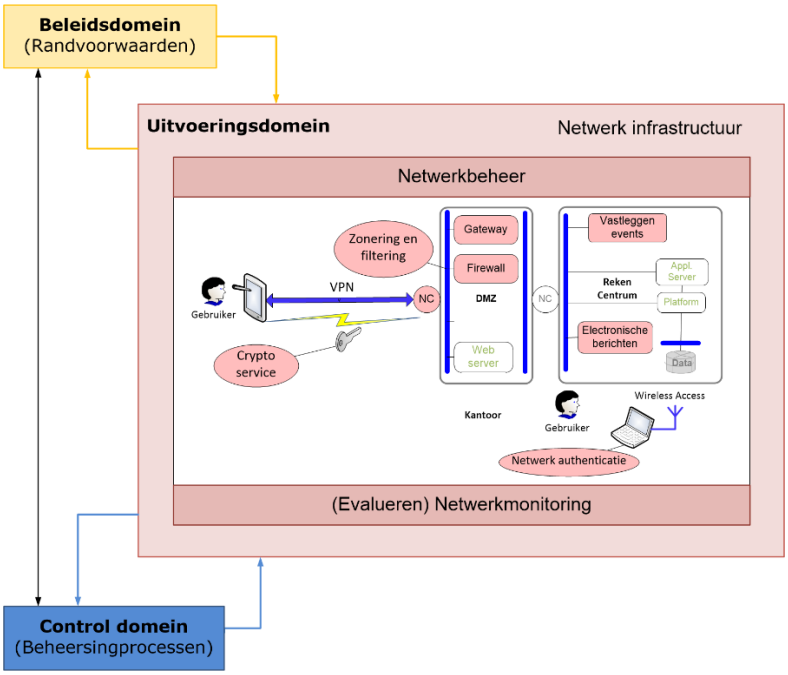
De positionering van dit themadocument in de context van baselines en overige documentatie en hulpmiddelen is weergegeven in afbeelding 3.



Afbeelding 3: Relatie BIO Thema-uitwerking Communicatievoorzieningen met aanpalende documenten

1.4 Globale relaties tussen beveiligingsobjecten

Afbeelding 4 geeft een voorbeeld van de toepassing van enkele beveiligingsobjecten in een informatievoorzieningslandschap waarin een organisatie met een gebruiker communiceert. Daarbij is sprake van netwerkconnecties die de verschillende netwerken en informatievoorzieningen met elkaar



verbinden.

Afbeelding 4: Toepassing beveiligingsobjecten

Veilige koppelingen tussen organisaties en gebruikers kunnen worden opgezet met VPN's.

Gateways en firewalls zorgen met zonering en filtering voor de beoogde scheiding van de binnen- en buitenwereld en een gecontroleerde doorgang van vertrouwde informatie.

Cryptografische services verzorgen de zonering voor het gegevenstransport via private en publieke netwerken, zodat informatie veilig kan worden uitgewisseld en bedrijfstoepassingen kunnen worden gebruikt.

In de beschermde kantooromgeving van grote organisaties worden mobiele werkplekken met het bedrijfsnetwerk verbonden via draadloze toegang en beveiligd met onder andere netwerkauthenticatie.

Een netwerkbeheerorganisatie draagt op basis van richtlijnen zorg voor de instandhouding van de netwerkbeveiliging en het actueel houden van beveiligingsmaatregelen.

Via het vastleggen van events, de evaluatie van de netwerkmonitoring en het evalueren van de netwerkbeveiliging, wordt de actuele werking van de maatregelen getoetst en waar nodig versterkt.

Meer over de technologie van beveiligingsobjecten is te vinden op NORA online onder het thema Beveiliging, bij de 'Patronen voor informatiebeveiliging'.

2 Beveiligingsobjecten Communicatievoorzieningen

2.1 Drie onderzoeksvragen

De beveiligingsobjecten die een rol spelen bij communicatievoorzieningen zijn afgeleid aan de hand van drie onderzoeksvragen, die vanuit de optiek van de BIVC-criteria (Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid) gesteld zijn:

- Welke elementen spelen vanuit de optiek van BIVC een rol bij de conditionering en sturing op communicatievoorzieningen en wat is de consequentie bij afwezigheid hiervan?
- Welke elementen spelen vanuit de optiek van BIVC een rol bij de uitvoering van communicatievoorzieningen en wat is de consequentie bij afwezigheid hiervan?
- Welke elementen spelen vanuit de optiek van BIVC een rol bij de beheersing van communicatievoorzieningen en wat is de consequentie bij afwezigheid hiervan?

2.2 Organisatie van applicatieontwikkelingsobjecten

De geïdentificeerde beveiligingsobjecten zijn ingedeeld naar drie domeinen: het beleids-, uitvoerings- en control-domein. De betekenis van deze domeinen is als volgt:

1. Beleidsdomein
   Dit domein schetst de randvoorwaarden, conditionele aspecten en beperkingen waaraan de inrichting van communicatievoorzieningen moet voldoen.

2. Uitvoeringsdomein
   Binnen dit domein bevinden zich beveiligingsobjecten die gerelateerd zijn aan de operationele activiteiten betreffende de inrichting en het beheer van communicatievoorzieningen.

3. Control-domein
   Dit domein omvat beoordelingsrichtlijnen voor het evalueren van de vastgestelde randvoorwaarden en de beveiligingsobjecten in het uitvoeringsdomein.

3 Beleidsdomein

3.1 Doelstelling

Het beleidsdomein omvat normatieve eisen voor beleid, die randvoorwaardelijk zijn bij de realisatie en exploitatie van veilige communicatievoorzieningen.

3.2 Risico's

Als beleid hiervoor ontbreekt, bestaat het risico dat onvoldoende sturing wordt gegeven aan de veilige inrichting van communicatievoorzieningen, met als mogelijk gevolg het ontstaan van datalekken en substantiële schade aan de bedrijfsvoering.

3.3 Objecten, controls en maatregelen

Tabel 1 is het resultaat van de SIVA-analyse op relevante objecten voor het communicatievoorzieningsbeleid. (Voor de betekenis en een korte uitleg van de SIVA-methodiek zie NORA online.) De afbeelding geeft een overzicht en de ordening van de beveiligingsobjecten in het beleidsdomein.

Voor de identificatie van objecten en de ordening is gebruik gemaakt van vier invalshoeken: intentie, functie, gedrag en structuur. De geelgekleurde objecten in de afbeelding zijn direct ontleend aan de BIO. Het witte object ontbreekt als control in de BIO maar is wel cruciaal voor deze BIO Thema-uitwerking.

Intentie	Functie	Gedrag	Structuur
B.01 Beleid en procedure voor informatietransport ((Operationeel) beleid)	B.01 Overeenkomst voor informatietransport (Organisatorische functie)	B.02 Cryptografiebeleid voor communicatie (Kwaliteitsfactor)	B.03 Organisatiestructuur netwerkbeheer (IT-organisatiestructuur)

Tabel 1: Beleidsobjecten met basiselementen voor communicatievoorzieningen per invalshoek

In de volgende paragrafen worden deze objecten uitgewerkt naar controls en maatregelen.

3.3.1 *B.01 Beleid, procedures en overeenkomsten voor informatietransport*

Objectdefinitie

Resultaat van een besluitvorming over - en een vastgelegde manier van handelen voor - de waarborging van de informatiebeveiliging in netwerken.

Objecttoelichting

Dit beveiligingsobject is direct ontleend aan de BIO2: 5.14. Dit object richt zich op de regels die nodig zijn voor het veilig transporteren van informatie over netwerken. In het te formuleren beleid worden onder andere standaarden en procedures beschreven voor het beveiligd inrichten en onderhouden van communicatievoorzieningen.

