Communicatievoorzieningen

BIO Thema-uitwerking

Februari 2021 [versie 2.0 definitief]

BIO Thema-uitwerking Communicatievoorzieningen

Titel	BIO Thema-uitwerking Communicatievoorzieningen
Datum	Februari 2021
Versie	2.0 definitief
Opdrachtgever	Voorzitter werkgroep BIO en directeur CIP
Regime	Becommentarieerde praktijk
Auteurs	Wiekram Tewarie (UWV/CIP) en Jaap van der Veen (CIP)
Reviewers	Versie 1.0: Jan Breeman (UWV), Paul Coret (Hoogheemraadschap Delfland), Peter van Dijk (VNG/IBD), Joop Hagman (Veiligheidsregio Noord-Holland Noord), Peter Kruger (Justitiële Informatiedienst) en René Reith (Provincie Zuid-Holland) Versie 2.0: CIP-kernteam

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Leeswijzer

Voorafgaand aan hoofdstuk 2 Beleidsdomein, 3 Uitvoeringsdomein en 4 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

Dit document bevat een referentiekader voor het thema Communicatievoorzieningen. Het is geënt op controls uit de Baseline Informatiebeveiliging Overheid (BIO) 2019, NEN-ISO/IEC 27002: 2017 (hierna genoemd ISO 27002), implementatiestandaarden-reeks ISO 27033 en tevens op best practices als: Bundesamt für Sicherheit in der Informationstechnik (BSI) en Standard of Good Practice (SoGP).

1.1 Opzet van het thema

Het thema Communicatievoorzieningen brengt de voor communicatiebeveiliging relevante controls uit de BIO overzichtelijk bij elkaar. Vervolgens zijn relevante items die ontbraken, aangevuld uit andere baselines, zoals de BSI en SoGP. 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 biedt, gerelateerd aan de ISO 27002, overzicht en een technische duiding van netwerkbeveiliging.

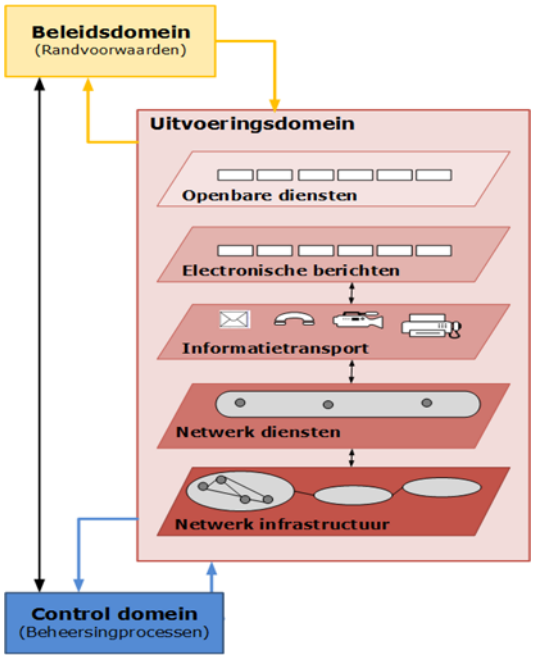
Dit thema volgt de standaardopzet voor BIO Thema-uitwerkingen:

1. Context en globale structuur van het thema (§1.2);
2. Scope en begrenzing van het thema (§1.3);
3. Globale relaties tussen de geïdentificeerde beveiligingsobjecten (§1.4);

1.2 Context van communicatievoorzieningen

De basis voor de uitwerking van het thema Communicatievoorzieningen is de BIO. In hoofdstuk 13 van de BIO worden verschillende type 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).

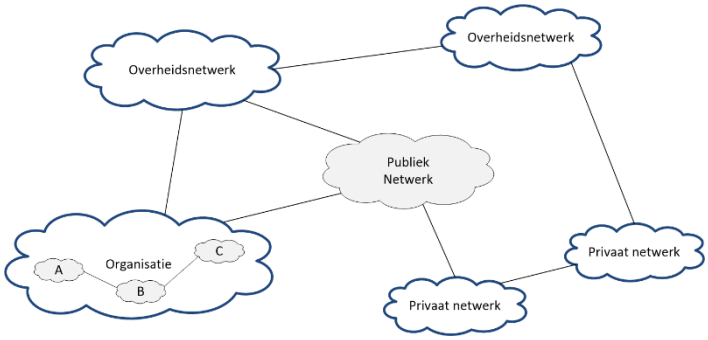


Afbeelding 1: Schematische weergave context communicatievoorzieningen

Iedere organisatie met klantprocessen past deze communicatievoorzieningen toe en heeft een of meer koppelingen met de buitenwereld ingericht. Deze communicatie verloopt altijd via het onderste element: de netwerkinfrastructuur. Het gebruik van netwerkvoorzieningen vindt plaats zowel mobiel als via vaste netwerkvoorzieningen.

In de praktijk bestaan er veel verschillende soorten koppelingen en een verscheidenheid aan netwerkvoorzieningen. Onderstaande afbeelding schetst de belangrijkste soorten van netwerkkoppelingen:

- Tussen organisaties onderling
- Tussen organisaties en publieke netwerken
- Binnen organisaties



Afbeelding 2: Soorten netwerkkoppelingen

Het doel van een netwerk is de uitwisseling van data tussen informatiedomeinen. Een informatiedomein bestaat uit een op hard- en softwarematige gebaseerde beveiligde verzameling van informatie.

De beveiligingsmaatregelen binnen de ISO-standaard hebben betrekking op de hiervoor vermelde communicatievoorzieningen. Een van de meest toegepaste beveiligingsmaatregelen van de netwerkinfrastructuur is segmentering en compartimentering, tezamen zonering genoemd.

Naast zonering zijn er andere beveiligingsobjecten van toepassing, zoals: 'vertrouwd toegangspad' en beveiliging in 'koppelvlakken'. Hiervoor bieden de NORA-patronen een praktische invulling.

In dit thema wordt een netwerk beschouwd als een infrastructuur (transportmedium), bestaande uit fysieke en logische verbindingen voorzien van koppelvlakken. Netwerken kunnen daarbij worden opgedeeld in segmenten, waarbij meerdere systemen logisch met elkaar gekoppeld zijn binnen één segment.

1.3 Scope en begrenzing

Dit thema omvat een set communicatie-beveiligingsobjecten en -maatregelen voor netwerkvoorzieningen[1], zoals weergegeven in afbeelding 1. De uitwerking van dit thema beperkt zich tot deze type communicatievoorzieningen.

