Versiegeschiedenis

Versie	Datum	Wijziging
1.0	11-2-2019	Eerste definitieve versie
1.1	31-7-2019	Antwoord 4 van onderwerp 16 bijgewerkt naar nieuwe datacenter standaarden en certificeringen.

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Quick scan Wbni

Kruis per onderwerp het antwoord aan dat op uw situatie van toepassing is.

		Antwoord				
Nr.	**Onderwerp**					**Toelichting / anders**
1	Organisatie van informatiebeveiliging	In mijn organisatie zijn verantwoordelijkheden voor informatiebeveiliging (nog) niet eenduidig belegd. ☐	Informatiebeveiligings-verantwoordelijkheden zijn duidelijk beschreven en belegd in de organisatie. ☐	Informatiebeveiligingsbeleid- en verantwoordelijkheden zijn duidelijk beschreven en de verantwoordelijkheid voor informatiebeveiliging is belegd tot op niveau van senior management. ☐	Informatiebeveiligingsbeleid- en verantwoordelijkheden zijn duidelijk beschreven en de verantwoordelijkheid voor informatiebeveiliging is belegd tot op niveau van senior management. Er is een Informatiebeveiligingstrategie opgesteld in lijn met de strategische doelen van de organisatie ☐	
2	Risicomanagement	Geen risico-analyse of risico-analyse niet actueel. ☐	De essentiële netwerk- en informatiesystemen zijn eenduidig in kaart gebracht en de grootste risico's zijn beschreven, inclusief de dreigingen en impact op deze systemen. ☐	De essentiële netwerk- en informatiesystemen zijn eenduidig in kaart gebracht en de grootste risico's zijn beschreven, inclusief de dreigingen en impact op deze systemen. Er wordt gebruik gemaakt van een erkende RA / RM methode en het rest-risico wordt bewust afgewogen. ☐	Er is een continu risico-analyse proces waarbij risico's periodiek worden geevalueerd op basis van dreigingen, kwetsbaarheden, maatregelen en impact. Dit proces wordt herzien na incidenten en is aligned met de informatiebeveiligingsstrategie. ☐	
3	Beveiligingsbeleid	Er is geen informatiebeveiligingsbeleid of deze is alleen mondeling overgebracht aan medewerkers. ☐	Er is een beleid voor de beveiliging van essentiële onderdelen van netwerk- en informatiesystemen. ☐	Er is beveiligingsbeleid en het beleid is goedgekeurd door senior management en er is rekening gehouden met van toepassing zijnde wet- en regelgeving. ☐	Er is beveiligingsbeleid, het beleid is goedgekeurd door senior management en er is rekening gehouden met van toepassing zijnde wet- en regelgeving en het informatiebeveiligingsbeleid wordt periodiek bijgewerkt. ☐	
4	Beveiligingstesten en audits	Er worden geen interne- of externe audits, controles of testen uitgevoerd. ☐	Netwerk- en informatiesystemen worden ad-hoc getest en geaudit. ☐	Er zijn procedures om testen en audits uit te voeren, inclusief de scope en frequentie. Periodiek worden netwerk- en informatiesystemen getest en geaudit volgens beschreven procedures. ☐	De effectiviteit van de procedures wordt regelmatig herzien en er is een helder overzicht van de uitgevoerde testen en audits, de bevindingen en de follow-up acties aan essentiële infrastructuur. De audits worden door een derde partij uitgevoerd. ☐	
5	Systeemontwikkeling: informatiebeveiliging	Informatiebeveiliging is geen integraal onderdeel van systeemontwikkeling ☐	Nieuwe systemen worden ontwikkeld volgens een gedocumenteerde methode waar informatiebeveiliging een onderdeel van is. ☐	Nieuwe systemen worden ontwikkeld volgens een gedocumenteerde methode waar informatiebeveiliging een onderdeel van is en de systemen worden uitgebreid op informatiebeveilgingsaspecten getoetst voordat zij in gebruik worden genomen. ☐	Nieuwe systemen worden ontwikkeld volgens een gedocumenteerde methode waar informatiebeveiliging een onderdeel van is en de systemen worden uitgebreid op informatiebeveilgingsaspecten getoetst voordat zij in gebruik worden genomen. Systeemontwikkelaars zijn opgeleid in secure development methodologies (b.v. secure coding) ☐	

6	Systeemontwikkeling: scheiding van de OTAP straat	Ontwikkeling, Test, Acceptatie en Productie zitten samen in één omgeving. ☐	Logische OTAP scheiding. Productie en acceptatie samen op een omgeving gescheiden van Ontwikkeling en Test. Ontwikkeling en Test zitten ieder in een aparte gescheiden omgeving. ☐	Fysieke en logische OTAP scheiding. Ontwikkeling, Test, Acceptatie en Productie zitten ieder in aparte van elkaar gescheiden omgevingen. Gevoelige of persoonsgegevens worden geanonimiseerd tijdens testwerkzaamheden en testgegevens worden verwijderd zodra de test gereed is. ☐	Fysieke en logische OTAP scheiding. Ontwikkeling, Test, Acceptatie en Productie zitten ieder in aparte van elkaar gescheiden omgevingen. Gevoelige of persoonsgegevens worden geanonimiseerd tijdens testwerkzaamheden en testgegevens worden verwijderd zodra de test gereed is. De scheiding van de OTAP-straat wordt periodiek getest op effectiviteit. ☐	
7	HRM: opleiding en awareness	De organisatie voorziet op ad-hoc basis het personeel van securitykennis, bijvoorbeeld bij een security incident. ☐	Personeel wordt voorzien van relevante securitykennis dmv documentatie en opleidingen (denk aan webpagina intranet etc.) ☐	Securitybewustzijn is opgenomen in het HR-beleid. ☐	Securitybewustzijn is opgenomen in het HR-beleid en het is opgenomen in de beoordelingscyclus van het personeel. ☐	
8	Assetmanagement	Er is geen inventarisatie van alle netwerk- en informatiesystemen en het het is niet duidelijk welke hiervan essentieel zijn zijn. ☐	Alle software en hardware assets zijn in kaart gebracht en dit is op een centrale plek gedocumenteerd. ☐	Alle software en hardware assets zijn in kaart gebracht en dit is op een centrale plek gedocumenteerd. Daarnaast is per asset bekend wie er verantwoordelijk voor is. ☐	Alle software en hardware assets zijn in kaart gebracht en dit is op een centrale plek gedocumenteerd. Daarnaast is per asset bekend wie er verantwoordelijk voor is en zijn er per asset security-eisen opgesteld waaraan zij moeten voldoen. ☐	
9	Ecosystemmanagement	Derde partijen zoals leveranciers en afnemers zijn niet duidelijk in beeld. ☐	Er is een overzicht met derde partijen en alle contracten met derden zijn beschikbaar en gedocumenteerd. ☐	Er is een overzicht met derde partijen en alle contracten met derden zijn beschikbaar en gedocumenteerd. Er is beveiligingsbeleid voor derde partijen (bijv. voor toeleveranciers) en eventuele restrisico's van die partijen worden beheerst. ☐	Er is een overzicht met derde partijen en alle contracten met derden zijn beschikbaar en gedocumenteerd. Er is beveiligingsbeleid voor derde partijen (bijv. voor toeleveranciers) en eventuele restrisico's van die partijen worden beheerst. Derde partijen worden geaudit op informatiebeveiligingsaspecten. ☐	
10	Netwerkintegriteit	Er wordt geen netwerkscheiding en monitoring toegepast. ☐	Netwerk zijn gescheiden van elkaar in verband met securitydoeleinden en de netwerken worden gemonitord. ☐	Er is een overzicht (netwerkkaart) waarin de scheidingen overzichtelijk zijn weergegeven obv kritieke componenten (bijv. scheiding operationele- en kantooromgeving). Verkeer tussen segmenten wordt gemonitord. ☐	Er is een overzicht (netwerkkaart) waarin de scheidingen overzichtelijk zijn weergegeven obv kritieke componenten (bijv. scheiding operationele- en kantooromgeving). Verkeer tussen segmenten wordt gemonitord. De zonering wordt regelmatig geëvalueerd na incidenten of bevindingen. ☐	
11	Cryptografie	Cryptografie wordt ad hoc gebruikt. ☐	Er wordt gebruik gemaakt van versleuteling voor de vertrouwelijkheid en integriteit van kritieke data in en buiten het bedrijf te waarborgen. ☐	Voor het gebruik van cryptografie bij kritieke data is beleid opgesteld en dit wordt periodiek herzien. ☐	Voor het gebruik van cryptografie bij kritieke data is beleid opgesteld en dit wordt periodiek herzien. Het beleid schrijft het gebruik van hashes voor om ongeoorloofde wijzigingen van kritieke data te monitoren. Het beleid wordt in de praktijk uitgevoerd. ☐	
12	Administration accounts (beheerderaccounts)	Er zijn geen beheeraccounts beschikbaar. Gebruikersaccounts worden gebruikt voor beheertaken. ☐	De organisatie heeft specifieke accounts voor het uitvoeren van beheertaken zoals installatie, onderhoud etc. van systemen die de essentiële dienstverlening ondersteunen en de autorisaties aan medewerkers met beheertaken toebedeeld. ☐	De organisatie heeft specifieke accounts voor het uitvoeren van beheertaken zoals installatie, onderhoud etc. van systemen die de essentiële dienstverlening ondersteunen en de autorisaties aan medewerkers met beheertaken toebedeeld. De beheeraccounts worden gemonitord en gelogd. ☐	Beheeraccounts worden gemonitord en gelogd. Er wordt bijv. gebruik gemaakt van privileged accountmanagement waarbij beheeracties worden gemonitord en gelogd. ☐	