Doelstelling	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.		
Risico	Onvoldoende mogelijkheden om sturing te geven aan informatietransport en inconsistenties in het uitvoeren van procedures en beheersmaatregelen over informatietransport.		
Control	Er behoren **beleidsregels, procedures of overeenkomsten** voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.		ISO 27002:2022: 5.14
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beleidsregels	1.	Het beleid, de procedures en overeenkomsten omschrijven de beheersmaatregelen die ervoor zijn ontworpen om overgedragen informatie (elektronisch, fysiek en mondeling) te beschermen tegen interceptie, toegang door onbevoegden, kopiëren, wijziging, foutieve routering, vernietiging en 'denial of service', met inbegrip van toegangsbeveiligingsniveaus die passend zijn bij de classificatie van de desbetreffende informatie en eventuele speciale beheersmaatregelen die vereist zijn om gevoelige informatie te beschermen, zoals het gebruik van cryptografische technieken.	ISO 27002:2022: 5.14
	2.	Het beleid, de procedures en overeenkomsten omschrijven de beheersmaatregelen om de traceerbaarheid en onweerlegbaarheid te waarborgen, met inbegrip van het in stand houden van een bewakingsketen voor informatie tijdens het overdragen.	ISO 27002:2022: 5.14
	3.	Het beleid, de procedures en overeenkomsten omschrijven de passende contactpersonen met betrekking tot het overdragen, met inbegrip van de eigenaren van de informatie, risico-eigenaren, beveiligingsfunctionarissen en beheerders van informatie, voor zover van toepassing.	ISO 27002:2022: 5.14
Procedures	4.	Het beleid, de procedures en overeenkomsten omschrijven de verantwoordelijkheden en aansprakelijkheden in geval van informatiebeveiligingsincidenten, zoals verlies van fysieke opslagmedia of gegevens.	ISO 27002:2022: 5.14
	5.	Het beleid, de procedures en overeenkomsten beschrijven het gebruik van een afgesproken labelsysteem voor gevoelige of essentiële informatie dat waarborgt dat de betekenis van de labels meteen duidelijk is en dat de informatie passend is beschermd.	ISO 27002:2022: 5.14
	6.	Het beleid, de procedures en overeenkomsten beschrijven de eisen met betrekking tot betrouwbaarheid en beschikbaarheid van de overdrachtdienst.	ISO 27002:2022: 5.14
Beheers-maatregelen	7.	Het beleid, de procedures en overeenkomsten beschrijven het aanvaardbaar gebruik van overdragen van informatiefaciliteiten.	ISO 27002:2022: 5.14
	8.	Het beleid, de procedures en overeenkomsten omschrijven de richtlijnen voor het bewaren en verwijderen van alle bedrijfsregistraties, met inbegrip van berichten.	ISO 27002:2022: 5.14

3.3.2 *B.02 Cryptografiebeleid voor communicatie*

Objectdefinitie

Resultaat van een besluitvorming over bindende afspraken omtrent de toepassing van cryptografie binnen netwerken en de communicatiediensten die over het netwerk geleverd worden.

Objecttoelichting

In de ISO 27002 2022 worden voor communicatievoorzieningen de volgende principes expliciet genoemd:

- Beschikbaar stellen van passende en beveiligde communicatievoorzieningen. De organisatie zorgt ervoor dat alle communicatievoorzieningen (inclusief methoden voor beveiligde toegang op afstand) voorzien in passende beveiligingseisen.
- Bescherming en levenscyclusbeheer van cryptografische beheersmaatregelen. Cryptografische controles (waaronder sleutels, certificaten, algoritmen en protocollen) worden gedurende hun volledige levenscyclus beschermd en beheerd.

Doelstelling	Het beheersen van cryptografie binnen netwerken en communicatiediensten.		
Risico	Onvoldoende mogelijkheid om sturing te geven aan de effectieve en betrouwbare inrichting van cryptografische beheersmaatregelen binnen netwerken en communicatiediensten.		
Control	**Regels** voor het doeltreffende gebruik van cryptografie, met inbegrip van het **beheer** van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.		BIO2: 8.24
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: • Wanneer cryptografie ingezet wordt. • Wie verantwoordelijk is voor de implementatie. • Wie verantwoordelijk is voor het sleutelbeheer. • Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum Standaardisatie worden toegepast. • De wijze waarop het beschermingsniveau vastgesteld wordt. • Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	BIO2: 8.24.01
	2.	Aanvullend schept het cryptografiebeleid voor communicatiediensten duidelijkheid over de volgende onderwerpen: • Welke typen gegevens voor welke communicatievorm moeten worden versleuteld. • Welke typen gegevens elektronisch worden ondertekend. • Aan welke standaarden cryptografische toepassingen dienen te voldoen. • In hoeverre backward compatibility voor algoritmen en protocollen voor netwerken mag worden toegepast.	CIP-netwerk

	3.	Procedures voor het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van cryptografische sleutels zijn vastgesteld.	ISO 27002:2022: 8.24
	4.	De inhoud van dienstverleningsovereenkomsten of contracten met externe leveranciers van cryptografische diensten, zoals met een certificerende instantie, omvat onder meer de aansprakelijkheid, betrouwbaarheid van dienstverlening en responstijden voor dienstverlening.	ISO 27002:2022: 8.24

3.3.3 *B.03 Organisatiestructuur netwerkbeheer*

Objectdefinitie

Structuur waarin personen met taken, verantwoordelijkheden en bevoegdheden samenwerken bij het netwerk- en communicatiebeheer.

Objecttoelichting

De Duitse BSI benoemt voor communicatievoorzieningen meerdere principes, die aangeven dat voor het beheer van netwerken een centrale organisatiestructuur benodigd is.

Doelstelling	Het invullen, coördineren en borgen van het netwerkbeheer.		
Risico	Het niet effectief tot uitvoering komen van het beleid.		
Control	In het beleid behoort te zijn vastgesteld dat een centrale **organisatiestructuur** gebruikt wordt voor het beheren van netwerken (onder andere Local Area Network (LAN) en Virtual Local Area Network (VLAN)) en zo veel mogelijk van de hardware- en softwarecomponenten daarvan.		BSI 200-2 2017: 4.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Organisatie-structuur	1.	In de organisatiestructuur voor het netwerkbeheer zijn onder andere de volgende beheersingsprocessen benoemd: configuratie-, performance-, fault- en beveiligingsbeheer (security management).	ISO 7498-4 1991: 4.5.1
	2.	De beheer(sings)processen hebben volgens het informatiebeveiligingsbeleid een formele positie binnen de gehele organisatie.	CIP-netwerk
	3.	De taken en verantwoordelijkheden van de verantwoordelijke functionarissen voor deze processen zijn duidelijk gedefinieerd.	CIP-netwerk

4 Uitvoeringsdomein

4.1 Doelstelling

Het doel van het uitvoeringsdomein is het zorgen dat de communicatievoorzieningen zijn ingericht volgens specifieke beleidsuitgangspunten en dat aan de eisen voor de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid bij zowel het ontwerp als de implementatie is voldaan.

4.2 Risico's

De belangrijkste risico's in het uitvoeringsdomein van communicatievoorzieningen zijn:

- negatieve beïnvloeding van beveiligingsniveaus door koppeling van netwerken;
- illegaal gebruik;
- onderbrekingen;
- afluistering van getransporteerde data;
- kwetsbaarheden in uitvoerbare code;
- fysieke of logische inbreuk op netwerkelementen.

4.3 Objecten, controls en maatregelen

Per beveiligingsobject zijn hierna controls en maatregelen opgenomen die risico's kunnen reduceren. In tabel 2 zijn de essentiële beveiligingsobjecten voor het uitvoeringsdomein van communicatievoorzieningen weergegeven en geordend naar de invalshoeken Intentie, Functie, Gedrag en Structuur. De roodgekleurde objecten in de afbeelding zijn direct ontleend aan de BIO2. De witte objecten ontbreken als control in de BIO2 maar zijn wel cruciaal voor deze BIO Thema-uitwerking. Ze zijn voor een groot deel ontleend aan de ISO 27033, deel 1 t/m 6.