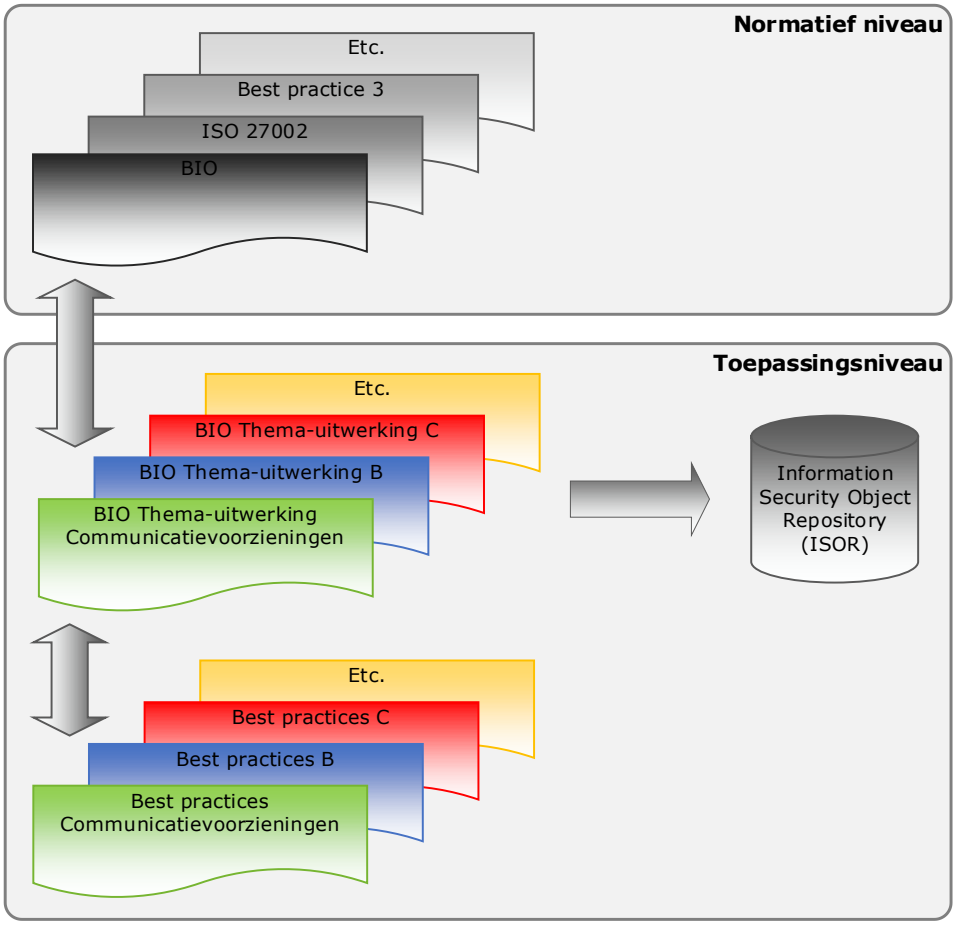
Er zijn essentiële objecten uit andere best practices dan de BIO gebruikt, die gerelateerd zijn aan dit type communicatievoorzieningen. Bepaalde type communicatiefaciliteiten, zoals: Voice over IP (VOIP), intranet en extranet zijn in dit thema niet uitgewerkt. Er wordt niet diepgaand ingegaan op:

- bepaalde type verbindingen, zoals Virtual Private Network (VPN)- en gateway-verbindingen;
- communicatievoorzieningen, zoals instant messaging en e-mail.

De begrenzing van dit document is in onderstaande afbeelding weergegeven.

[1] Hiervoor zijn de ISO-standaarden: ISO 27033 1 t/m 6 en NORA-patronen in adviserende zin beschikbaar.

De ISO 27033 draagt de titel: Information technology - Security techniques - Network security, bedoeld als implementatiegids voor de ISO 27002. De ISO 27033 bestaat uit 6 delen. Deel 1 bevat algemene controls voor communicatiebeveiliging, deel 2 beschrijft ontwerprichtlijnen voor de uitvoering, deel 3 referentiescenario's, deel 4 gateways, deel 5 VPN en deel 6 Wireless-IP netwerktoegang.



Afbeelding 3: Relatie BIO Thema-uitwerking met aanpalende documenten

1.4 Globale relaties tussen de beveiligingsobjecten

Onderstaande afbeelding 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.

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

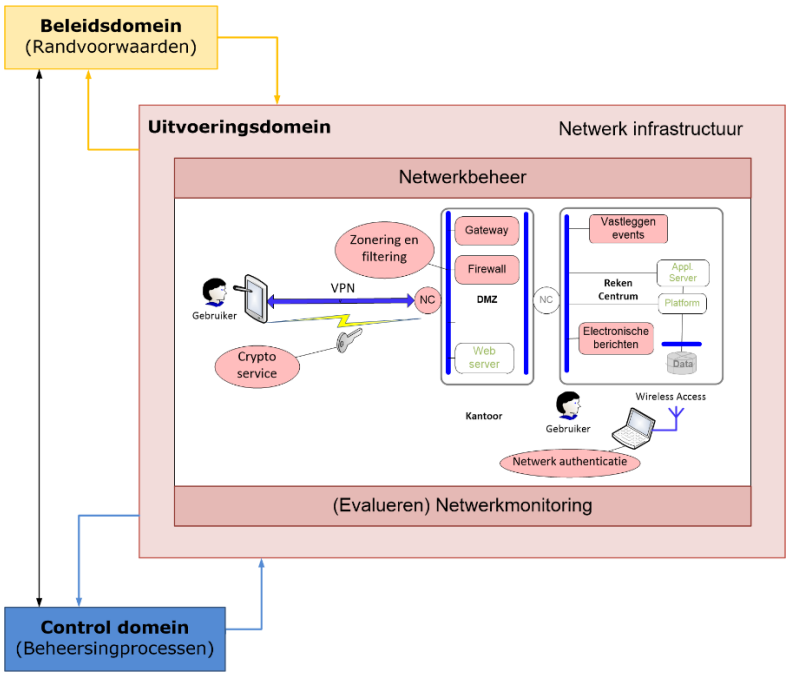
Gateways en firewalls zorgen met zonering en filtering voor de beoogde scheiding van de binnen- en buitenwereld en een gecontroleerde doorgang van vertrouwde informatie.

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 worden beveiligd met onder andere netwerkauthenticatie.

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

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



Afbeelding 4: Toepassing van beveiligingsobjecten

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

2 Beleidsdomein

2.1 Doelstelling

Dit domein beschrijft BIO-normatieve eisen voor beleid, die randvoorwaardelijk en bedoeld zijn voor de realisatie en operatie van communicatievoorzieningen.

2.2 Risico's

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

2.3 Objecten, controls en maatregelen

Onderstaande afbeelding is het resultaat van de SIVA-analyse op relevante objecten voor het informatievoorzieningsbeleid. SIVA staat voor Structuur, Inhoud, Vorm en Analysevolgorde. Het wit ingekleurde object ontbreekt als control in de BIO maar is wel cruciaal voor dit thema.