13	Identificatie en authenticatie	Het is niet duidelijk wie toegang krijgt tot de netwerk- en informatiesystemen en er wordt geen gebruikersauthenticatie toegepast. ☐	Gebruikers en systemen hebben unieke ID's en worden geauthenticeerd voordat zij toegang krijgen tot netwerk- en informatiesystemen. ☐	Gebruikers en systemen hebben unieke ID's en worden geauthenticeerd voordat zij toegang krijgen tot netwerk- en informatiesystemen. Log-in pogingen worden gelogd en gemonitord. ☐	Gebruikers en systemen hebben unieke ID's en worden geauthenticeerd voordat zij toegang krijgen tot netwerk- en informatiesystemen. Log-in pogingen worden gelogd en gemonitord. Er worden verschillende authenticatiemechanismen gebruikt, afhankelijk van de toegangsrechten (SSO, 2FA etc.) en de fysieke locatie van de gebruiker. ☐	
14	Toegangsrechten	Toegangsrechten tot netwerk- en informatiesystemen worden ad-hoc toegekend. ☐	Netwerk- en informatiesystemen staan alleen geautoriseerd gebruik toe obv rollen en functies. ☐	Er is toegangsbeleid met beschrijving van rollen, groepen, toegangsrechten en procedures voor het toekennen en intrekken van rechten en de toegekende rechten worden geëvalueerd (autorisatiebeheer). ☐	Er is toegangsbeleid met beschrijving van rollen, groepen, toegangsrechten en procedures voor het toekennen en intrekken van rechten en de toegekende rechten worden geëvalueerd (autorisatiebeheer). Toegekende rechten worden regelmatig gecontroleerd. ☐	
15	Security-onderhoud: software updates en patches	Updates en patches van netwerk- en informatiesystemen worden op op ad-hoc basis uitgevoerd. ☐	Kritische en security updates/patches worden uitgevoerd volgens vastgelegde procedures. ☐	Kritische en security updates/patches worden uitgevoerd volgens vastgelegde procedures. Updates/ patches worden getest voordat zij worden gebruikt. ☐	Kritische en security updates/patches worden uitgevoerd volgens vastgelegde procedures. Updates/ patches worden getest voordat zij worden gebruikt. Bij de kritieke systemen wordt periodiek gecontroleerd of zij voorzien zijn van de meeste actuele updates en patches. ☐	
16	Fysieke- en omgevingsbeveiliging	Er wordt geen gebruik gemaakt van toegangsbeveiliging. ☐	Ongeautoriseerde toegang tot faciliteiten en infrastructuur wordt voorkomen. ☐	Fysieke beveiliging van netwerk- en informatiesystemen voldoet aan basis beveiligingsnormen (Afgesloten en speciaal hiervoor toegeruste klimaat geconditioneerde ruimte, Pasjes toegangssysteem, UPS: overbrugging ihgv korte uitval energievoorziening, brandblussers). ☐	Netwerk en informatiesystemen zijn ondergebracht in een datacenter (Beveiligd en ervoor toegerust gebouw, fysieke bewaking, Brand detectie/blussysteem, CCTV 24/7 bewaking, Bezoekersregistratie, pasjes toegangssysteem, UPS, Nood aggegraat, etc.) dat gecertificeerd is volgens internationale standaarden zoals ISO 27001, TIA-942, SOC 1 Type II, SOC 2 Type II, etc. ☐	
17	Detectie, logging, monitoring en correlatie	Logs worden niet gemaakt of slechts gebruikt ná een incident. ☐	Er is beleid en er zijn procedures om security-incidenten te detecteren tijdens kantooruren. ☐	Er is beleid en er zijn procedures om security-incidenten 24/7 te detecteren. Er is een systeem in werking voor incidentdetectie, correlatie en response (bijv een SIEM) op basis van stand-by diensten. ☐	Er is een security operations center actief met 24uurs operatie em de detectiesystemen worden periodiek en onaangekondigd getest op effectiviteit. ☐	
18	Incidentmanagement	Incidenten worden ad-hoc afgehandeld. ☐	Er is een incidentmanagementproces dat voorschrijft hoe incidenten worden afgehandeld. ☐	Er is een incidentmanagementproces dat voorschrijft hoe incidenten worden afgehandeld. Er wordt een register met security-incidenten bijgehouden. ☐	Er is een incidentmanagementproces dat voorschrijft hoe incidenten worden afgehandeld. Er wordt een register met security-incidenten bijgehouden. Het proces wordt getest en geactualiseerd met, onder andere, red en blue teaming. ☐	
19	Communicatie met autoriteit	Er zijn geen afspraken vastgelegd over de communicatie van incidenten. Incidenten worden ad-hoc gecommuniceerd. ☐	Er is een proces geïmplementeerd dat incidenten onverwijld meldt bij bevoegde toezichthouders. ☐	Er is een proces geïmplementeerd dat incidenten onverwijld meldt bij bevoegde toezichthouders. Het proces wordt regelmatig getest en indien nodig herzien. ☐	Er is een proces geïmplementeerd dat incidenten onverwijld meldt bij bevoegde toezichthouders. Het proces wordt regelmatig getest en indien nodig herzien. Het proces is onderdeel van het crisismanagementproces. ☐	

20	BCM	Er zijn geen continuïteitsmaatregelen genomen, de AED heeft geen helder beeld over de mate van beschikbaarheid van de essentiële dienst en er zijn geen uitwijkvoorzieningen in het geval van rampen. ☐	Continuïteit en uitwijkvoorzieningen worden op ad hoc basis geregeld. ☐	De doelen van het continuiteitsmanagement zijn duidelijk uitgeschreven en vastgelegd in een continuïteitsstrategie en uitgewerkt in concrete plannen. Er is beleid met dreigingsanalyses, hersteltijden, uitwijkplannen etc. voor het geval de dienst uitvalt. ☐	De doelen van het continuiteitsmanagement zijn duidelijk uitgeschreven en vastgelegd in een continuïteitsstrategie en uitgewerkt in concrete plannen. Er is beleid met dreigingsanalyses, hersteltijden, uitwijkplannen etc. voor het geval de dienst uitvalt. Alle personeel dat betrokken is bij de continuiteit van de AED is goed getraind in haar rollen en verantwoordelijkheden met betrekking tot netwerk- en informatiesystemen. Het volledige personeel weet wat van hen verwacht wordt in het geval van een crisis. Er vinden periodiek testen plaats en die bevindingen worden verwerkt in de processen. ☐	
21	Crisisproces- en organisatie	Crisissituaties worden op ad-hoc basis afgehandeld. ☐	Er is crisismanagementbeleid en draaiboek voor het afhandelen van security-incidenten waar scenario's, rollen en verantwoordelijkheden in zijn beschreven. ☐	Er is crisismanagementbeleid en draaiboek voor het afhandelen van security-incidenten waar scenario's, rollen en verantwoordelijkheden in zijn beschreven. Het crisismanagementbeleid en de draaiboeken worden periodiek herzien. ☐	Er is crisismanagementbeleid en draaiboek voor het afhandelen van security-incidenten waar scenario's, rollen en verantwoordelijkheden in zijn beschreven. Het crisismanagementbeleid en de draaiboeken worden periodiek herzien. Er worden periodiek crisismanagement oefeningen gehouden. ☐	

Proces dossierreview:
1. 5.1.2.e voert de dossierreview ten behoeve van de volledigheid uit.
2. 5.1.2.e voeren de dossierreview ten behoeve van de inhoud uit.
3. Het rapport wordt na afronding van alle punten uit 1 en 2 ondertekend door 5.1.2.e (via 5.1.2.e).
4. Na ondertekening en versturen rapport rond 5.1.2.e haar dossierreview af.