Intentie	Functie	Gedrag	Structuur
U.01 Richtlijn voor netwerkbeveiliging (Wet)	U.03 Netwerkbeveiligingsbeheer (Proces)	U.08 Gateways en firewalls (Verbinding (koppeling/interactie))	U.16 Netwerkbeveiligingsarchitectuur (IT-architectuur)
U.02 Beveiligde inlogprocedure ((Operationeel) beleid)	U.04 Vertrouwelijkheids- of geheimhoudingsovereenkomst (Organisatorische functie)	U.09 Virtual Private Network (Protocol)	/
/	U.05 Beveiliging netwerkdiensten (Beschermingsfunctie)	U.10 Cryptografische services (Protocol)	/
/	U.06 Zonering en filtering (Beschermingsfunctie)	U.11 Draadloze toegang (Verbinding (koppeling/interactie))	/
/	U.07 Elektronische berichten (In-/outputfunctie)	U.12 Netwerkconnectie (Verbinding (koppeling/interactie))	/

/	/	U.13 Netwerkauthenticatie (Authenticatie)	/
/	/	U.14 Netwerkbeheeractiviteiten (Handeling)	/
/	/	U.15 Logging en monitoring (Handeling)	/

Tabel 2: Uitvoeringsobjecten met -basiselementen voor communicatievoorzieningen per invalshoek

4.3.1 *U.01 Richtlijn voor netwerkbeveiliging*

Objectdefinitie

Systematisch ontwikkelde aanbevelingen voor de beveiliging van het ontwerp, de implementatie en het beheer van communicatievoorzieningen.

Objecttoelichting

De beveiliging van netwerken moet steunen op vastgelegde en nagevolgde principes en richtlijnen. Dit is van belang voor de consistentie en de controleerbaarheid van de maatregelen. Bij de uitwerking van dit object is onder meer gebruik gemaakt van de ISO 27033 (deel 1 t/m 6).

Doelstelling	Het bewerkstelligen van de benodigde coördinatie van activiteiten binnen netwerkbeveiliging.		
Risico	Aanzienlijke negatieve gevolgen voor de bedrijfsactiviteiten door het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van netwerkcomponenten en/of de uitgewisselde gegevens.		
Control	Organisaties behoren hun netwerken te beveiligen op basis van richtlijnen voor **ontwerp**, **implementatie** en **beheer**[1].		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Ontwerp	1.	De voorbereiding van veilige netwerkontwerpen omvat tenminste de volgende stappen: • identificatie van middelen (assets); • inventarisatie van functionele eisen; • beoordeling van functionele eisen in de context van het beoogd gebruik; • evaluatie van bekende toepassingsmogelijkheden en hun beperkingen; • evaluatie van bestaande ontwerpen en implementaties.	ISO 27033-2 2012: 6.1

[1] Voorbeeld: ISO 27033 deel 2.

	2.	Leidende ontwerpprincipes, zoals 'defence in depth' (of anders geformuleerd: 'inbraak betekent geen doorbraak') worden gehanteerd. Robuustheid (resilience) van het ontwerp, zoals dat onder meer bereikt kan worden door het toepassen van redundancy, back-up van configuratiegegevens en snel beschikbare reservedelen, bepaalt de beschikbaarheid van netwerken.	ISO 27033-2: 2012 7.2.4
	3.	Netwerkbeveiliging is gebaseerd op ITU-T X.80x (zie de ISO 27001 2017 Annex C).	CIP-netwerk
	4.	Netwerkontwerpen zijn gestructureerd gedocumenteerd in actuele overzichten.	CIP-netwerk
Implementatie	5.	De implementatie van netwerkbeveiliging is gebaseerd op het netwerkontwerp, zoals hierboven is bedoeld (en dat de richtlijnen volgt van de ISO 27033-2 2012, hoofdstuk 8).	CIP-netwerk
Beheer	6.	Netwerken zijn zo opgezet dat ze centraal beheerd kunnen worden.	CIP-netwerk

4.3.2 *U.02 Beveiligde inlogprocedure*

Objectdefinitie

Vastgelegde manier van handelen voor het inloggen op informatiesystemen.

Objecttoelichting

De toegang tot systemen en toepassingen wordt beheerst met beveiligde inlogprocedures. Daarbij dient de geclaimde identiteit op passende wijze en met gebruik van een geschikte techniek te worden vastgesteld. De procedure om in te loggen wordt zo ontworpen, dat de kans op onbevoegde toegang minimaal is.

Doelstelling	Het voorkomen van onbevoegde toegang tot (communicatie)systemen en toepassingen.		
Risico	Misbruik en verlies van gevoelige gegevens en beïnvloeding van beschikbaarheid van (communicatie)systemen.		
Control	Er behoren beveiligde **authenticatietechnologieen en -procedures** te worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.		ISO 27002:2022: 8.05
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Authenticatiet echnologieen en -procedures	1.	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	BIO2: 8.05.01
	2.		

	3.	Toegang tot netwerken is beperkt tot geautoriseerde gebruikers (en geautoriseerde applicaties). Drie expliciete inlogmechanismen en hun toepassingsgebieden zijn: • Remote login Voor gebruikers die van buiten inloggen op de door de organisatie beheerde bedrijfsnetwerken. • Versterkte authenticatie Voor toepassingen waarbij de 'standaard'-authenticatie van gebruikers (en applicaties) kan worden gecompromitteerd. • Single Sign-On Voor situaties waarbij netwerken worden geacht authenticatie-checks uit te voeren voor verschillende toepassingen.	CIP-netwerk

4.3.3 *U.03 Netwerkbeveiligingsbeheer*

Objectdefinitie

Instandhoudingsproces voor beveiligingsprocedures en -mechanismen van een netwerk.

Objecttoelichting

Het beheer en de beheersing van netwerken zijn randvoorwaarden voor netwerkbeveiliging. Ze vormen garanties voor de veiligheid van de informatie die via netwerken en ondersteunende informatieverwerkende faciliteiten wordt getransporteerd.

Doelstelling	Het bereiken van de netwerkbeveiligingsdoelen en het in goede staat houden van de netwerkbeveiliging.		
Risico	Informatie in netwerken is niet beschermd.		
Control	Netwerken en netwerkapparaten behoren te worden beveiligd**, beheerd** en **beheerst** om informatie in systemen en toepassingen te beschermen.		ISO 27002:2022: 8.20
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beheerd	1.	Voor het beheer van netwerkapparatuur zijn verantwoordelijkheden en procedures vastgesteld.	ISO 27002:2022: 8.20.b
	2.	Netwerken worden geregistreerd en gemonitord volgens vastgelegde procedures en richtlijnen.	ISO 27002:2022: 8.20.f
	3.	Beheeractiviteiten worden nauwgezet gecoördineerd, zowel om de dienstverlening voor de organisatie te optimaliseren als om te zorgen dat beheersmaatregelen consistent in de hele informatieverwerkende infrastructuur worden toegepast.	ISO 27002:2022: 8.20.g
	4.	Er zijn procedures opgesteld om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens die via openbare of draadloze netwerken worden verzonden te waarborgen, en om aangesloten systemen en toepassingen te beschermen.	ISO 27002:2022: 8.20.e
Beheerst	5.	De operationele verantwoordelijkheid voor netwerken zijn gescheiden van de operationele activiteiten met de ICT-systemen,	ISO 27002:2022: 8.20.d

	6.	De verbinding van systemen en apparaten met het netwerk wordt beperkt, gefilterd en geauthenticeerd (bijvoorbeeld door firewalls).	ISO 27002:2022: 8.20.i,j
	7.	Netwerkapparatuur is gehardened en netwerkbeheerkanalen zijn gescheiden van regulier netwerkverkeer.	ISO 27002:2022: 8.20.k,l
	8.	Kritieke subnetwerken kunnen tijdelijk worden geïsoleerd bij (vermoedelijke) aanvallen.	ISO 27002:2022: 8.20.m
	9.	Kwetsbare netwerkprotocollen zijn uitgeschakeld.	ISO 27002:2022: 8.20.n
	10.	Netwerkcomponenten voldoen minimaal aan het vertrouwelijkheidsniveau van het netwerk waarvan ze onderdeel zijn.	BIO2: 8.20.01
	11.	Toegang tot beheerinterfaces van netwerkcomponenten zijn zo veel als mogelijk gescheiden van het gebruikersnetwerk.	BIO2: 8.20.02

4.3.4 *U.04 Vertrouwelijkheids- of geheimhoudingsovereenkomst*

Objectdefinitie

Geheel van afspraken over het waarborgen van de vertrouwelijkheid/geheimhouding van informatie.