Afbeelding 5 geeft een overzicht en de ordening van objecten. Voor de identificatie van de objecten en de ordening is gebruik gemaakt van basiselementen (zie de grijs gemarkeerde tekst) ingedeeld naar de invalshoek: Intentie, Functie, Gedrag of Structuur).

Afbeelding 5: Overzicht communicatievoorzieningenobjecten in het beleidsdomein

2.3.1 B.01 Beleid en procedures informatietransport

Definitie

De waarborging van de bescherming van informatie in netwerken, door inzet van beheerprocedures voor informatietransport en het hanteren van procedures voor het bewaking van netwerken.

Toelichting

De ISO 27002 2017: 14.2.1 formuleert 'Beveiligd ontwikkelen' als een eis voor het opbouwen van een beveiligde dienstverlening, architectuur, software en beveiligd systeem. Dit object richt zich op inrichtings- en onderhoudsaspecten van communicatievoorzieningen. In het te formuleren beleid worden onder andere standaarden en procedures beschreven voor het beveiligd inrichten en onderhouden van communicatievoorzieningen.

Doelstelling	Het beheersen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tijdens transport in netwerken.		
Risico	Onvoldoende mogelijkheden om sturing te geven aan informatietransport en sturing te geven aan inconsistenties in het uitvoeren van procedures en beheersmaatregelen over informatietransport.		
Control	Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele **beleidsregels**, **procedures** en **beheersmaatregelen** voor transport van kracht te zijn.		BIO 2019: 13.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beleidsregels	1.	Het beleid of de richtlijnen omschrijven het aanvaardbaar gebruik van communicatiefaciliteiten.	ISO 27002 2017: 13.2.1d
	2.	Het beleid of de richtlijnen omschrijven het toepassen van cryptografie voor de bescherming van de vertrouwelijkheid, integriteit en authenticiteit van informatie.	ISO 27002 2017: 13.2.1f
	3.	Het beleid of de richtlijnen omschrijven welk type verkeer niet over draadloze netwerken verstuurd mag worden.	CIP
Procedures	4.	De procedures beschrijven het beveiligen van informatie tegen onderscheppen, kopiëren, wijzigen, foutieve routering en vernietiging.	ISO 27002 2017: 13.2.1a
	5.	De procedures beschrijven het opsporen van en beschermen tegen malware die kan worden overgebracht met elektronische communicatie (zie paragraaf 12.2.1 van de ISO 27002 2017).	ISO 27002 2017: 13.2.1b
	6.	De procedures beschrijven het beschermen van als bijlage gecommuniceerde gevoelige informatie.	ISO 27002 2017: 13.2.1c
Beheers-maatregelen	7.	E-mailberichten worden met vastgelegde procedures en richtlijnen veilig en geautomatiseerd doorgestuurd.	ISO 27002 2017: 13.2.1h

2.3.2 B.02 Overeenkomsten informatietransport

Definitie

De contracten en afspraken waarin het dienstverleningsniveau, de beveiligingsmechanismen en de beheersingseisen voor netwerkdiensten zijn vastgelegd, zowel voor intern geleverde diensten als voor uitbestede diensten.

Toelichting

Bij het gebruik van communicatievoorzieningen behoren beveiligingsprincipes in acht te worden genomen. In de BIO 2019-control 13.2.2 wordt één principe expliciet genoemd: 'Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.'. Andere baselines (zoals de SoGP) beschrijven nog verschillende andere relevante inrichtingsprincipes.

Doelstelling	Vastgelegde en nagekomen SMART-afspraken over het gewenste beveiligingsniveau voor informatietransport over netwerken.

Risico	Niet helder is welke partij verantwoordelijk gesteld kan worden bij het niet halen van het gewenste beveiligingsniveau voor het transporteren van informatie over netwerken.		
Control	**Overeenkomsten** behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.		BIO 2019: 13.2.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Overeen-komsten	1.	Overeenkomsten over informatietransport bevatten onder andere de volgende elementen: • directieverantwoordelijkheden voor het beheersen en notificeren van overdracht, verzending en ontvangst; • procedures voor het waarborgen van de traceerbaarheid en onweerlegbaarheid; • speciale en vereiste beheersmaatregelen voor het beschermen van gevoelige informatie, zoals cryptografie; • het handhaven van een bewakingsketen voor informatie tijdens de verzending; • acceptabele niveaus van toegangsbeveiliging.	ISO 27002 2017: 13.2.2a, b, i, j en k
	2.	In de overeenkomst behoren alle betrokken partijen expliciet genoemd te zijn.	CIP

2.3.3 B.03 Cryptografiebeleid voor communicatie

Definitie

Het beleid en de afspraken specifiek gericht op de toepassing van cryptografie binnen netwerken en communicatieservices.

Toelichting

In de ISO 27002 2017 worden voor communicatievoorzieningen de volgende principes expliciet genoemd:

- het, met inbegrip van methoden voor het beveiligen van de toegang op afstand, beschikbaar stellen van passende communicatievoorzieningen;
- tijdens hun gehele levenscyclus dient beleid te worden ontwikkeld en geïmplementeerd ter bescherming van informatie en voor de bescherming, het gebruik en de levensduur van cryptografische beheersmaatregelen (zoals cryptosleutels).

Doelstelling	Het beheersen van cryptografie binnen netwerken en communicatieservices.	
Risico	Onvoldoende mogelijkheid om sturing te geven aan de effectieve en betrouwbare inrichting van cryptografische beheersmaatregelen binnen netwerken en communicatieservices.	
Control	Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Cryptografie-beleid	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 wordt vastgesteld. • Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	BIO 2019: 10.1.1.1
	2.	Aanvullend bevat het cryptografiebeleid voor communicatieservices het volgende: • Welk type gegevens moet voor welke communicatievorm worden versleuteld. • Welk type 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

2.3.4 B.04 Organisatiestructuur netwerkbeheer

Definitie

De opzet van de administratieve organisatie van het netwerk- en communicatiebeheer.

Toelichting

In de ISO 27002 2017 worden geen organisatorische principes genoemd voor communicatievoorzieningen. De Duitse BSI benoemt daarvoor meerdere principes, die aangeven dat in het beleid is vastgesteld, 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
	3.	De taken en verantwoordelijkheden van de verantwoordelijke functionarissen voor deze processen zijn duidelijk gedefinieerd.	CIP

3 Uitvoeringsdomein

3.1 Doelstelling

Het doel van het uitvoeringsdomein is te waarborgen dat de netwerkinfrastructuur is ingericht conform specifieke beleidsuitgangspunten en dat aan de eisen ten aanzien van de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid bij het ontwerp en implementatie is voldaan.