Nr	Sub	Onderwerp	Bevindingen reviewer	Reactie inspecteurs
ALGEMEEN				
1	a	De checklist 'volledigheid' (dossierreview door 5.1.2.e) is uitgevoerd (voor zo ver als mogelijk).		
	b	Punten uit de dossierreview van 5.1.2.e zijn afgehandeld.		
UITVOERING				
2	a	Bevindingen zijn eenduidig vastgelegd (het is duidelijk wat de bevindingen zijn).		
	b	Bevindingen zijn aantoonbaar gewogen (wat neem je wel/niet op in het rapport, zie ook onderstaande tabel vanaf regel 20).		
	c	Bevindingen zijn met evidence onderbouwd (verwijzing naar gespreksverslag of andere evidence).		
RAPPORTAGE				
3	a	Bevindingen zijn in het rapport overgenomen (zie 1b).		
	b	Het rapport bevat naast negatieve bevindingen (verbeterpunten) ook een beknopte omschrijving van wat goed gaat (in control), zodat de leze de bevinding kan duiden.		
	c	De geformuleerde actie en planning van een AED op een bevindingen is in het rapport opgenomen.		
4	a	Het rapport bevat geen adviezen.		
	b	Het rapport bevat geen oordelen.		
	c	Het rapport bevat geen conclusie.		
	d	Het rapport bevat geen subjectieve teksten.		

Tabel bij 2b.

	Onderkend AED	Onderkend AT
Weinig impact	Wel opnemen Geen feedback Geen monitoring	Wel opnemen Wel / geen feedback Monitoring account mngt
Veel impact	Wel opnemen Wel feedback Monitoring d.m.v.....	Wel opnemen Wel feedback Monitoring d.m.v.....

Laat de checklist na afronding van de inspectie invullen door 5.1.2.e
Op basis van de ingevulde checkllist leggen de inspecteurs een reactie in dit document vast.
Te allen tijde moet het dossier minimaal voldoen aan de **vetgedrukte** onderwerpen.

Nr	Sub	Onderwerp	Bevindingen reviewer	Reactie inspecteurs
ALGEMEEN				
1	a	De directory van het dossier is omschreven conform de naamgevingsconventie (202x xx x omschrijving)		
2	a	Het dossier kent de volgende structuur*: 001 Planning 002 Uitvoering 003 Rapportage		
PLANNING				
3	a	In de directory 001 Planning zijn minimaal de volgende documenten opgenomen: **- een ondertekende aankondigingsbrief met RP2000 nummer** - de self assessment **- bewijs dat de aankondigingsbrief is verzonden naar de AED**		
	b	De documenten zijn op de templates van het dummy dossier gebaseerd.		
	c	De documenten bevatten de juiste naamgevingsconventie.		
	d	De selectie van de deelwaarneming is gebaseerd op het risicomodel		
UITVOERING				
4	a	In de directory 002 Uitvoering zijn minimaal de volgende documenten opgenomen: - het originele ingevulde self assessment van de AED - het ingevulde ingevulde toetsingskader - de afstemming van de bevindingen		
	b	De documenten zijn op de templates van het dummy dossier gebaseerd.		
	c	De documenten bevatten de juiste naamgevingsconventie.		
	e	**Uit de afstemming van de bevindingen (of aanvullend document) blijkt dat 'hoor en wederhoor' met de AED heeft plaatsgevonden.**		
RAPPORTAGE				
5	a	Er is een inhoudelijke review uitgevoerd door één van de Lead IT Auditors		
	b	In de directory 003 Rapportage zin minimaal de volgende documenten opgenomen: **- de ondertekende eindrapportage met RP2000 nummer** **- bewijs dat de eindrapportage is verzonden naar de AED**		
	c	Het document is op de templates van het dummy dossier gebaseerd.		
	d	Het document bevat de juiste naamgevingsconventie.		

* Tip: maak eventueel een (of meerdere) map 'Archief' aan om concept versies in op te slaan. Zo is het direct duidelijk wat de definitieve versies van docementen zijn.

Toetsingskader op basis van ISO27001						In te vullen door de inspecteur												
Onderwerp	Subonderwerp		Doelstelling	Goodpractice (ISO27002)	Verseist volwassenheidsniveau	Aandachtspunten voor de inspecteur	Interview	Eigen waarneming	Beleid, procedure of instrcutie	Schermafdruk	Documentatie	Deelwaarneming	Interview verslag	Verslag overige evidence (eigen waarneming, beleid, procedure of instructie, schermafdruk en documentatie)	Afgerond?	Afgestemd met AED	Volwassenheid volgen inspecteur	Eventuele acties naar aanleiding van de inspectie
<NR> <PROCES>				Ga bij de beoordeling van deze doelstelling ten minste in op:														
	<NR>	<SUBONDERWERP>	<DOELSTELLING>	<GOODPRACTICES>	3		☑	☐	☑	☐	☑	☑	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Zie tab A.12.1	Verwijzing naar evidence: Bevindingen inspecteur:	Nee			Omschrijving: Actiehouder: Deadline:
					3		☑	☐	☑	☐	☑	☐	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur:		Nee	☐ ☐		
					3								Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur:	Verwijzing naar evidence: Bevindingen inspecteur:	Nee			Omschrijving: Actiehouder: Deadline:
					3		☑ ☑	☐ ☐	☑ ☐	☐ ☐	☑ ☑	☑ ☐	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur:	Verwijzing naar evidence: Bevindingen inspecteur:	Nee	☐ ☐		Omschrijving: Actiehouder: Deadline:

Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (033) 460 08 00
F (033) 460 08 50
www.agentschaptelecom.nl

Instructie deelwaarneming

Datum
25 mei 2021

Nummer
5.1.2.e

Onderwerp Instructies voor het toepassen van de deelwaarneming voor Reguliere Inspectie 2021

Reguliere Inspectie
Er is een procesbeschrijving waarin de stappen zijn beschreven van de reguliere inspectie[1]. Dit document is een aanvullende toelichting over het toepassen van de deelwaarneming voor review van de reguliere inspectie.

Selecteren beheersdoelen voor de (5) deelwaarnemingen
De AED's worden gevraagd om een selfassessment in het kader van reguliere inspectie uit te voeren. Een onderdeel van de self-assessment is het selecteren van 5 beheersdoelen die tijdens de inspectie dieper wordt nagegaan of het volwassenheidsniveau dat de AED heeft aangegeven gestaafd kan worden met bewijsmateriaal. Het doel is vast te stellen of het aangegeven volwassenheidsniveau van de AED juist en volledig zijn onderbouwd.

Centrale vraag
Vraagstelling: Geef de BBNI-selfassessment inclusief onderbouwing van de AED een betrouwbaar beeld van het volwassenheidsniveau?

Auditvariabelen
Om een antwoord te kunnen geven op de centrale vraag zal de volgende deelvraag (variabele) beantwoord moeten worden.