Objecttoelichting

In vertrouwelijkheids- of geheimhoudingsovereenkomsten worden, binnen juridisch afdwingbare voorwaarden, de eisen vastgelegd voor de benodigde bescherming van vertrouwelijke informatie.

Doelstelling	Het beschermen van vertrouwelijke informatie van de organisatie bij (keten)partners en dienstverleners van de organisatie.	
Risico	Dienstverleners en partners zijn niet (voldoende) bekend met de actuele benodigde eisen van de organisatie voor het beschermen van informatie.	
Control	**Vertrouwelijkheids- of geheimhoudingsovereenkomsten** die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	ISO 27002:2022: 6.6
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Vertrouwelijkheids- of geheimhoudingsovereenkomsten	1.	Bij het opstellen van eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten wordt rekening gehouden met ten minste de volgende elementen: • definitie van de te beschermen (vertrouwelijke) informatie; • looptijd van de overeenkomst, inclusief eventuele onbeperkte geheimhouding of geheimhouding tot de informatie openbaar is; • vereiste acties bij beëindiging van de overeenkomst; • verantwoordelijkheden van de ondertekenaars ter voorkoming van ongeoorloofde openbaarmaking; • eigendom van informatie, handelsgeheimen en intellectuele eigendom; • toegestaan gebruik van de vertrouwelijke informatie en de rechten van de ondertekenaar; • recht op audit en monitoring van activiteiten waarbij vertrouwelijke informatie is betrokken; • procedure voor notificatie en melding van lekken of ongeoorloofde openbaarmaking; • voorwaarden voor retourneren of vernietigen van informatie na beëindiging; • maatregelen die worden getroffen bij niet-naleving van de overeenkomst.	ISO 27002:2022: 6.6.a t/m j

4.3.5 *U.05 Beveiliging netwerkdiensten*

Objectdefinitie

Geheel van specifieke eisen aan maatregelen voor de beveiligingsmechanismen, het dienstverleningsniveau en de kwaliteit van beheerprocessen.

Objecttoelichting

De eisen die aan dienstverleners gesteld worden voor communicatievoorzieningen betreffen enerzijds de verantwoordelijkheden voor de informatiebeveiliging van het transport en de distributie van informatie en anderzijds de beveiligde toegang tot de transportvoorzieningen zelf.

Doelstelling	Het waarborgen van continuïteit en veiligheid van de dienstverlening en bedrijfsvoering, bij uitval van netwerkdiensten.		
Risico	Uitval van kritische processen van de organisatie.		
Control	**Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen** voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en gemonitord**.**		ISO 27002:2022: 8.21
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-mechanismen	1.	De noodzakelijke beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen van netwerkdiensten zijn geïdentificeerd, geïmplementeerd en worden gemonitord. Dit geldt zowel voor intern geleverde als voor uitbestede netwerkdiensten.	ISO 27002:2022: 8.21

	2.	Bij transport van gegevens over draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied worden gegevens versleuteld met uitzondering van metagegevens die noodzakelijk zijn om het transport tot stand te laten komen. De inrichting van de versleuteling is risicogericht en houdt rekening met de noodzakelijke beschermingstermijn en het noodzakelijke beschermingsniveau. Hierbij wordt waar mogelijk gebruik gemaakt van encryptiemiddelen waarvoor de Unit Weerbaarheid van het NBV van de AIVD een positief inzetadvies heeft afgegeven. Als de Unit Weerbaarheid geen encryptiemiddelen heeft geadviseerd, wordt in overleg met de CISO een andere geschikte versleutelingsmethodiek gekozen en ingericht.	BIO2: 8.21.04
	1.	De volgende Open Systems Interconnection (OSI)-lagen moeten beveiligingsmechanismen voor communicatie bevatten: • Applicatieniveau Voor authenticiteit, integriteit, vertrouwelijkheid en onweerlegbaarheid: encryptie. • Transportniveau Voor veilige point-to-point verbindingen: encryptie. • Netwerkniveau Voor veilige communicatie tussen devices, firewalls en netwerkverbindingen: VPN en encryptie.	CIP-netwerk
Dienstverle-ningsniveaus	2.	Het dienstverleningsniveau wordt afgestemd op de volgende eisen: • de vereiste performance en beschikbaarheid van het netwerk; • de toegestane verbindingstypen; • de toegestane netwerkprotocollen; • de toegepaste applicaties op de te leveren netwerkservices; • de beoogde architectuur- en ontwerpprincipes.	CIP-netwerk
Beheereisen	3.	Het dataverkeer van of naar de vertrouwde omgeving, wordt bewaakt/geanalyseerd op verdacht verkeer met detectievoorzieningen.	BIO2: 8.21.02
	4.	Bij ontdekte nieuwe dreigingen vanuit overheidsmaatregel 8.21.02 worden deze doorgeleid, rekening houdend met de geldende juridische kaders gedeeld binnen de overheid.	BIO2: 8.21.03
	5.	In koppelpunten met externe of onvertrouwde zones en vanwege netwerksegmentatie zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en te mitigeren.	BIO2: 8.21.01
	6.	Met de communicerende partijen worden afspraken gemaakt over: • de wederzijdse authenticatie; • de bevoegdheden voor het gebruik van de dienst; • de integriteit en vertrouwelijkheid van transacties, belangrijke documenten en de onweerlegbaarheid van de ontvangst; • een passende verificatie voor de controle van de transactie.	CIP-netwerk

4.3.6 *U.06 Zonering en filtering*

Objectdefinitie

Scheiding van netwerken in afzonderlijke fysieke of logische domeinen, alsmede de regulering van toegang en informatiestromen tot deze domeinen.

Objecttoelichting

Door scheiding aan te brengen in netwerken, ook wel segmentering genoemd, kunnen netwerken worden beheerd, beveiligd en beheerst. Om vervolgens vanuit het ene netwerk naar het andere veilig te kunnen communiceren, zijn gecontroleerde doorgangen nodig. In die doorgangen worden filtermechanismen aangebracht, die alleen toegestane communicatie doorlaten en de toegang beperken tot geautoriseerde personen, processen of apparaten. De scheiding met gecontroleerde doorgangen heet 'zonering'.

Doelstelling	Het voorkomen van kruisbesmetting en discontinuïteit van de organisatie ten gevolgde van besmetting op een plek/een proces.		
Risico	Verspreiding van aanvallen, indringers, ongewenste inhoud, virussen etc. in de organisatie.		
Control	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden **gescheiden (in domeinen)**.		ISO 27002:2022: 8.22
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gescheiden (in domeinen)	1.	Netwerken worden gesegmenteerd in afzonderlijke netwerkdomeinen (logisch of fysiek) op basis van betrouwbaarheids-, kritikaliteits- of gevoeligheidsniveaus, organisatieafdelingen of een combinatie daarvan. De buitengrenzen van elk domein zijn duidelijk gedefinieerd.	CIP-netwerk
	2.	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	BIO2: 8.22.01
	3.	De toegang tussen netwerkdomeinen wordt beheerst door gateways (bijvoorbeeld firewalls of filterende routers). De criteria voor segmentatie en de toegestane toegang via gateways zijn gebaseerd op een beoordeling van de beveiligingseisen, de classificatie van informatie en het onderwerpspecifieke toegangsbeveiligingsbeleid.	ISO 27002:2022: 8.22
	4.	Draadloze netwerken worden gescheiden van interne netwerken en personeelnetwerken. Voor gevoelige omgevingen wordt draadloze toegang behandeld als een externe verbinding en via een gateway gesegmenteerd van interne systemen.	ISO 27002:2022: 8.22

4.3.7 *U.07 Elektronische berichten*

Objectdefinitie

Geautomatiseerd of via een gebruikersinteractie elektronisch uitwisselen van informatie.

Objecttoelichting

Beveiliging van elektronisch berichtenverkeer omvat bijvoorbeeld e-mail, webverkeer, chatsessies en streaming van audio en video. Maatregelen ter bescherming van het berichtenverkeer betreffen:

- een correcte adressering;
- een geautoriseerde toegang;
- een integer datatransport;
- het toereikend zijn van de beschikbaarheid;
- het voldoen aan (wettelijke) bepalingen voor de elektronische handtekening en onweerlegbaarheid.