3.2 Risico's

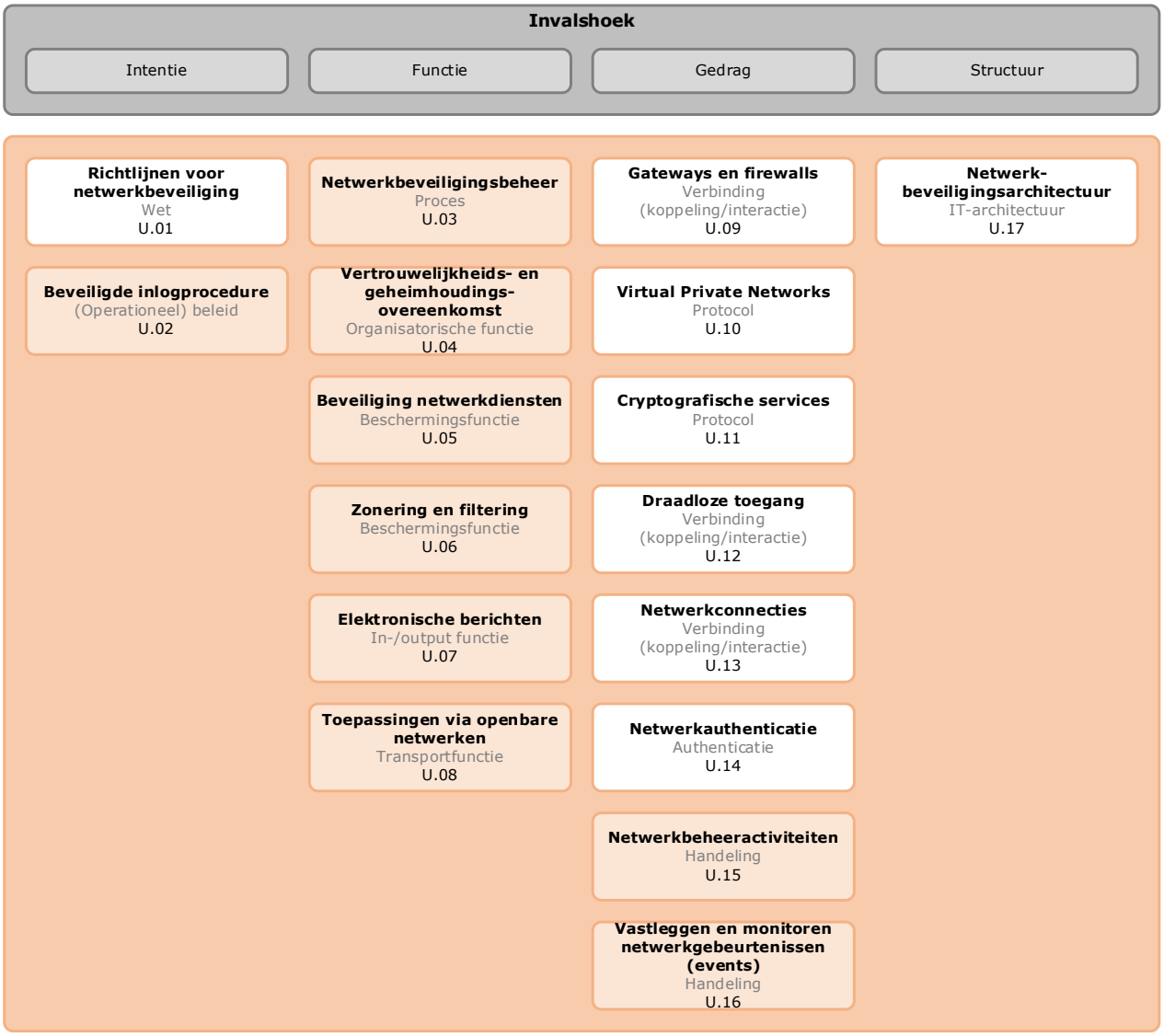
De belangrijkste risico's van netwerk(diensten) zijn:

- 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.

3.3 Objecten, controls en maatregelen

Per object zijn hierna de maatregelen uitgewerkt die risico's kunnen reduceren. Voor de implementatie wordt verwezen naar de zes uitvoeringskaders van de ISO 27033 en het NORA-thema Beveiliging.

In de onderstaande afbeelding zijn de essentiële objecten voor communicatievoorzieningen weergegeven in de kolommen: Intentie, Functie, Gedrag en Structuur. Voor de wit ingekleurde objecten heeft de BIO geen control gedefinieerd. Deze objecten zijn voor een groot deel afkomstig uit de ISO 27033 deel 1 t/m 6.



Afbeelding 6: Overzicht communicatievoorzieningenobjecten in het uitvoeringsdomein

3.3.1 U.01 Richtlijnen voor netwerkbeveiliging

Definitie

De algemene operationele beveiligingsrichtlijnen voor het ontwerp, de implementatie en het beheer van communicatievoorzieningen.

Toelichting

De ISO 27002 2017 beschrijft geen operationele principes voor communicatievoorzieningen, maar verwijst hiervoor naar de ISO 27033 (deel 1 t/m 6). Enkele principes zijn in de ISO 27002 expliciet genoemd, onder andere dat de bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten (voortdurend) dienen te worden gewaarborgd.

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

3.3.2 U.02 Beveiligde inlogprocedure

Definitie

De inlogprocedure is gerelateerd aan de aspecten aanmelden en procedure.

1. Aanmelden (inloggen) behelst het leggen van een verbinding via authenticatiemiddelen.
2. De procedure is de samenhangende beschrijving van welke activiteiten moeten plaatsvinden.

Toelichting

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

[2] Voorbeeld: ISO 27033 deel 2.

Doelstelling	Onbevoegde toegang tot (communicatie)systemen en toepassingen voorkomen.		
Risico	Misbruik en verlies van gevoelige gegevens en beïnvloeding van beschikbaarheid van (communicatie)systemen.		
Control	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde **inlogprocedure**.		BIO 2019: 9.4.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Inlogproce-dure	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.	BIO 2019: 9.4.2.2
	2.	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	BIO 2019: 9.4.2.1
	3.	Toegang tot netwerken is beperkt tot geautoriseerde gebruikers (en geautoriseerde applicaties). Drie gebieden waarvoor expliciete inlogmechanismen worden toegepast, zijn: 1. Remote login Voor gebruikers die van buiten inloggen op de door de organisatie beheerde bedrijfsnetwerken. 2. Versterkte authenticatie Voor toepassingen waarbij de 'standaard'-authenticatie van gebruikers (en applicaties) kan worden gecompromitteerd. 3. Single Sign-On Voor situaties waarbij netwerken worden geacht authenticatie-checks uit te voeren voor verschillende toepassingen.	CIP

3.3.3 U.03 Netwerkbeveiligingsbeheer

Definitie

Het beheer van beveiligingsprocedures en -mechanismen.