Variabele 1: *De volwassenheidsniveaus zijn juist en volledig onderbouwd.*
Door onderstaande 2 normen te toetsen wordt de variabele beantwoord.

Norm A1	*De opgevraagde 5 beheersdoelen zijn met evidence onderbouwd (juistheid en volledigheid)*
Norm A2	*De opgeleverde bewijsstukken sluiten aan op het volwassenheidsniveau (juistheid) die zij zelf aangegeven hebben in de BBNI self-assessment.*

Objecten

[1] buiten reikwijdte

De beheersdoelen worden op basis van het risicomodel geselecteerd. Hiervan wordt gebruik gemaakt van zowel een interne als een externe analyse. Uit een gezamenlijke workshop met de inspecteurs zijn de volgende dreigingen/ onderwerpen (externe analyse) uit voortgekomen namelijk:

- business continuity management (BCM);
- supply chain management (SCM);
- vulnerability management.

De vastlegging van deze 3 thema's zijn verwerkt in een risicomodel[2]. Aanvullend zal er nog 2 aanvullende dreigingen/thema's geselecteerd moeten worden op basis van interne analyse van de individuele AED. Deze 2 thema's worden bepaald door de toegewezen inspecteurs voor de desbetreffende AED o.b.v. de volgende punten in te vullen in het risicomodel[3].

1. De volgende tabbladen invullen in het risicomodel (zie aanvullende toelichting over het risicomodel[4]):

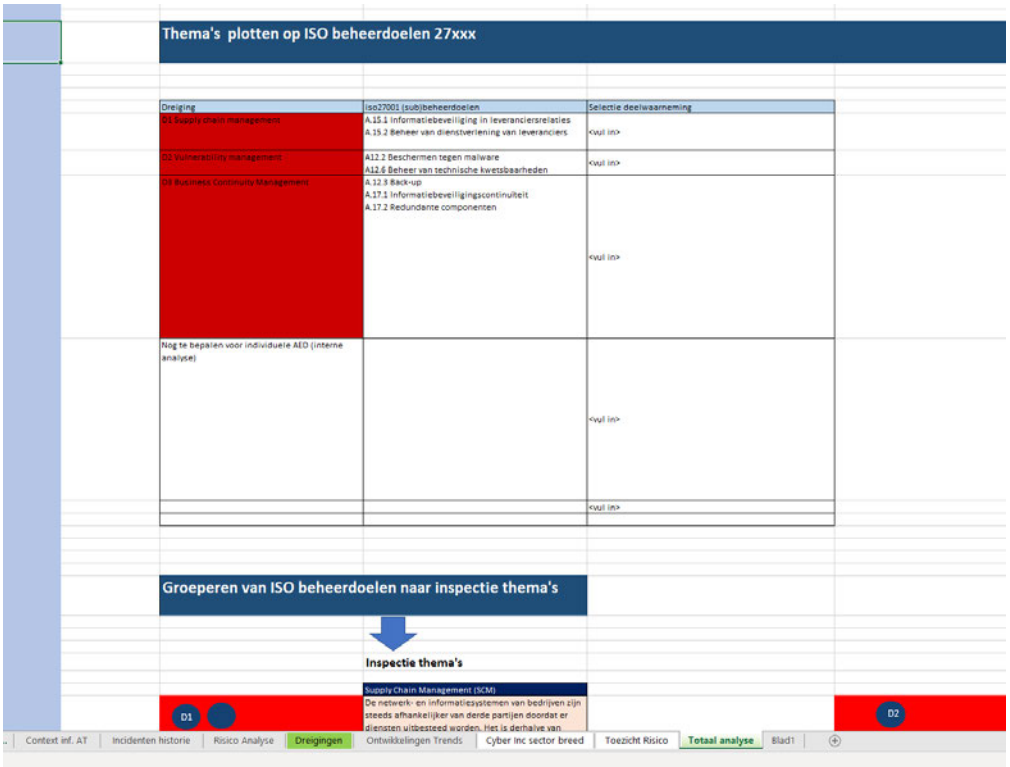
- Incidenten historie AED (reeds ingevuld, vul eventueel aan en verwijder de niet relevante incidenten);
- Context informatie AT (o.a. bijvangst uit thema inspecties en accountgesprekken en specifieke ontwikkelingen of dreigingen voor desbetreffende AED bepalen) die interessant zijn om als onderwerp te nemen voor de deelwaarneming. Neem een toelichting op indien onderwerpen interessant zijn, maar al op een andere manier zijn geadresseerd (bv. voortgang bewaken via accountmanagement gesprek);
- AED self-assessment resultaten 2019 en van 2021, wat valt op en wat is mogelijk interessant om als onderwerp te nemen voor de deelwaarneming. Een voorbeeld kan zijn dat een onderwerp in 2021 veel hoger scoort t.o.v. 2019, dit kan een aanleiding zijn om dit onderwerp in de deelwaarneming te betrekken.

2. Volgende stap zijn de dreigingen plotten in het risicomodel tabblad "totaal analyse" en dit ook vast te leggen. Indien dreigingen/risico's vanuit verschillende tabbladen overlappen, kun je een pijl trekken tussen de blauwe bollen. Zo voorkom je dubbelingen in de heatmap.
(Wat rood scoort is mogelijk een onderwerp om mee te nemen in de deelwaarneming). De beschreven methode is een raamwerk waarbij het gebruik van 'gezond verstand' en vakkundige oordeelsvorming een grote rol blijft spelen. Indien er meer dan 5 onderwerpen zijn, dien je te onderbouwen welke 5 onderdeel zijn van de deelwaarneming en waarom andere niet onderdeel hiervan zijn. Indien er minder dan 5 onderwerpen zijn, kan je 2 extra beheerdoelen selecteren uit de onderwerpen 'Supply chain management', 'Vulnerability management' of 'Business Continuity Management'.

Het ingevulde risicomodel van Enexis kan als voorbeeld worden gehanteerd. Zie:
buiten reikwijdte [redacted]

2 buiten reikwijdte [redacted]
3 buiten reikwijdte [redacted]
4 buiten reikwijdte [redacted]

Van 5 thema's naar concrete beheersdoelen om te toetsen
Er zijn drie thema's al geplot op ISO beheersdoelen[5]. Als voorbeeld nemen we SCM thema. Hierbij is het de bedoeling om één beheersdoel als deelwaarneming voor de thema SCM te selecteren keuze tussen A15.1 (informatiebeveiliging in leveranciersrelaties) of A15.2 (beheer van dienstverlening van leveranciers). Vervolgens te toetsen of het beheersdoel is onderbouwd met evidence (juistheid en volledigheid) en of de opgeleverde bewijsstukken aansluiten op het volwassenheidsniveau (juistheid) die zij hebben aangegeven. Voor de andere 4 thema's wordt er eveneens verwacht dat per thema één beheersdoel uit de ISO wordt geselecteerd om te reviewen.



Nog uit te werken zijn de andere nog te bepalen thema's uit de interne analyse die gekoppeld moet worden aan ISO (sub) beheersdoelstellingen.

Let op: De AED wordt vooraf niet ingelicht over de beheersdoelstellingen waar we dieper op ingaan tijdens de inspectie. Wel kan hem worden medegedeeld dat we op een aantal onderwerpen dieper ingaan zodat hij zich kan voorbereiden.
Het aantal van 5 deelwaarnemingen kan naar beneden gesteld worden naar minimaal 3 deelwaarnemingen indien het niet binnen de gestelde tijd uitgevoerd kan worden.

5 buiten reikwijdte

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

BBNI Self-Assessment Handleiding
Concept en Tool

BBNI Self-Assessment Handleiding – Concept en Tool
Agentschap Telecom
Versie 1.2
10/05/2021

INHOUDSOPGAVEN

1. Introductie **3**

2. Doel **4**

3. ASSESSMENT MODEL **4**

3.1. Concept *4*

3.2. Scope *4*

3.3. Extra Standaarden *5*

3.4. Volwassenheidsmodel *5*

4. ASSESSMENT TOOL **8**

4.1. Kennismaken met de tool *8*

4.2. Gebruik van de tool *8*

5. Resultaten van het assessment **10**

6. Ondersteuning **10**

1. INTRODUCTIE

De EU-richtlijn 2016/1148, bekend als de richtlijn voor netwerk- en informatiesystemen (NIS) is goedgekeurd door het EU-parlement in juli 2016. De EU-richtlijn 2016/1148 behandelt maatregelen op hoog niveau om de veerkracht van aanbieders van vitale diensten tegen cyberaanvallen te waarborgen.