Doelstelling	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.		
Risico	Het aantasten van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie in elektronisch berichtenverkeer.		
Control	Er behoren regels, procedures of overeenkomsten voor **informatieoverdracht** te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.		ISO 27002:2022: 5.14
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Informatieoverdracht	1.	Internetfacing-informatiesystemen en e-mail-berichtenverkeer blijven voldoen aan de verplichte beveiligingsstandaarden, zie hiervoor de website van het Forum Standaardisatie en het Cyberbeveiligingsbesluit. Hierop wordt gestuurd met de metingen van internet.nl. Daarbij dienen alle onderdelen te worden ingesteld zodat een optimale beveiliging wordt bereikt zonder afbreuk te doen aan de functionaliteit van de geboden dienst.	BIO2: 5.14.01
	2.	De entiteit maakt bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated (OV)-certificaten. De entiteit maakt bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten vloeien voort uit een risicoanalyse, aansluitvoorwaarden of wetgeving.	BIO2: 5.14.02
	3.	Geavanceerde en/of gekwalificeerde elektronische handtekeningen voldoen aan de Advanced Electronic Signatures (AdES Baseline Profiles), zoals opgenomen in de Lijst open standaarden van Forum Standaardisatie.	BIO2: 5.14.03
	4.	Van alle internetfacing-informatiesystemen, webapplicaties, IP-adressen en API's is er een actuele registratie.	BIO2: 5.14.04
	5.	Publiek toegankelijke websites worden bekend gemaakt via het Register Internetdomeinen Overheid (RIO). Deze informatie wordt ten minste iedere zes maanden geactualiseerd.	BIO2: 5.14.05

	6.	In het beleid, de procedures en overeenkomsten met betrekking tot elektronisch transport van informatie zijn onder meer de volgende regels opgenomen: • bescherming tegen malware die via elektronische communicatie kan worden verspreid; • beveiliging van gevoelige informatie die als bijlage wordt verzonden; • het voorkomen van het versturen van documenten en berichten naar onjuiste adressen of nummers; • voorafgaande toestemming voor het gebruik van externe openbare communicatiediensten (zoals instant messaging, sociale netwerken, file sharing en cloudopslag); • toepassing van sterkere authenticatie bij het verzenden van informatie via openbaar toegankelijke netwerken; • beperkingen op het gebruik van elektronische communicatiefaciliteiten (bijvoorbeeld het automatisch doorsturen van e-mail naar externe adressen); • het advies aan personeel en andere belanghebbenden om geen essentiële of gevoelige informatie via sms of andere instant messaging-diensten te verzenden.	ISO 27002:2022: 5.14

4.3.8 *U.08 Gateways en firewalls*

Objectdefinitie

Beveiligingsmechanismen voor zonering en filtering.

Objecttoelichting

Gateways en firewalls realiseren de maatregelen voor zowel zonering als filtering. De implementatiestandaard voor gateways, de ISO 27033-4 2014, bevat hiervoor het principe dat gateways en firewalls filterfuncties behoren te bevatten, die zodanig geconfigureerd zijn dat alle netwerkverkeer, zowel inkomend als uitgaand, wordt gecontroleerd en dat uitsluitend toegestaan netwerkverkeer wordt doorgelaten.

Doelstelling	Het detecteren en blokkeren van ongeautoriseerd inkomend en uitgaand dataverkeer.		
Risico	Misbruik van netwerkverkeer van buitenaf en naar buiten toe.		
Control	De **filterfuncties** van gateways en firewalls behoren zo te zijn geconfigureerd, dat inkomend en uitgaand netwerkverkeer wordt gecontroleerd en dat daarbij in alle richtingen uitsluitend het vanuit beveiligingsbeleid **toegestaan** netwerkverkeer wordt doorgelaten.		ISO 27033-4 2014: 6
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Filterfuncties	1.	Voor elke gateway of firewall bestaat een actueel configuratiedocument dat de complete configuratie en de functionele eisen van de gateway of firewall beschrijft.	SoGP 2018: NC1.5.11
	2.	De filterfuncties van gateways en firewalls zijn instelbaar.	SoGP 2018: NC1.5.5

	3.	Gebeurtenissen worden vastgelegd in auditlogs en worden, indien aanwezig, doorgegeven aan centrale systemen, zoals het Security Information and Event Management systeem (SIEM).	CIP-netwerk
Toegestaan	4.	Uitsluitend toegestaan netwerkverkeer wordt doorgelaten.	CIP-netwerk

4.3.9 *U.09 Virtual Private Network*

Objectdefinitie

Beveiligingsmechanisme voor het inrichten van vertrouwde toegang tussen twee of meer netwerkknooppunten.

Objecttoelichting

Een VPN is een zoneringsmaatregel die een strikte scheiding van netwerkconnecties met andere netwerken mogelijk maakt tussen zowel publieke als private netwerken. De ISO 27033-5 2013 is een implementatiestandaard voor VPN's en bevat een aantal eisen die gesteld moeten worden aan VPN's.

Doelstelling	Het zorgen voor een veilige verbinding, waarbij getransporteerde informatie over netwerken vertrouwelijk blijft.		
Risico	Onbevoegden krijgen toegang tot getransporteerde informatie over de netwerken.		
Control	Een VPN behoort een strikt **gescheiden end-to-end connectie** te geven, waarbij de getransporteerde informatie, is voorbehouden aan tot de organisatie die de VPN gebruikt.		ISO 27033-5 2013: 6.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gescheiden end-to-end connectie	1.	De end-to-end connectie: • wordt gecreëerd door scheiding van de adresseringsruimte en routeringen tussen VPN's over het onderliggende netwerk; • geeft garanties dat de interne structuur van het onderliggende netwerk niet zichtbaar is voor andere netwerken; • biedt bescherming tegen denial of service attacks en ongeautoriseerde toegang; • biedt bescherming tegen label spoofing (het mogelijk injecteren van foute labels).	ISO 27033-5 2013: 7

4.3.10 *U.10 Cryptografische services*

Objectdefinitie

IT-services voor de versleuteling van het netwerkverkeer, die op meerdere lagen van het Open Systems Interconnection (OSI)-model kunnen voorkomen.

Objecttoelichting

Cryptografische services van communicatievoorzieningen zijn beheersmaatregelen ter bescherming van de integriteit en vertrouwelijkheid van gegevens. Cryptografie wordt behalve voor de versleuteling van informatie (zonering) ook gebruikt voor de authenticatie en autorisatie van gegevens en

netwerkconnecties. Cryptografische services voor de communicatie met partners en burgers maken gebruik van Public-Key-Infrastructure (PKI)-middelen, zoals de aan certificaten gebonden private en publieke sleutels.

De ISO 27002 2022 normeert het beleid voor cryptografie en sleutelbeheer. Het NCSC en de Unit Weerbaarheid van het NBV van de AIVD adviseert passende beheersmaatregelen.

Doelstelling	Het behouden van de vertrouwelijkheid en integriteit van de getransporteerde informatie.		
Risico	Het openbaar worden van vertrouwelijke informatie en/of het corrumperen van informatie door kwaadwillenden.		
Control	Ter bescherming van de **vertrouwelijkheid** en **integriteit** van de getransporteerde informatie behoren passende **cryptografische beheersmaatregelen** te worden ontwikkeld, geïmplementeerd en ingezet.		ISO 27002:2022: 8.24
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Vertrouwelijk-heid	1.	Vanwege de vertrouwelijkheid van de communicatie tussen de zender en ontvanger wordt versleuteling toegepast op een of meer van de juiste verbindingslagen (OSI-laag 1 t/m 7). PKI faciliteert deze functie.	ISO 27033-1 2015: 8.8
Integriteit	2.	Vanwege de integriteit van de communicatie tussen de zender en ontvanger wordt een digitale ondertekening toegepast. Toepassingsvoorbeelden zijn: • communicatieprotocollen die de ontvangst onweerlegbaar maken; • applicatieprotocollen die de signatuur van de zender gebruiken voor onweerlegbaarheid van de ontvangst en de integriteit van de data.	ISO 27033-1 2015: 8.8
Cryptogra-fische beheers-maatregelen	3.	Cryptografische beheersmaatregelen zijn opgenomen in de inventaris van de bedrijfsmiddelen. Voor alle cryptografische beheersmaatregelen is vastgesteld waar ze worden ingezet, wie ervoor verantwoordelijk is en hoe ze actueel worden gehouden.	BIO2: 8.24.02
	4.	De sterkte van de cryptografie wordt gebaseerd op de actuele adviezen van het NCSC en de Unit Weerbaarheid van het NBV van de AIVD.	BIO2: 8.24.04
	5.	Er zijn afspraken over reservecertificaten van een alternatieve leverancier als uit de risicoafweging blijkt dat deze noodzakelijk zijn als onderdeel van gereedheid voor bedrijfscontinuïteit.	BIO2: 8.24.05

4.3.11 *U.11 Draadloze toegang*

Objectdefinitie

Communicatie van apparaten met een computernetwerk via elektromagnetische straling.