Toelichting

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

Doelstelling	Het bereiken van de netwerkbeveiligingsdoelen en de netwerkbeveiliging behouden in de gewenste/een bruikbare staat.
Risico	Informatie in netwerken is niet beschermd.

Control	Netwerken behoren te worden **beheerd** en **beheerst** om informatie in systemen en toepassingen te beschermen.		BIO 2019: 13.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beheerd	1.	Voor het beheer van netwerkapparatuur zijn verantwoordelijkheden en procedures vastgesteld.	ISO 27002 2017: 13.1.1a
	2.	Netwerken worden geregistreerd en gemonitord conform vastgelegde procedures en richtlijnen.	ISO 27002 2017: 13.1.1d
	3.	Beheeractiviteiten worden nauwgezet gecoördineerd, zowel om de dienstverlening voor de organisatie te optimaliseren als om te waarborgen dat beheersmaatregelen consistent in de hele informatieverwerkende infrastructuur worden toegepast.	ISO 27002 2017: 13.1.1e
	4.	Ter bescherming tot netwerkdiensten en/of - voor zover noodzakelijk - van toepassingen zijn voor het beperken van de toegang procedures opgesteld.	CIP
Beheerst	5.	De functies van operationeel netwerkbeheer en overige computerbewerkingen zijn gescheiden.	ISO 27002 2017: 13.1.1b
	6.	Systemen worden voorafgaand aan de toegang tot het netwerk geauthentiseerd.	ISO 27002 2017: 13.1.1f

3.3.4 U.04 Vertrouwelijkheids- en geheimhoudingsovereenkomst

Definitie

De eisen die aan dienstverleners en partners gesteld worden in de operatie voor het waarborgen van de vertrouwelijkheid en geheimhouding van gegevens en de uitvoering van bedrijfsprocessen.

Toelichting

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 waaraan dienstverleners en partners worden blootgesteld.	
Risico	Dienstverleners en partners zijn niet (voldoende) bekend met de actuele benodigde eisen van de organisatie voor het beschermen van informatie.	
Control	Eisen voor **vertrouwelijkheids- of geheimhoudingsovereenkomsten** die de behoeften van de organisatie, betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	BIO 2019: 13.2.4
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Vertrouwelijkheids- of geheimhoudingsovereenkomsten	1.	Voor de vertrouwelijkheids- of geheimhoudingsovereenkomsten worden de volgende elementen in overweging genomen: • de looptijd van een overeenkomst; • de benodigde acties bij beëindiging; • de acties van ondertekenaars bij onbevoegde openbaarmaking van informatie; • hoe het eigendom van vertrouwelijke informatie zich verhoudt tot de bescherming; • het toegelaten gebruik van vertrouwelijke informatie en de rechten van de ondertekenaar om informatie te gebruiken; • de voorwaarden voor het teruggeven of vernietigen van informatie na beëindiging; • de acties in geval van schending van de overeenkomst; • de privacyregelgeving (Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)).	ISO 27002 2017: 13.2.4b, c, h, e, f, i en j

3.3.5 U.05 Beveiliging netwerkdiensten

Definitie

De eisen die aan dienstverleners gesteld worden voor de te nemen maatregelen voor de beveiligingsmechanismen, het dienstverleningsniveau en de kwaliteit van beheerprocessen.

Toelichting

De eisen 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	Bij uitval van netwerkdiensten kan de continuïteit van de bedrijfsvoering optimaal gecontinueerd worden; een contante beschikbaarheid en continuïteit garanderen.		
Risico	Uitval van kritische processen van de organisatie.		
Control	**Beveiligingsmechanismen**, **dienstverleningsniveaus** en **beheereisen** voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.		BIO 2019: 13.1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-mechanismen	1.	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het Nationaal Bureau Verbindingsveiligheid (NBV) een positief inzetadvies heeft afgegeven.	BIO 2019: 13.1.2.3
	2.	De noodzakelijke beveiligingsmechanismen in de vorm van technische beveiligingsfuncties, zoals segmentatie, detectie en protectie, monitoring en versleuteling van het dataverkeer zijn vastgelegd in een overeenkomst.	ISO 27002 2017: 13.1.2

	3.	Beveiligingsmechanismen voor communicatie worden voorzien op de volgende Open Systems Interconnection (OSI)-lagen: • Applicatieniveau Voor authenticiteit, integriteit, vertrouwelijkheid en onweerlegbaarheid: encryptie. • Transportniveau Voor veilige point to point-verbindingen: encryptie. • Netwerkniveau Voor veilige communicatie tussen devices, encryptie, firewalls en netwerkverbindingen: VPN.	CIP
Dienstverle-ningsniveaus	4.	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
Beheereisen	5.	Het dataverkeer dat de organisatie binnenkomt of uitgaat, wordt bewaakt/geanalyseerd op kwaadaardige elementen middels detectie-voorzieningen (zoals beschreven in de richtlijn voor implementatie van detectie-oplossingen), zoals het Nationaal Detectie Netwerk of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	BIO 2019: 13.1.2.1
	6.	Bij ontdekte nieuwe dreigingen vanuit de analyse op kwaadaardige elementen worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het Nationaal Cybersecurity Centrum (NCSC) of de sectorale Computer Emergency Response Team (CERT), bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	BIO 2019: 13.1.2.2

3.3.6 U.06 Zonering en filtering

Definitie

Dit object gaat over de aspecten scheiding en gecontroleerde doorgang:

1. Scheiding is het positioneren van netwerken in afzonderlijke fysieke ruimten of het segmenteren van netwerken in afzonderlijk te beveiligen (logische) domeinen.
2. Gecontroleerde doorgang is het reguleren van de toegang van personen tot netwerkvoorzieningen en/of het en filteren van informatiestromen met beleidsregels met filters en algoritmen.

Toelichting

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 die communicatie doorlaat, die vanuit het beleid is

toegestaan en waarmee ongeoorloofde toegang wordt voorkomen. De scheiding met gecontroleerde doorgangen heet 'zonering'.