In Nederland moeten digitale dienstverleners en aangewezen aanbieders van essentiële diensten (AED) in de sectoren energie en digitale infrastructuur voldoen aan de Wet Beveiliging Netwerk- en Informatiesystemen (WBNI), de integratie van de NIS-richtlijn in de nationale wetgeving. Ze moeten maatregelen nemen om incidenten te voorkomen en incidenten met aanzienlijke gevolgen melden. Agentschap Telecom is vanaf 9 november 2018 toezichthouder op deze wet.

Samen met de WBNI treedt op 9 november 2018 ook het Besluit Beveiliging Netwerk- en Informatiesystemen (BBNI) in werking, met de BBNI wordt er een nadere invulling gegeven aan de zorgplicht. De BBNI duidt de vitale aanbieders aan die onder de verplichtingen van de WBNI vallen, en de volgende beveiligingsdomeinen:

- **Risico gebaseerde aanpak**: De aanbieder heeft een actueel overzicht van de netwerk- en informatiesystemen die zijn essentiële dienst ondersteunen. De aanbieder stelt een risicoanalyse op met inachtneming van de relevante normen en ontwikkelingen. In de analyse beschrijft hij de risico's en de wijze waarop hij de risico's tot een aanvaardbaar niveau verkleint. Hij motiveert waarom dit niveau proportioneel en aanvaardbaar is. Hierbij houdt hij niet alleen rekening met de organisatie-specifieke en sectorspecifieke risico's, maar ook met het maatschappelijke belang van zijn essentiële dienst en met de stand van de techniek. Hij zorgt ervoor dat de resultaten van de risicoanalyse inzichtelijk en toetsbaar zijn en hij verwerkt de resultaten in risicogerichte beveiligings- en beheersmaatregelen.

- **Organisatie van netwerk- en informatiebeveiligingsbeheer:** De aanbieder zorgt voor het opstellen, uitvoeren, handhaven, bewaken en uitdragen van een informatiebeveiligingsbeleid op basis van de relevante normen en de stand der techniek. Hij heeft een informatiebeveiligingsstrategie die in lijn is met zijn strategische doelen en met het maatschappelijke belang van zijn essentiële dienst. Hij heeft de taken, bevoegdheden en verantwoordelijkheden voor de beveiliging en beheer van zijn netwerk- en informatiesystemen duidelijk in de organisatie belegd.

- **Incidenten voorkomen**: De aanbieder draagt zorg voor een gelaagde beveiligingsstrategie gericht op het adequaat beheersen van risico's voor de netwerk- en informatiesystemen die de essentiële dienst ondersteunen. Onderdeel van deze beveiligingsstrategie vormt onder andere het toepassen van defense in depth en passend lifecycle-, asset- en patchmanagement. Deze en andere maatregelen, zoals identificatie- en toegangsmanagement, zijn op risicoanalyses gebaseerd. De aanbieder is daardoor in staat om tijdig en adequaat om te gaan met geïdentificeerde kwetsbaarheden en dreigingen. Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op voor hem relevante beveiligingsadviezen en dreigingsinformatie beoordeelt hij of gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's tot een aanvaardbaar niveau te reduceren.

- **Detectie en respons:** De aanbieder neemt passende maatregelen om incidenten te kunnen detecteren, analyseren en vastleggen en om hun gevolgen zo veel mogelijk te beperken. Hij monitort structureel relevante netwerk- en informatiesystemen, legt relevante handelingen op die systemen onweerlegbaar vast en bewaart die gegevens lang genoeg om incidenten te kunnen analyseren. Hij houdt hierbij rekening met door de overheid beschikbaar gestelde

relevante dreigingsinformatie. Hij hanteert procedures om op consistente en doeltreffende wijze op te treden bij incidenten.

- **Gevolgen van incidenten beperken**: De aanbieder zorgt voor het opstellen van een bedrijfscontinuïteitsbeleid en een crisismanagementbeleid voor de netwerk- en informatiesystemen. Onderdeel van zijn crisismanagementbeleid is ten minste een plan dat hem in staat stelt de essentiële dienst zo spoedig mogelijk te herstellen na een incident. Het crisismanagementbeleid wordt daartoe periodiek in de praktijk beoefend.

In het toezicht op deze partijen onderkent Agentschap Telecom 3 stappen:

1. Inventarisatie
2. Self-Assessment
3. WBNI thematische onderzoeken (op basis van dreigingsmonitoring)

2. DOEL

AT heeft een zelfevaluatietool gebouwd met de volgende doelen:

- Bewustwording vergroten over de huidige beveiligingspositie van de AED's
- Dienen als communicatiekanaal tussen Agentschap Telecom en AED om de volwassenheid van hun beveiligingsprogramma te bepalen
- Het ondersteunen van AED om te voldoen aan de gestelde BBNI vereisten.

3. ASSESSMENT MODEL

3.1. Concept

De voorgestelde beoordeling van de volwassenheid van AED-beveiliging ten opzichte van BBNI is gebaseerd op de volgende concepten:

- **Self-assessment:** de AED geeft een eigen visie op hoe de beveiligingseisen worden benaderd, beheerd, ingezet en onderhouden vanuit het perspectief van governance en implementatie.
- **Op vertrouwen gebaseerd:** hoewel bewijzen en gedetailleerdere beoordelingen kunnen worden gevraagd als vervolg op deze regelmatige inspecties, is het belangrijk om te benadrukken dat dit een gezamenlijke inspanning is, gebaseerd op vertrouwen tussen AED en de overheid, die tot doel heeft de betrouwbaarheid van nationale kritische diensten.
- **Focus op kwalitatieve compliance:** de belangrijkste output van de beoordeling zijn de omschrijvingen in vrije tekst van hoe de AEDs de beveiligingsvereisten benaderen, beheren, implementeren, bedienen en onderhouden. De kwantitatieve scores zijn nuttig om een algemeen beeld te geven, er zijn in dit stadium geen kwantitatieve doelstelling of minimumdrempels verplicht.
- **Beoordeling van governance en Implementatie:** de kwalitatieve compliance wordt beschreven vanuit de governance (strategie, aanpak, gedocumenteerd beleid en processen) en Implementatie (inzet, exploitatie, onderhoud) perspectieven**.**

3.2. Scope

AED's worden door Agentschap Telecom uitgenodigd om zichzelf te beoordelen met behulp van dit model en deze tool.

Binnen elke AED zijn de systemen die binnen het bereik moeten worden beschouwd degene die een directe impact hebben op de levering van de essentiële dienst. Systemen/ afdelingen die financiële,

reputatieschade of andere gevolgen hebben voor de AED, maar niet in staat zijn om de levering van de essentiële dienst in gevaar te brengen, hoeven niet meegenomen te worden in de tool.

3.3. Extra Standaarden

Zoals eerder vermeld, beoogt het assessment te meten of wordt voldaan aan de BBNI-standaard.
Om dit te bereiken, wordt ook rekening gehouden met andere normen om extra context, diepgang en relevantie te bieden aan kritieke infrastructuren:

- **ISO 27001**: gezien de populariteit van deze standaard onder kritieke infrastructuren voor het bouwen en exploiteren van een informatiebeveiligingsbeheersysteem, waren de beoordelingsvragen gebaseerd op de vereisten van deze standaard.
- **NIST CSF:** Dit populaire raamwerk is doelbewust gebouwd om kritieke infrastructuren te ondersteunen bij een zelfevaluatie, het opstellen van routekaarten voor veiligheid en biedt een tastbare benadering van cyber security activiteiten. De vragen in het assessment zijn toegewezen aan de vijf NIST CSF-functies.
- **IEC 62443-2-1 en 62443-3-3:** ISO-vereisten werden in kaart gebracht aan deze twee normen van de IEC 62443-familie om extra relevantie te bieden voor de AED die industrieel van aard zijn. Het IEC 62443-2-1 heeft betrekking op beveiligingsbeheer bij eigenaren van assets en het IEC 62443-3-3 raamwerk heeft betrekking op de implementatie van beveiligingscontroles in industriële automatiseringssystemen.