Objecttoelichting

Draadloze toegang (wireless access), bedoeld voor mobiele communicatie, is kwetsbaarder dan toegang via vaste verbindingen. De implementatiestandaard ISO 27033-6 2016 beschrijft de operationele maatregelen voor draadloze netwerken.

Doelstelling	De beperking van het gebruik van devices tot bevoegde personen en het behoud van beschikbaarheid, integriteit en vertrouwelijkheid van draadloze communicatie.		
Risico	Draadloos verzonden informatie komt in handen van onbevoegden terecht.		
Control	Draadloos verkeer behoort te worden beveiligd met **authenticatie** van devices, **autorisatie** van gebruikers **en versleuteling** van de communicatie.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Authenticatie, autorisatie en versleuteling	1.	Omdat draadloze netwerken altijd en overal fysiek benaderbaar zijn, worden de volgende algemene maatregelen en beveiligingslagen altijd toegepast: • netwerktoegangscontrole (IEEE 802.1x) en apparaat-authenticatie (EAP-TLS); ter bescherming van netwerken tegen aansluiting van ongeautoriseerde gebruikers; • integriteitcontrolemechanismen; ter voorkoming van man-in-the-middle attacks; • encryptie op netwerkniveau; het sterkst mogelijke algoritme/protocol wordt standaard toegepast met backwards compatibility-mogelijkheden voor de ondersteuning van oudere of minder sterke protocollen; • autorisatie van mobiele clients, bijvoorbeeld via Media Access Control (MAC)-adresfiltering; • toegangscontrole van eindgebruikers, bijvoorbeeld via Role Based Access Control (RBAC); • niet toegestane typen netwerkverkeer worden geblokkeerd; • niet benodigde functies zijn altijd uitgeschakeld (hardening); • bekende kwetsbaarheden in de systeemsoftware worden doorlopend opgelost (patching en patchmanagement).	SoGP 2018: NC1.3.5

4.3.12 *U.12 Netwerkconnectie*

Objectdefinitie

Verbinding met de op het netwerk aangesloten computers.

Objecttoelichting

Het geheel van netwerkconnecties kan, vooral in grotere organisaties, complexe vormen aannemen. Een goed overzicht en inzicht is daarom van groot belang bij het beheer. De ISO 27033-2 2012 benoemt in een principe dat alle gebruikte segmenten, routeringen, verbindingen en aansluitpunten van een bedrijfsnetwerk bekend behoren te zijn en te worden bewaakt.

Doelstelling	Het door een compleet inzicht omtrent routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk kunnen minimaliseren van uitval, bij storingen en calamiteiten.

Risico	Bij beheer, storingen en calamiteiten kan niet of minder effectief worden gereageerd.		
Control	Alle gebruikte routeringen, segmenten, **verbindingen** en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden **bewaakt**.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verbindingen	1.	Voor de beheersing van netwerken zijn minimaal nodig: • de identificatie van alle soorten netwerkverbindingen die worden gebruikt; • een actuele lijst van toegestane en gebruikte protocollen; • een actuele lijst van gebruikte netwerktoepassingen; • een continu onderzoek naar beveiligingsrisico's voor netwerken; • een actuele netwerktopologie en daarvoor geldende beveiligingseisen.	SoGP 2018: NC1.4.1a
Bewaakt	2.	Netwerken worden bewaakt op het beoogd gebruik en overtreding van het beveiligingsbeleid wordt gelogd.	CIP-netwerk

4.3.13 *U.13 Netwerkauthenticatie*

Objectdefinitie

Voorziening die controleert of een apparaat geautoriseerd is om op het netwerk te kunnen worden aangesloten.

Objecttoelichting

Inherent aan het protocol IEE 801.x dient authenticatie van netwerkknooppunten te worden toegepast om het onbevoegd aansluiten van netwerkdevices te voorkomen (bijvoorbeeld door 'sniffing': ofwel afluisteren).

Doelstelling	Het toelaten van uitsluitend vooraf toegestane netwerkdevices op het netwerk.		
Risico	Ongeautoriseerde netwerkdevices worden aangesloten op het netwerk.		
Control	**Authenticatie van netwerkknooppunten** behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Authenticatie van netwerkknoop punten	1.	Alvorens logisch toegang te verkrijgen tot een netwerk wordt de authenticiteit van een aangesloten netwerk-device gecontroleerd (EAP-TLS).	CIP-netwerk
	2.	Alleen de specifiek voor het netwerk toegestane netwerkdevices worden logisch gekoppeld aan het netwerk (IEE 802.1x).	CIP-netwerk

4.3.14 *U.14 Netwerkbeheeractiviteiten*

Objectdefinitie

Geheel van activiteiten, benodigd voor het beheer en het beschikbaar stellen van netwerken door daartoe bevoegde beheerders.

Objecttoelichting

Netwerkbeheer is een randvoorwaarde voor informatiebeveiliging. Beheeractiviteiten behoren nauwgezet te worden gecoördineerd met het oog op coherente toepassing daarvan, alsook ter borging van een ongestoorde en veilige dienstverlening.

Doelstelling	Het bereiken en behouden van het noodzakelijke netwerkbeveiligingsniveau.		
Risico	Informatie in netwerken is niet beschermd.		
Control	Netwerken behoren te worden **beheerd** en **beheerst** om informatie in systemen en toepassingen te beschermen.		ISO 27002:2022: 8.20
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**

Beheerd	1.	Netwerkbeveiligingsbeheer omvat activiteiten, methoden, procedures en gereedschappen voor administratie, onderhoud en veilig beschikbaar stellen van netwerkverbindingen. Met name geldt daarbij:
		• Administratie:
		  ○ Het continue actualiseren van de netwerktopologie.
		  ○ Het beheersen en 'huishouden' van netwerk-resources en de wijze waarop die beschikbaar zijn gesteld.
		• Beschikbaarheidsbeheer:
		  ○ Het zorgdragen dat netwerkfaciliteiten constant beschikbaar zijn en dat het netwerk wordt gemonitord, zodat onderbrekingen zo vroeg mogelijk worden ontdekt en verholpen.
		• Incidentmanagement:
		  ○ Het zorgdragen dat op alle incidenten en bevindingen actie wordt ondernomen, met rapportage.
		• Technische kwetsbaarhedenmanagement:
		  ○ Het verzamelen en uitvoeren van beveiligingsupgrades, zoals het aanbrengen van patches tegen kwetsbaarheden in firmware of netwerk-Operating Software (OS) en het nemen van preventieve maatregelen voor fysieke kwetsbaarheden, zoals ongeautoriseerde toegang tot netwerkbekabeling.
		  ○ Het verhelpen van fysieke kwetsbaarheden in het netwerk, zoals bescherming tegen ongeautoriseerde (fysieke) toegang van netwerksegmenten.
			ISO 27033-2 2012: 8.4

Beheerst	2.	Netwerkbeheer omvat het doorvoeren van logische en fysieke wijzigingen in netwerken, zoals het aanpassen van de zonering (logisch) en patching van netwerkbekabeling in netwerk-verdeelkasten (fysiek).	CIP-netwerk

4.3.15 *U.15 Logging en monitoring*

Objectdefinitie

Het vastleggen van netwerk-events, het onderkennen van informatiebeveiliging gerelateerde gebeurtenissen en het signaleren van afwijkingen van verwacht gedrag.