Doelstelling	Veilig communiceren vanuit het ene naar het andere netwerk.		
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)**.		BIO 2019: 13.1.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gescheiden (in domeinen)	1.	Het netwerk is in (logische of fysieke) domeinen (of zones) opgedeeld op grond van risico's voor onderlinge negatieve beïnvloeding van informatiesystemen binnen een domein en het beoogde betrouwbaarheidsniveau.	CIP
	2.	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	BIO 2019: 13.1.3.1
	3.	Perimeters van netwerkzones worden nauwkeurig gedefinieerd en de gecontroleerde doorgang van de informatie tussen netwerkdomeinen wordt beheerst met een gateway (bijvoorbeeld een firewall en een filterende router).	ISO 27002 2017: 13.1.3
	4.	Draadloze toegang tot gevoelige domeinen wordt behandeld als een externe verbinding en wordt beveiligd met de eisen geldend voor externe verbindingen.	ISO 27002 2017: 13.1.3

3.3.7 U.07 Elektronische berichten

Definitie

De beveiliging van het elektronisch berichtenverkeer, bijvoorbeeld e-mail, web-verkeer, chatsessies en 'streaming' van audio en video. Beveiliging omvat maatregelen voor de bescherming van het berichtenverkeer zoals geautoriseerde toegang, correcte adressering en integer datatransport, beschikbaarheid en (wettelijke) bepalingen voor elektronische handtekening en onweerlegbaarheid.

Toelichting

Beveiliging van elektronisch berichtenverkeer omvat e-mail, web-verkeer, 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	Elektronisch berichtenverkeer blijft beschikbaar, integer en vertrouwelijk.

Risico	Aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie in elektronisch berichtenverkeer.		
Control	Informatie die is opgenomen in elektronische berichten behoort **passend** te zijn beschermd.		BIO 2019: 13.2.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Passend	1.	Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen phishing en afluisteren van de 'pas- toe-of-leg-uit'-lijst van het Forum Standaardisatie.	BIO 2019: 13.2.3.1
	2.	Voor veilige berichtenuitwisseling met basisregistraties wordt, conform de 'pas-toe-of-leg-uit-lijst van het Forum Standaardisatie, gebruik gemaakt van de actuele versie van Digikoppeling.	BIO 2019: 13.2.3.2
	3.	Bij web- en mailverkeer van gevoelige gegevens wordt gebruik gemaakt van PKI-Overheid-certificaten. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	BIO 2019: 13.2.3.3
	4.	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard of de ETSI TS 102 176-1 (en relevante standaarden uit de pas-toe-of-leg-uit lijst van het Forum Standaardisatie).	BIO 2019: 13.2.3.4
	5.	Voor de beveiliging van het elektronische berichtenverkeer worden passende maatregelen getroffen, zoals: • de berichten te beschermen tegen onbevoegde toegang, wijziging of weigering van dienstverlening met het classificatieschema van de organisatie; • een correcte adressering en het transport van het bericht waarborgen; • de herstelbaarheid van onderbroken communicatie en de beschikbaarheid van de dienst; • de wettelijke bepalingen zoals eisen voor elektronische handtekeningen; • het toestemming verkrijgen van het verantwoordelijke management en de gegevenseigenaren, voorafgaand aan het gebruiken van externe openbare diensten zoals instant messaging, sociale netwerken of het delen van bestanden; • de 2-factorauthenticatie voor de toegang vanuit de openbaar toegankelijke netwerken.	ISO 27002 2017: 13.2.3a t/m f

3.3.8 U.08 Toepassingen via openbare netwerken

Definitie

Het gebruik van openbare netwerken voor de uitwisseling van informatie van uitvoeringsdiensten vereist bescherming tegen inbraak waarmee frauduleuze praktijken, geschillen over contracten en onbevoegde openbaarmaking of onbevoegde wijziging kan worden voorkomen.

Toelichting

Het via openbare netwerken, zoals het internet, beschikbaar stellen van ICT-toepassingen vereist aanvullende maatregelen ten opzichte van het beschikbaar stellen via besloten netwerken, zoals LAN's en het intranet. Organisaties bepalen zelf welke maatregelen toereikend zijn voor het beperken van risico's als gevolg van frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging of verminking van gegevens.

Doelstelling	Het effectief beveiligen van het netwerkverkeer via openbare netwerken.		
Risico	Frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.		
Control	Informatie die deel uitmaakt van uitvoeringsdiensten en die via **openbare netwerken** wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.		BIO 2019: 14.1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Openbare netwerken	1.	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

3.3.9 U.09 Gateways en firewalls

Definitie

Een beveiligingsmechanisme voor zonering en gecontroleerde toegang.

Toelichting

Gateways en firewalls realiseren de maatregelen voor zowel zonering als voor filtering en zijn niet expliciet genormeerd in de ISO 27002 2017. 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	Ongeautoriseerd inkomend en uitgaand dataverkeer te detecteren en blokkeren.	
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 filterfunctie 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 Security Information and Event Management (SIEM).	CIP
Toegestaan	4.	Uitsluitend toegestaan netwerkverkeer wordt doorgelaten.	CIP

3.3.10 U.10 Virtual Private Networks

Definitie

Een beveiligingsmechanisme voor het inrichten van een vertrouwd toegangspad tussen twee of meerdere netwerk-nodes.

Toelichting

Een VPN is een zoneringsmaatregel die een strikte scheiding van netwerkconnecties met andere netwerken mogelijk maakt tussen zowel publieke als private netwerken. Een VPN is niet expliciet genormeerd in de ISO 27002 2017. De ISO 27033-5 2013 is een implementatiestandaard voor 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 die over een VPN wordt getransporteerd, is ingeperkt 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

3.3.11 U.11 Cryptografische services

Definitie

De versleuteling van het netwerkverkeer, met hardware- of softwarevoorzieningen, die op alle zeven lagen van het OSI-model kunnen voorkomen. 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.

Toelichting

De ISO 27002 2017 normeert het beleid voor cryptografie en sleutelbeheer.

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.

De 'pas-toe-en-leg-uit'-lijst van het Forum Standaardisatie benoemt passende beheersmaatregelen.

Doelstelling	Het behouden van de vertrouwelijkheid en integriteit van de getransporteerde informatie.		
Risico	Het aanpassen van de vertrouwelijkheid en de integriteit van getransporteerde informatie door onbevoegden.		
Control	Ter bescherming van de **vertrouwelijkheid** en **integriteit** van de getransporteerde informatie behoren passende **cryptografische beheersmaatregelen** te worden ontwikkeld, geïmplementeerd en ingezet.		ISO 27033-1 2015: 7.2.2.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Vertrouwelijk-heid	1.	Voor het waarborgen van de vertrouwelijkheid van 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.	Voor het waarborgen van 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 ontvangen data.	ISO 27033-1 2015: 8.8
Cryptogra-fische	3.	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas-toe-of-leg-uit'-lijst van het Forum Standaardisatie.	BIO 2019: 18.1.5.1
Beheers-maatregelen	4.	Cryptografische algoritmen voldoen aan de hoogst mogelijke industrie-standaarden, voor de sterkte, met een voor de toepassing en contextrelevante sleutellengte en algoritme, zoals uit de Forum Standaardisatie-lijst: • Advanced Encryption Standard (AES); • sleutellengte 128 bit voor 'lichte' en 192 of 256 bits voor 'zware' toepassingen.	CIP

3.3.12 U.12 Draadloze toegang

Definitie

De toegang tot draadloze netwerken bedoeld voor mobiele communicatie.