3.4. Volwassenheidsmodel

Bij de uitvoering van het toezicht op de wet Beveiliging Netwerk- en Informatiesystemen door AT worden reguliere inspecties uitgevoerd bij de onder toezicht gestelde AED's. Bij deze reguliere inspecties voeren de AED periodieke self assessments uit. In de self assessment zijn volwassenheidsniveaus opgenomen. Bij het invullen van het self assessment houden de AED's bij het toekennen van de volwassenheidsniveaus, rekening met de definities in onderstaande tabel.

De onderstaande tabel is tot stand gekomen mede op basis van gehanteerde volwassenheidsniveau 's door De Nederlandse Bank (DNB)[1], het volwassenheidsmodel Informatiebeveiliging van NBA-LIO en NOREA[2] en het CMM-I model[3].

Het volwassenheidsmodel kent een vijftal niveaus van volwassenheid. Deze worden hieronder verder toegelicht.

[1] Bron: https://www.toezicht.dnb.nl/binaries/50-237685.pdf
[2] Bron: https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/
[3] Bron: https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

Figuur 1: Volwassenheidsmodel Niveaus

Niveau	Definitie van het volwassenheidsniveau	Criteria ter verduidelijking
1	**Initieel** – De beheersmaatregel is (gedeeltelijk) gedefinieerd maar wordt op inconsistente wijze uitgevoerd. Er is een grote afhankelijkheid van individuen bij de uitvoering van de beheersmaatregel.	Geen of beperkte beheersmaatregel geïmplementeerd. Niet of ad-hoc uitgevoerd. Niet /deels gedocumenteerd. Wijze van uitvoering afhankelijk van individu (niet gestandaardiseerd)
2	**Herhaalbaar maar informeel** – De beheersmaatregel is aanwezig en wordt op consistente en gestructureerde, maar op informele wijze uitgevoerd.	De uitvoering van de beheersmaatregel is gebaseerd op een informele maar wel gestandaardiseerde werkwijze. Deze werkwijze is niet volledig gedocumenteerd. In dit geval is wel het bestaan en de werking van maatregelen vast te stellen. Er is niet geborgd dat procedures conform een standaard template van de organisatie zijn opgesteld. Er is niet geborgd dat procedures periodiek worden geëvalueerd. De procedure is door de procesmanager vastgesteld (niet door het management). De effectiviteit van maatregelen wordt niet actief gemonitord, maar is wel vast te stellen.

3	**Gedefinieerd** – De opzet van de beheersmaatregel is gedocumenteerd en wordt op gestructureerde en geformaliseerde wijze uitgevoerd. De vereiste effectiviteit van de beheersmaatregel is aantoonbaar en wordt getoetst.	Beheersmaatregel is gedefinieerd o.b.v. risico assessment (risico gebaseerd). Gedocumenteerd en geformaliseerd (geaccordeerd door het management). Verantwoordelijkheden en taken zijn eenduidig vastgelegd en toegewezen. Opzet, bestaan en effectieve werking zijn aantoonbaar. Effectieve werking van controls wordt periodiek getoetst (actief monitoren). De toetsing vindt risico gebaseerd plaats en toont aan dat de control effectief is over een langere periode (>6 maanden). De uitvoering van de beheersmaatregel wordt aan het management gerapporteerd.
4	**Beheerst en meetbaar** – De effectiviteit van de beheersmaatregel wordt periodiek geëvalueerd. Daar waar nodig wordt de beheersmaatregel verbeterd of vervangen door andere beheersmaatregel(en). De evaluatie wordt vastgelegd.	Criteria voor niveau 3 plus de volgende onderscheidende criteria: Periodieke (control) evaluatie en opvolging vindt plaats. Evaluatie is gedocumenteerd. Taken en verantwoordelijkheden voor het evalueren zijn geformaliseerd. Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de instelling en is minimaal jaarlijks. In de evaluatie worden (operationele) incidenten meegenomen. De uitkomsten van de evaluatie wordt aan het management gerapporteerd.
5	**Continu verbeteren** – De beheersmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering van de effectiviteit van de maatregelen. Hierbij wordt gebruik gemaakt van externe data en benchmarking. Medewerkers zijn pro-actief betrokken bij de verbetering van de beheersmaatregelen	Criteria voor niveau 4 plus de volgende onderscheidende criteria: Continu evalueren van de beheersmaatregelen om de effectiviteit van beheersmaatregelen voortdurend te verbeteren. Gebruik makend van resultaten uit self-assessments, gap en root cause analyses. De getroffen beheersmaatregelen worden gebenchmarkt op basis van externe data en zijn 'Best Practice' in vergelijking met andere organisaties.

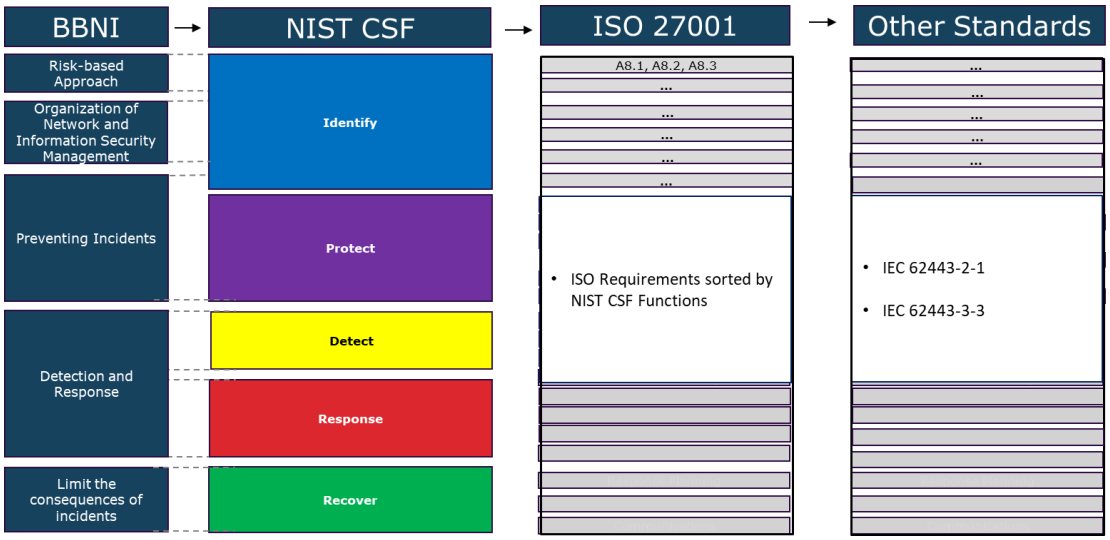
4. ASSESSMENT TOOL

4.1. Kennismaken met de tool

Er is een op Excel gebaseerde tool gebouwd om de self assessment te ondersteunen.

De belangrijkste input is de kwalitatieve nalevingsbeschrijving van hoe de AED de invulling van de van elke beheersdoelstelling aanpakken. De beschrijving bevat antwoorden op de vragen die bij elke vereiste horen en beschrijft, indien van toepassing, het huidige standpunt van governance en Implementatie.

De tool zelf biedt context aan de assessment vragen door ze toe te wijzen aan de BBNI-domeinen, NIST CSF-functies en IEC 62443-2-1 en IEC 62443-3-3-vereisten. Figuur 2.



Figuur 2: Assessment Tool - Process Flow

Ten slotte voert de tool een volwassenheidsscore uit voor elke ISO-vereiste, volgens het volwassenheidsmodel beschreven in paragraaf 3.4. De tool biedt ook grafische visualisaties van volwassenheidsscores per BBNI-domein.

Er wordt vanuit gegaan dat de AED, toegang hebben tot de laatst gepubliceerde versies van de bovengenoemde normen, aangezien deze niet als onderdeel van de assessmenttoolkit worden aangeboden.