Objecttoelichting

Het gebruik van communicatievoorzieningen impliceert een grote stroom van gebeurtenissen (events), die continue moeten worden geregistreerd en bewaakt. Afwijkingen op verwacht gedrag of voorgeschreven beleid worden gesignaleerd, geanalyseerd en beoordeeld op risico's. Schadelijke events kunnen hierdoor worden gesignaleerd en eventuele schade hersteld. Op basis van deze voorvallen kan worden geleerd en kunnen beveiligingsmaatregelen worden aangescherpt.

Voor dit proces kan gebruik gemaakt worden van een SIEM-systeem of van een functioneel gelijkwaardig systeem. Voor het beoordelen van de gebeurtenissen is specifieke deskundigheid vereist.

Doelstelling	Het tijdig detecteren, vastleggen en analyseren van ongeoorloofde en/of onjuiste gebeurtenissen in netwerken, gericht op het voorkomen en kunnen herstellen van de situatie.		
Risico	Afwijkingen van normaal gedrag zijn niet zichtbaar en niet te onderzoeken. Herstelacties kunnen niet tijdig worden genomen.		
Control	Netwerken, systemen en toepassingen behoren te worden **gemonitord** op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren; logbestanden worden **geregistreerd en bewaard**.		ISO 27002:2022: 8.16
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gemonitord	1.	De informatieverwerkende omgeving wordt gemonitord met een detectie- en response-oplossing, waarmee aanvallen kunnen worden gedetecteerd en afwijkingen worden adequaat en tijdig behandeld.	BIO2: 8.16.03
	2.	De SIEM en/of het Security Operations Centre (SOC) hebben eenduidige regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	BIO2: 8.16.02
	3.	Bij ontdekte nieuwe dreigingen (aanvallen) worden deze binnen geldende juridische kaders verplicht gedeeld met de daarvoor aangewezen Computer Emergency Response Team (CERT).	BIO2: 8.16.01
Geregistreerd en bewaard	4.	Aan logboeken en bewaking worden strenge eisen gesteld. Voor de kritieke componenten zijn geavanceerde beveiligingen voor logboeken en bewaking gedefinieerd.	CIP-netwerk
	5.	De toegang tot en het beheer van de loggings- en monitoringsfunctionaliteit is beperkt tot geselecteerde en geautoriseerde medewerkers.	CIP-netwerk
	6.	Wijzigingen in logging en monitoring worden gecontroleerd door onafhankelijke en geautoriseerde medewerkers. (Logregels mogen nooit worden gewijzigd; deze zijn immers bedoeld om als bewijslast te kunnen gebruiken.)	CIP-netwerk
	7.	De bewaartermijn van logbestanden en gegevens in het Security Incident en Event Monitoring (SIEM) worden risicogericht bepaald, rekening houdend met het scenario dat aanvallers langdurig binnen zijn.	BIO2: 8.15.04

4.3.16 *U.16 Netwerkbeveiligingsarchitectuur*

Objectdefinitie

Modelmatige beschrijving van de samenhang van technische beveiligingsfuncties in een netwerk.

Objecttoelichting

In de ISO 27033 deel 2 2012 wordt over netwerkbeveiligingsarchitectuur geschreven dat deze de samenhang van het netwerk beschrijft en structuur biedt voor de beveiligingsmaatregelen.

De netwerkbeveiligingsarchitectuur moet zijn gebaseerd op het vigerende bedrijfsbeleid, leidende principes en geldende normen en standaarden.

Doelstelling	Het verkrijgen van inzicht in het netwerkbeveiligingslandschap en de inrichting van de samenhangende beveiligingsmaatregelen.		
Risico	Geen sturing hebben op de netwerkbeveiliging.		
Control	De beveiligingsarchitectuur behoort de **samenhang** van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende principes en de geldende normen en standaarden.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Samenhang	1.	De beveiligingsarchitectuur staat niet op zichzelf, maar is verweven met de architectuur van het te beveiligen netwerk.	CIP-netwerk
	2.	De beveiligingsarchitectuur is gelaagd, zoals in: het (Nederlandse Overheid Referentie Architectuur) NORA-beveiligingsmetamodel of Sherwood Applied Business Security Architecture (SABSA®).	CIP-netwerk
	3.	De netwerktopologie is in kaart gebracht en wordt continu actueel gehouden.	CIP-netwerk

5 Control-domein

5.1 Doelstelling

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

- de controls voldoende zijn ingericht en functioneren om de beschikbaarheid, integriteit en betrouwbaarheid van netwerkdiensten te kunnen garanderen;
- het beoogde beveiligingsniveau van technische netwerkdiensten en netwerkcomponenten 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

Als de noodzakelijke control-maatregelen binnen de organisatie ontbreken, is het niet zeker dat de netwerkomgeving aan de beoogde organisatorische en beveiligingsvoorwaarden voldoet en dat de naleving van deze voorwaarden toereikend is ingericht. Ook kan niet worden vastgesteld dat gewenste beveiligingsmaatregelen worden nageleefd.

5.3 Objecten, controls en maatregelen

Tabel 3 is het resultaat van de SIVA-analyse op relevante objecten voor netwerk-control. De blauwgekleurde objecten zijn afgeleid van de BIO2. De witte objecten zijn afgeleid van overige best practices.

Intentie	Functie	Gedrag	Structuur
C.01 Naleving richtlijn netwerkbeheer en evaluaties ((Operationeel) beleid)	C.02 Compliance-toets netwerkbeveiliging (Organisatorische functie)	C.04 Evalueren netwerkgebeurtenissen (monitoring) (Event/historie)	C.05 Beheersorganisatie netwerkbeveiliging (IT-organisatiestructuur)
/	C.03 Evalueren robuustheid netwerkbeveiliging (Proces)	/	/

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

De objecten van het control-domein van communicatievoorzieningen zijn in onderstaande paragrafen uitgewerkt naar controls en maatregelen.

5.3.1 *C.01 Naleving richtlijn netwerkbeveiliging en evaluaties*

Objectdefinitie

Toets op het nakomen van de richtlijn voor netwerkbeveiliging.

Objecttoelichting

Voor het beheer en de beveiliging van het netwerk zijn richtlijnen opgesteld. De naleving van deze richtlijnen moet worden bewaakt door periodieke evaluaties, waarbij ook het functioneren van de richtlijnen zelf onderwerp van beschouwing is.

Doelstelling	Het vaststellen of de richtlijnen voor de netwerkbeveiliging nog steeds worden nagevolgd en effectief zijn.		
Risico	Geen of onvoldoende inzicht of de richtlijnen voor netwerkbeveiliging effectief zijn.		
Control	De effectiviteit van de richtlijnen voor de netwerkbeveiliging behoort periodiek **getoetst en geëvalueerd** te worden.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Getoetst en geëvalueerd	1.	De naleving van de richtlijnen voor netwerkbeveiliging wordt periodiek getoetst en geëvalueerd door een audit met tenminste de volgende elementen: • netwerktopologie/-ontwerp met principes als ‘defence in depth’ en ‘inbraak betekent geen doorbraak’; • identificatie- en authenticatiemechanismen; • autorisatiemechanismen en een actuele administratie van de uitgegeven rechten; • actuele beleidsregels voor de netwerkbeveiliging; • aanwijzingen voor hardening van netwerkcomponenten; • verifieerbare auditlogoplossing.	ISO 27033-2 2012: 8.7

5.3.2 *C.02 Compliance-toets netwerkbeveiliging*

Objectdefinitie

Periodieke toetsing op de naleving van het beveiligingsbeleid voor netwerkdiensten.

Objecttoelichting

In de praktijk is het noodzakelijk gebleken om regelmatig te toetsen of de beoogde beveiliging van de netwerkvoorzieningen nog volgens het actuele beveiligingsbeleid functioneert. Het accent ligt hier op de naleving van het beleid. Periodiek dienen zowel de organisatorische als technische aspecten van de maatregelen, zoals: de taken en verantwoordelijkheden, de beschikbaarheid van voldoende technische middelen etc., beoordeeld te worden. Als resultaat dient hierover een rapportage van bevindingen aan het management te worden uitgebracht.