Toelichting

Draadloze toegang (wireless access) is niet expliciet genormeerd in de ISO 27002 2017. De implementatiestandaard ISO 27033-6 2016 beschrijft de operationele maatregelen voor de relatief kwetsbare draadloze netwerken.

Doelstelling	Het zorgen dat onbevoegden geen gebruik kunnen maken van devices waartoe ze niet gemachtigd zijn en dat het draadloze verkeer beschikbaar, integer en vertrouwelijk blijft.		
Risico	Draadloos verkeer 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
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) beschermt netwerken tegen aansluiting van ongeautoriseerde gebruikers. • Integriteitcontrolemechanismen voorkomen 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

3.3.13 U.13 Netwerkconnecties

Definitie

De verbindingen netwerkeindpunten (nodes) worden beheerd en zijn vastgelegd in een netwerktopologie.

Toelichting

Netwerkconnecties zijn niet expliciet genormeerd in de ISO 27002 2017. 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	Bij beheer, storingen en calamiteiten weet de organisatie wat er aan gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk aanwezig is. De uitval wordt geminimaliseerd.		
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
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verbindingen	1.	Voor de beheersing van netwerken worden de volgende minimumeisen toegepast: • 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

3.3.14 U.14 Netwerkauthenticatie

Definitie

Een voorziening die controleert of een netwerkdevice geautoriseerd is om op het netwerk te worden aangesloten.

Toelichting

Netwerkauthenticatie is niet expliciet genormeerd in de ISO 27002 2017. Inherent aan het protocol IEE 801.x dient, om het onbevoegd aansluiten van netwerkdevices te voorkomen, authenticatie van netwerk-nodes te worden toegepast. Sniffing, ofwel afluisteren, is één van de vormen van onbevoegde toegang.

Doelstelling	Dat alleen vooraf toegestane netwerkdevices op het netwerk worden toegelaten.	
Risico	Ongeautoriseerde netwerkdevices worden aangesloten op het netwerk.	
Control	**Authenticatie van netwerk-nodes** behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.	CIP
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Authenticatie van netwerk-nodes	1.	Alvorens logisch toegang te verkrijgen tot een netwerk, wordt de authenticiteit van een aangesloten netwerk-device gecontroleerd (EAP-TLS).	CIP
	2.	Alleen de specifiek voor het netwerk toegestane netwerk-devices worden logisch gekoppeld met de in het netwerk aanwezige clients en informatiesystemen (IEE 802.1x).	CIP

3.3.15 U.15 Netwerkbeheeractiviteiten

Definitie

De activiteiten die uitsluitend door netwerkbeheerders kunnen worden uitgevoerd op communicatievoorzieningen.

Toelichting

Netwerkbeheer is een randvoorwaarde voor informatiebeveiliging. Beheeractiviteiten behoren nauwgezet te worden gecoördineerd, zowel voor een optimale dienstverlening als om te waarborgen dat de beheersmaatregelen consistent worden toegepast binnen de gehele informatieverwerkende infrastructuur.

Doelstelling	Het bereiken van de netwerkbeveiligingsdoelen en de netwerkbeveiliging behouden in de gewenste/een buikbare staat.	
Risico	Informatie in netwerken is niet beschermd.	
Control	Netwerken behoren te worden **beheerd** en **beheerst** om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1
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. In het bijzonder 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 patching van netwerkbekabeling in netwerkverdeelkasten.	CIP

3.3.16 U.16 Vastleggen en monitoren netwerkgebeurtenissen (events)

Definitie

Het uniek en onveranderlijk vastleggen van (beveiligings)gebeurtenissen in een netwerk (in een auditlogfile) en het controleren van deze vastleggingen.

Toelichting

Op communicatievoorzieningen vinden geautomatiseerde en handmatige activiteiten en zowel gewenste als ongewenste gebeurtenissen plaats. Informatiebeveiliging impliceert dat deze events worden gemonitord, de ernst daarvan wordt beoordeeld en dat de risico's worden vastgelegd. Met deze registratie kunnen situaties worden hersteld en kan van voorvallen worden geleerd zodat schade in de toekomst mogelijk wordt voorkomen. 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 achteraf kunnen vaststellen of de beveiliging van het netwerk niet is verstoord en bij verstoring kan de situatie hersteld worden.		
Risico	Het niet kunnen achterhalen van de oorzaak van beveiligingsinbreuken.		
Control	Logbestanden van informatiebeveiligingsgebeurtenissen in netwerken, behoren te worden **gemaakt en bewaard** en regelmatig te worden **beoordeeld** (op de ernst van de risico's).		BIO 2019: 12.4.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gemaakt en bewaard	1.	Overtredingen van het actuele netwerkbeleid (afwijkingen van de baseline) worden geregistreerd en vastgelegd in auditlogs.	CIP
Beoordeeld	2.	Het beoordelen van overtredingen wordt geautomatiseerd uitgevoerd bijvoorbeeld met SIEM of functioneel gelijkwaardige systemen en beoordeeld door deskundigen.	CIP

3.3.17 U.17 Netwerkbeveiligingsarchitectuur

Definitie

De beschrijving en beelden van de structuur en onderlinge samenhang van de verschillende beveiligingsfuncties in een netwerk.

Toelichting

Beveiligingsarchitectuur is niet expliciet genormeerd in de ISO 27002 2017. In de ISO 27033 deel 2 2012 wordt over netwerkbeveiligingsarchitectuur beschreven dat deze - gebaseerd is op het vigerende bedrijfsbeleid, leidende principes en geldende normen en standaarden - de samenhang van het netwerk beschrijft en structuur biedt voor de beveiligingsmaatregelen. Daarbij behoort het redundant uitvoeren van componenten of architecturen in overweging te worden genomen.

Doelstelling	Het bieden van een netwerkbeveiligingslandschap dat in samenhang is beveiligd en inzicht geeft in de inrichting daarvan.		
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
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 systeem.	CIP
	2.	De beveiligingsarchitectuur is gelaagd, zoals: • het (Nederlandse Overheid Referentie Architectuur) NORA-beveiligingsmetamodel; • SABSA®.	CIP

	3.	De netwerktopologie is in kaart gebracht en wordt continu actueel gehouden.	CIP

4 Control-domein

4.1 Doelstelling

Het doel van het control-domein (beheersing) is te zorgen en/of vast te stellen dat:

- netwerkdiensten veilig zijn ingericht voor het leveren van de beoogde prestaties;
- het beoogde beveiligingsniveau van technische netwerkdiensten en netcomponenten kan worden gegarandeerd.