4.2. Gebruik van de tool

De tool is gemaakt om intuïtief en vanzelfsprekend te zijn, maar de volgende opmerkingen kunnen het gebruik ervan verder verduidelijken:

- Hoewel de **assessment vragen** weergeven wat de BBNI vereisten zijn, is het raadzaam dat de AED verwijzen naar de overeenkomstige vereisten van bijvoorbeeld de ISO, NIST en voor industriële infrastructuren IEC om de compliance beschrijvingen te verrijken.
- **Kwalitatieve compliance beschrijvingen** zullen, waar van toepassing, de huidige stand van zaken van governance en implementatie bevatten. In de beschrijvingen wordt vermeld hoe de AED de vereiste integreert in zijn strategie, cyberbeveiligingsbeleid, norm, processen en procedures en moet omvatten hoe de AED de vereisten heeft ingezet, functioneert, handhaaft ter ondersteuning van de doelstellingen en doelen die in het beleid zijn vermeld.

- **Kwantitatieve compliance beschrijvingen** worden geselecteerd uit de vijf mogelijke opties, die elk overeenkomen met een vastgesteld volwassenheidsniveau. Als de AED, voor een bepaalde vereiste, zeer uiteenlopende volwassenheidsniveaus vertoont (bijv. Beleid en processen die volledig zijn gedocumenteerd en goedgekeurd maar helemaal niet zijn geïmplementeerd, of bestaande technologische oplossingen, maar niet gereguleerd door enige documentatie), kiest de AED de laagste volwassenheidsniveau van de twee.

Tabel 1 bevat voorbeelden van kwalitatieve beschrijvingen voor toegangscontrole.

Tabel 1: Voorbeelden van beschrijvingen voor toegangscontrole

Niveau	Definitie van het volwassenheidsniveau	Getroffen beheersmaatregelen
1	**Initieel**	Uit interviews blijkt dat beheerders het gebruik dienen te verantwoorden in een Word-document. Dit is niet vastgelegd in een procedure. De inspecteur stelt op basis van logging vast dat het Word-document niet volledig is. Enkele beheerders verantwoorden het gebruik namelijk niet.
2	**Herhaalbaar maar informeel**	De beheerders delen een anoniem beheeraccount. Uit interviews blijkt dat beheerders het gebruik dienen te verantwoorden in een Word-document. Dit is niet vastgelegd in een procedure. De inspecteur stelt op basis van logging vast dat het Word-document juist en volledig is.
3	**Gedefinieerd**	Beheerders gebruiken een persoonlijk account. De noodzaak van beheerrechten dat het beheeraccount heeft, is toegelicht in een document dat is vastgesteld en geaccordeerd door het management. Op basis van een periodiek controle stelt de manager vast of de beheerders nog de juiste rechten hebben. De manager rapporteert de uitkomst van de controle in zijn kwartaalrapportage aan het senior management.
4	**Beheerst en meetbaar**	Conform de procedure evalueert de manager jaarlijks of de noodzaak van beheerrechten nog actueel is. Het bespreekt dit overzicht met de beheerders en legt de resultaten van deze bespreking vast. Het versiebeheer van het document met de noodzaak van beheerrechten wordt bijgewerkt.
5	**Continu verbeteren**	Het logische toegangsbeveiligingsproces maakt onderdeel uit van het risk management proces van de organisatie. Middels het 3 lines of defence model worden maatregelen ieder kwartaal getoetst en verantwoord. Uit de verantwoording blijkt dat wijzigingen in functies en uitdiensttreding tijdig worden verwerkt. De kan doordat de manager de wijzigingen van HR al voorafgaand aan de uitvoering (wijzigen functie / uitdienst) al ontvangt.

Belangrijk om nogmaals te benadrukken dat het doel van dit assessment niet is om een bepaald BBNI-volwassenheidsniveau te behalen, maar om verbeterpunten te identificeren waar de AED zich op korte / middellange termijn op zal richten. Daarom zal de nadruk vooral liggen op de kwalitatieve beschrijvingen.

5. RESULTATEN VAN HET ASSESSMENT

De beoordelingsresultaten worden gerapporteerd aan Agentschap Telecom volgens deze werkwijze:

- Het te verzenden bestand is een Excel-bestand waarin de tool volledig is ingevuld, met bestandsnaam: BBNI_Self-Assessment_v1.00_ [AED-naam] _ [Datum].xlsx;
- Om de vertrouwelijkheid te waarborgen, zal het bestand worden geencrypt , bijvoorbeeld met 7-Zip;
- Het bestand wordt geüpload met behulp van de Agentschap Telecom Inforportaal;
- Het bestand moet 30 dagen vóór de geplande inspectiedatum opgeleverd zijn aan Agentschap Telecom.

6. ONDERSTEUNING

Ondersteuningsverzoeken worden ingediend bij de contactpersoon binnen Agentschap Telecom.

Voortgang

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Ga naar de volgende vraag

BBNI		ISO 27001	Vragen voor AED	AED Antwoorden
BBNI Domeinen	**Omschrijving van de BBNI Domeinen**	**Titel**	**Vragen**	**Kwalitatief**
Risicogebaseerde Aanpak	De aanbieder heeft een actueel overzicht van de netwerk- en informatiesystemen die zijn essentiële dienst ondersteunen. De aanbieder stelt een risicoanalyse op met inachtneming van de relevante normen en ontwikkelingen. In de analyse beschrijft hij de risico's en de wijze waarop hij de risico's tot een aanvaardbaar niveau verkleint. Hij motiveert waarom dit niveau proportioneel en aanvaardbaar is. Hierbij houdt hij niet alleen rekening met de organisatie-specifieke en sectorspecifieke risico's, maar ook met het maatschappelijke belang van zijn essentiële dienst en met de stand van de techniek. Hij zorgt ervoor dat de resultaten van de risicoanalyse inzichtelijk en toetsbaar zijn en hij verwerkt de resultaten in risicogerichte beveiligings- en beheersmaatregelen.	Verantwoordelijkheid voor Bedrijfsmiddelen	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de centrale vastlegging van de inventaris 2. de actualiteit van de vastlegging 3. het eigenaarschap van de bedrijfsmiddelen 4. het juist gebruiken van de bedrijfsmiddelen	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Informatieclassificatie	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop classificatie van informatie heeft plaats gevonden 2. de vastlegging van de classificatie 3. de wijze waarop informatie conform de classificatie gelabeld is 4. de maatregelen die getroffen zijn om de geclassificeerde informatie te hanteren, verwerken en te communiceren	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Behandelen van Media	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop geclassificeerde informatie wordt beheert over de gehele levenscyclus van bedrijfsmiddelen	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Risicobeoordeling van Informatiebeveiliging	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop informatiebeveiliging in het risicomanagement is geïntegreerd. 2. de wijze waarop informatiebeveiligingsrisico's worden geidentificeerd, geanalyseerd en geëvalueerd.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Behandeling van Informatiebeveiligingsrisico's	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop beheersmaatregelen worden vastgesteld en implementatie wordt geborgd.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

		Context van de Organisatie	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. De manier waarop de sociale en economische impact van het bedrijf op internationaal, nationaal en lokaal niveau wordt meegenomen in het informatiebeveiligingsbeheersysteem. 2. De manier waarop de behoeften, verwachtingen en regelgeving van internationale, nationale en lokale belanghebbenden worden meegenomen in het beheersysteem voor informatiebeveiliging 3. De reikwijdte van het informatiebeheersysteem, rekening houdend met eerdere onderwerpen.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Leiderschap	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. De manier waarop het topmanagement blijk geeft van betrokkenheid bij het informatiebeveiligingsbeheersysteem 2. De manier waarop het informatiebeveiligingsbeleid is uitwerkt, gepubliceerd en is onderhouden 3. De manier waarop de rollen en verantwoordelijkheden zijn toegewezen om de juiste implementatie en beheer van het informatiebeveiligingsbeheersysteem te waarborgen	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Informatiebeveiligingsdoelstellingen en Planning om Deze te Bereiken	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de manier waarop informatiebeveiligingsdoelstellingen en de plannen om deze te bereiken realistisch en meetbaar zijn, middelen zijn toegewezen, zijn gecommuniceerd, waar nodig bijgewerkt en gebaseerd zijn op een risico analyse. 2. de wijze waarop beleidsregels tot stand zijn gekomen, goedgekeurd, gepubliceerd en gecommuniceerd. 3. de waarborgen dat het beleid voortdurend passend, adequaat en doeltreffend is.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Ondersteuning	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de manier waarop middelen en competenties worden toegewezen aan het opzetten, implementeren, onderhouden en continu verbeteren van het informatiebeveiligingsbeheersysteem 2. de manier waarop relevante medewerkers op de hoogte zijn gebracht van het informatiebeveiligingsbeleid 3. de manier waarop interne en externe communicatie omtrent informatiebeveiliging wordt afgehandeld 4. de manier waarop alle benodigde informatiebeveiligingsdocumentatie wordt gemaakt, bijgewerkt en wordt beheerd.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