Doelstelling	Het vaststellen of de inrichting van netwerk(diensten) voldoet aan het beveiligingsbeleid.		
Risico	Afwijkingen op het beveiligingsbeleid worden niet gesignaleerd.		
Control	De **naleving** van een, volgens het beveiligingsbeleid, veilige **inrichting** van netwerk(diensten), behoort **periodiek** gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het **verantwoordelijke** management (compliancy-toetsen).		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Naleving	1.	De naleving van het netwerkbeveiligingsbeleid wordt periodiek getoetst en geëvalueerd door een audit met tenminste de volgende elementen: • netwerktopologie/-ontwerp met principes als 'defence in depth' en 'inbraak betekent geen doorbraak'; • identificatie- en authenticatiemechanismen; • autorisatiemechanismen en een actuele administratie van de uitgegeven rechten; • actuele beleidsregels voor de netwerkbeveiliging; • aanwijzingen voor hardening van netwerkcomponenten; • verifieerbare auditlogoplossing.	ISO 27033-2 2012: 8.7
Inrichting	2.	De controlelijst voor een veilige inrichting van netwerk(diensten) is samengesteld vanuit: • een actueel beveiligingsbeleid; • gerelateerde security operation-documentatie; • specifieke beveiligingsarchitectuur voor netwerk en communicatie(diensten); • het beleid voor toegang tot security gateway services; • bedrijfscontinuïteitsplannen; • relevante beveiligingscondities voor netwerkverbindingen.	CIP-netwerk
Periodiek	3.	Informatiesystemen worden periodiek gecontroleerd op de technische naleving van beveiligingsnormen en risico's op de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarhedenanalyses of penetratietesten.	ISO 27001:2022: 5.36, 8.8
Verantwoor-delijke	4.	De resultaten van de beoordelingen behoren te worden gerapporteerd aan het management dat de beoordelingen heeft geïnitieerd en, indien van toepassing, het topmanagement. Deze registraties behoren te worden bewaard.	ISO 27001:2022: 5.35

5.3.3 *C.03 Evalueren robuustheid netwerkbeveiliging*

Objectdefinitie

Beoordeling van de relatieve sterkte van beveiligingsfuncties in communicatievoorzieningen.

Objecttoelichting

Binnen de infrastructuur bevinden zich diverse netwerkvoorzieningen die het fundament vormen voor de gegevensuitwisseling. Het is noodzakelijk om regelmatig te toetsen of de robuustheid van de beveiliging van de netwerkvoorzieningen voldoet aan de gestelde eisen en proportioneel is ten opzichte

van de dreigingen. Periodiek dienen zowel de organisatorische als de technische aspecten van beveiligingsmaatregelen te worden beoordeeld en gerapporteerd aan het verantwoordelijke management.

Doelstelling	Het vaststellen of de beveiliging van het complete netwerk nog voldoet aan de gestelde eisen en in balans is met de dreigingen.		
Risico	Afwijkingen op de benodigde robuustheid van de beveiligingsmaatregelen worden niet gesignaleerd. De robuustheid is niet in evenwicht met de risico's/dreigingen.		
Control	De **robuustheid** van de beveiligingsmaatregelen en de naleving van het netwerkbeveiligingsbeleid behoren periodiek getest en aangetoond te worden.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Robuustheid	1.	De teststrategie voor netwerkbeveiliging is vastgelegd en geactualiseerd en bevat tenminste de volgende onderzoekselementen: • de robuustheid van het ontwerp met principes als 'defence in depth' en 'inbraak betekent geen doorbraak'; • de sterkte van Identificatie-, Authenticatie en Autorisatie (IAA)-mechanismen en de relevantie van uitgegeven rechten; • de juiste implementatie van de beleidsregels voor netwerkbeveiliging; • de verificatie van de hardening van netwerkcomponenten; • de verificatie van de auditlogoplossing; • de bruikbaarheid en functionele doelmatigheid van beveiligingsmaatregelen; • informatie over gebeurtenissen en incidenten, gerapporteerd door servicepersoneel en eindgebruikers.	CIP-netwerk

5.3.4 *C.04 Evalueren netwerkgebeurtenissen (monitoring)*

Objectdefinitie

Beoordeling van de (doorlopend) verzamelde beveiliging gerelateerde gebeurtenissen in netwerken.

Objecttoelichting

Het evalueren van de beveiligingsfuncties is cruciaal voor zekerheid over het bereiken van het beoogde beveiligingsniveau. Daarvoor moet het beheer van de beveiligingsfuncties worden vastgelegd in auditlogs en worden beoordeeld. De auditlogs dienen zodanig te worden ingericht dat netwerkbeheerders geen toegang kunnen hebben tot de vastgelegde beheerhandelingen.

Doelstelling	Het mogelijk maken van detectie en onderzoek van netwerkgebeurtenissen.
Risico	Na een gebeurtenis kan niet de benodigde actie worden ondernomen en niet worden vastgesteld wie welke handeling heeft uitgevoerd.

Control	Toereikende logging en monitoring behoren te zijn ingericht, om detectie, vastlegging en **onderzoek van gebeurtenissen** mogelijk te maken, die mogelijk van invloed op of relevant kunnen zijn voor de informatiebeveiliging.		ISO 27033-1 2015: 8.5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Onderzoek van gebeurte-nissen	1.	Zeer belangrijke onderdelen van netwerkbeveiliging zijn het: • via auditlogging en continue monitoring en gekoppeld aan detectie registreren van gebeurtenissen; • onderzoek uit te voeren en vervolgens; • snel reageren.	CIP-netwerk
	2.	Continue bewaking via monitoring legt de volgende informatie vast: • auditlogs vanuit de netwerkcomponenten: firewalls, router, servers etc.; • analyse-informatie vanuit Intrusion Detection Systems (IDS); • resultaten vanuit netwerkscanningsactiviteiten.	CIP-netwerk

5.3.5 *C.05 Beheersorganisatie netwerkbeveiliging*

Objectdefinitie

Doelgerichte bundeling van kennis en vaardigheden tussen personen met taken, verantwoordelijkheden en bevoegdheden voor het beheersen van en rapporteren over netwerken en communicatievoorzieningen.

Objecttoelichting

Het adequaat beheersen en beheren van de communicatievoorzieningen vereist een toereikende organisatiestructuur waarin de procesverantwoordelijkheden en de bevoegdheden van de functionarissen zijn vastgelegd en op het juiste niveau zijn gepositioneerd.

Doelstelling	Het invullen, coördineren en borgen van de beheersing van de netwerkbeveiliging.		
Risico	De beheerorganisatie voor netwerkbeveiliging is niet effectief ingericht waardoor de netwerkbeveiliging niet optimaal functioneert.		
Control	Alle **verantwoordelijkheden** bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.		ISO 27002:2022: 5.2 BIO2: 5.02.01
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verantwoordel ijkheden	1.	De communicatievoorzieningen worden geïdentificeerd en gedefinieerd.	CIP-netwerk

	2.	Beheerderstaken vereisen in sommige gevallen vergaande bevoegdheden met risico's voor de doelorganisatie. Het beleggen van de juiste verantwoordelijkheden en het toezien op het beoogde gebruik daarvan vergt extra aandacht. De volgende onderwerpen zijn daarbij van belang: • De entiteit die verantwoordelijk is voor de communicatievoorzieningen wordt bepaald en de taken die voortvloeien uit die verantwoordelijkheid zijn actueel, vastgelegd en bekend. • De rollen en (speciale) bevoegdheden van netwerkbeheerders zijn gedefinieerd en gedocumenteerd. • De netwerkbeheerders zijn en blijven goed opgeleid en competent voor de uitvoering van hun taken. • De coördinatie en het overzicht van informatiebeveiligingsaspecten van dienstverleners is geïdentificeerd, gedocumenteerd en wordt continu gemonitord.	ISO 27002:2022: 5.2