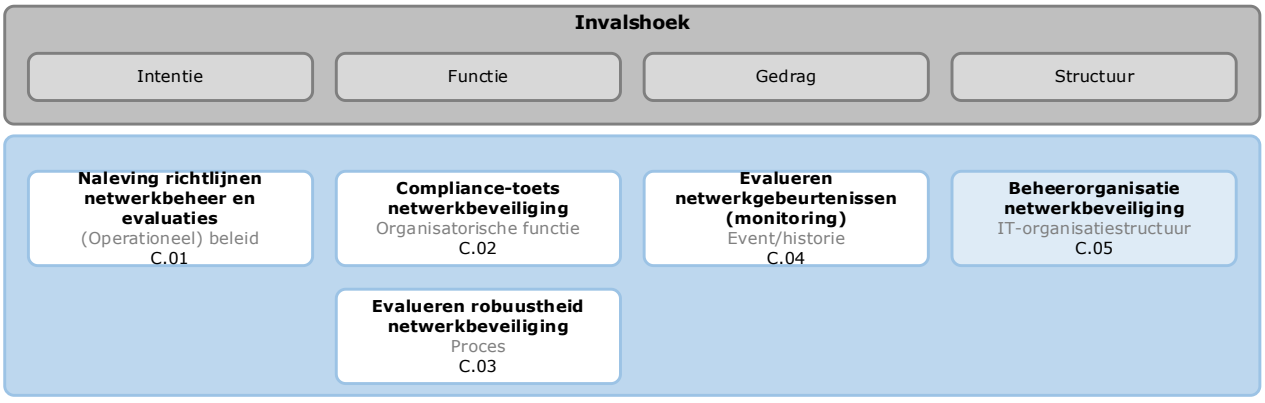
Dit betekent dat de organisatie over adequate beheersingsorganisaties beschikt en waarin beheerprocessen zijn vormgegeven.

4.2 Risico's

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

4.3 Objecten, controls en maatregelen

Onderstaande afbeelding is het resultaat van de SIVA-analyse op relevante objecten voor netwerk-control. Beheersing van netwerk(diensten) beoogt de beveiligingsrisico's te beperken. Hiertoe dienen periodiek door bepaalde functionarissen met specifieke bevoegdheden controleactiviteiten te worden verricht. Deze activiteiten dienen ondersteund te worden met procedures en richtlijnen (instructies). De structuur van de beheersingsorganisatie beschrijft de samenhang van de ingerichte processen.



Afbeelding 7: Overzicht communicatievoorzieningenobjecten in het control-domein

4.3.1 C.01 Naleving richtlijnen netwerkbeheer en evaluaties

Definitie

Een evaluatie op de naleving van het netwerkbeveiligingsbeleid.

Toelichting

Organisaties wisselen steeds meer elektronisch informatie uit, zowel met andere organisaties als met thuiswerkende medewerkers. Gelet op risico's van virussen en andere malware, maar ook van het weglekken van informatie, moeten communicatievoorzieningen continu worden onderhouden, bewaakt en geëvalueerd. Ook dient speciale aandacht besteed te worden aan de uitgewisselde informatie.

Doelstelling	Het vaststellen of de richtlijnen voor het naleven van het netwerkbeveiligingsbeleid nog steeds effectief zijn.		
Risico	Geen of onvoldoende inzicht of de richtlijnen voor het naleven van het netwerkbeveiligingsbeleid het netwerkbeveiligingsbeleid effectief toetsten.		
Control	Richtlijnen voor de **naleving** van het netwerkbeveiligingsbeleid behoren periodiek getoetst en geëvalueerd te worden.		CIP
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

4.3.2 C.02 Compliance-toets netwerkbeveiliging

Definitie

Een periodieke toetsing en een managementrapportage over de naleving van het beveiligingsbeleid voor netwerkdiensten.

Toelichting

In de praktijk is het noodzakelijk gebleken om regelmatig te toetsen of de beoogde beveiliging van de netwerkvoorzieningen nog conform 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	Vast te stellen of de inrichting van de netwerk(diensten) voldoet aan het beveiligingsbeleid.
Risico	Afwijkingen op het beveiligingsbeleid worden niet gesignaleerd.

Control	De naleving van een, conform 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
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Inrichting	1.	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
Periodiek	2.	Informatiesystemen worden jaarlijks gecontroleerd op de technische naleving van beveiligingsnormen en risico's op de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarhedenanalyses of penetratietesten.	ISO 27002 2017: 18.2.3
Verantwoor-delijke	3.	De resultaten worden gerapporteerd aan het verantwoordelijke management.	ISO 27002 2017: 18.2.1

4.3.3 C.03 Evalueren robuustheid netwerkbeveiliging

Definitie

De toetsing op de robuustheid (resilience) van beveiligingsfuncties in communicatievoorzieningen.

Toelichting

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. Het accent ligt hier op de vraag of de sterkte van de beveiliging voldoet aan de actuele eisen. Periodiek dienen zowel de organisatorische als de technische aspecten van beveiligingsmaatregelen beoordeeld te worden, die vervolgens worden gerapporteerd aan het verantwoordelijke management.

Doelstelling	Het vaststellen of de beveiliging van het complete netwerk nog 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
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

4.3.4 C.04 Evalueren netwerkgebeurtenissen (monitoring)

Definitie

Het beoordelen van de (doorlopend) verzamelde beveiligingsgerelateerde gebeurtenissen in netwerken.

Toelichting

Het beveiligen 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	Detectie, vastlegging en onderzoek mogelijk te maken van netwerkgebeurtenissen, die mogelijk van invloed op of relevant kunnen zijn voor de informatiebeveiliging.		
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** mogelijk te maken **van gebeurtenissen**, 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

	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

4.3.5 C.05 Beheerorganisatie netwerkbeveiliging

Definitie

De opzet van een toereikende organisatiestructuur voor het beheren van en rapporteren over netwerken en communicatievoorzieningen.

Toelichting

Het adequaat beheersen en beheren van de communicatievoorzieningen vereist een organisatiestructuur waarin de procesverantwoordelijkheden en de toereikende 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.		BIO 2019: 6.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Verantwoorde-lijkheden	1.	De communicatievoorzieningen worden geïdentificeerd en gedefinieerd.	CIP
	2.	Beheerderstaken vereisen in sommige gevallen vergaande bevoegdheden met risico's voor de doelorganisatie. Het beleggen van de juiste verantwoordelijkheden en toezien op het beoogde gebruik daarvan vergt extra aandacht, te weten: • De entiteit die verantwoordelijk is voor de communicatievoorzieningen wordt bepaald en de taken en details, vanuit de 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 2017: 6.1.1b, d en e