Organisatie van netwerk en Informatiebeveiligingsbeheer	De aanbieder zorgt voor het opstellen, uitvoeren, handhaven, bewaken en uitdragen van een informatiebeveiligingsbeleid op basis van de relevante normen en de stand der techniek. Hij heeft een informatiebeveiligingsstrategie die in lijn is met zijn strategische doelen en met het maatschappelijke belang van zijn essentiële dienst. Hij heeft de taken, bevoegdheden en verantwoordelijkheden voor de beveiliging en beheer van zijn netwerk- en informatiesystemen duidelijk in de organisatie belegd.	Uitvoering	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de manier waarop het plan om te voldoen aan de informatiebeveiligingsdoelstellingen is geïmplementeerd, inclusief risicobeoordelingen en risicobehandelingsplannen.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Prestatie-evaluatie	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de manier waarop het bedrijf een informatiebeveiligingsbeheerssysteem onderhoudt en verbetert, inclusief interne audits en periodieke management reviews.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Verbetering	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de manier waarop het bedrijf de geschiktheid, adequaatheid en doeltreffendheid van de informatiebeveiligingsbeheerssysteem voortdurend verbetert, inclusief de manier waarop het omgaat met non-conformiteiten.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Aansturing Door de Directie van de Informatiebeveiliging	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop beleidsregels tot stand zijn gekomen, goedgekeurd, gepubliceerd en gecommuniceerd. 2. de waarborgen dat het beleid voortdurend passend, adequaat en doeltreffend is en op welke wijze verantwoording wordt afgelegd.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Interne organisatie	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de rollen en verantwoordelijkheden voor informatiebeveiliging zijn gedefinieerd en toegewezen. 2. de scheiding tussen conflicterende takenwordt toegepast waar het risico bestaat op onbevoegde of onbedoelde aanpassing van bedrijfsmiddelen. 3. de wijze waarop informatiebeveiliging in projecten wordt beheerst volgens het beleid voor risicomanagement.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Voorafgaand aan het Dienstverband	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop screening wordt toegepast 2. de wijze waarop in contracten medewerkers en contractanten gewezen worden op informatiebeveiliging	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

		Tijdens het Dienstverband	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de manier waarop security awareness vorm wordt gegeven 2. de wijze waarop is geborgd dat medewerkers en contracten zich aan de informatiebeveiliging houden. 3. de formele en gecommuniceeerde disciplinaire procedure en toepassing hiervan tegen medewerkers en contractanten die inbreuk hebben gepleegd op de informatiebeveiliging	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beëindiging en Wijziging van Dienstverband	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop gewaarborgd wordt dat bij beëindiging van het dienstverband alle toegangsmiddelen worden ingetrokken alsmede alle eigendommen van de organisatie geretouneerd worden.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Bedieningsprocedures en Verantwoordelijkheden	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop wordt gewaarborgd dat sytemen voor hun primaire functies beschikbaar zijn 2. de manier waarop beheer van wijzigingen en capaciteit is ingericht 3. de scheiding tussen ontwikkel-, test-, en acceptatieomgeving en de productieomgeving	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Naleving van Wettelijke en Contractuele Eisen	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop relevante wet- en regelgeving is vastgesteld, gedocumenteerd en actueel wordt gehouden. 2. de wijze waarop registraties in overeenstemming met de relevante wet- en regelgeving	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Informatiebeveiligingsbeoordelingen	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop onafhankelijke beoordeling van informatiebeveiliging wordt uitgevoerd. 2. de frequentie van onafhankelijke beoordeling van informatiebeveiliging.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beheer van Dienstverlening van Leveranciers	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop het monitoren en beoordelen van de dienstverlening van leveranciers plaatsvindt. 2. de verantwoordelijkheden voor het beheer van leveranciersrelaties.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

		Mobiele Apparatuur en Telewerken	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop beleid en ondersteunende beveiligingsmaatregelen, om risico's die het gebruik van bedrijfsmiddelen met zich mee brengen te beheersen, tot stand zijn gekomen en hoe deze geïmplementeerd is	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Bedrijfseisen voor Toegangsbeveiliging	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. welke regels opgesteld zijn voor de toegang tot bedrijfsmiddelen (informatie), deze regels bevatten toegangsbeveiliging, -rechten en beperkingen voor specifieke gebruikersrollen 2. welke regels opgesteld zijn voor toegang tot netwerken en netwerkdiensten 3. de aanwezigheid van kritische functies	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beheer van Toegangsrechten van Gebruikers	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop in-, door-, en uitstroom van medewerkers beheerst wordt 2. de wijze waarop toegang tot systemen ingericht is 3. hoeverre aanvullende maatregelen getroffen zijn voor kritische functies	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Gebruikersverantwoordelijkheden	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. hoeverre geheime authenticatieinformatie van toepassing is binnen de organisatie 2. de wijze waarop bewustwoording tot stand komt bij de gebruikers van deze informatie	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Toegangsbeveiliging van Systeem en Toepassing	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de inlogprocedure tot systemen en toepassingen 2. het systeem van wachtwoordbeheer	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beveiligde Gebieden	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop fysieke beveiligingszones zijn gedefinieerd 2. de maatrgelen die zijn getroffen om deze fysieke beveiligingszones te beschermen, zodanig dat alleen bevoegd personeel toegang krijgt	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

Incidenten Voorkomen	De aanbieder draagt zorg voor een gelaagde beveiligingsstrategie gericht op het adequaat beheersen van risico's voor de netwerk- en informatiesystemen die de essentiële dienst ondersteunen. Onderdeel van deze beveiligingsstrategie vormt onder andere het toepassen van defense in depth en passend lifecycle-, asset- en patchmanagement. Deze en andere maatregelen, zoals identificatie- en toegangsmanagement, zijn op risicoanalyses gebaseerd. De aanbieder is daardoor in staat om tijdig en adequaat om te gaan met geïdentificeerde kwetsbaarheden en dreigingen. Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op voor hem relevante beveiligingsadviezen en dreigingsinformatie beoordeelt hij of gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's tot een aanvaardbaar niveau te reduceren.	Apparatuur	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop is vastgesteld welke kritieke apparatuur beschermd dient te worden 2. de maatregelen die getroffen zijn om verstoring van deze apparatuur te voorkomen en de beveiliging ervan	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Cryptografische Beheersmaatregelen	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop het gebruik van cryptografische maatregelen benaderd is 2. de getroffen maatregelen in lijn zijn met het risico van de informatie die beschermd dient te worden 3. de wijze waarop sleutelbeheer voor cryptografische sleutels is ingericht	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beheer van Netwerkbeveiliging	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de maatregelen die zijn getroffen om de veiligheid van informatie te waarborgen. 2. de maatregelen die zijn getroffen om aangesloten diensten tegen onbevoegde toegang te beschermen. 3. scheiding in netwerken.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Informatietransport	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop informatie wordt uitgewisseld binnen en buiten de organisatie. 2. de maatregelen die zijn getroffen om de beveiliging van informatie tijdens transport te borgen.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Testgegevens	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. De wijze waarop testgegevens worden beveiligd.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beheersing van Operationele Software	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de procedure voor het beheerst in productie brengen van operationele systemen 2. de wijze waarop life-cycle management is ingericht binnen de organisatie 3. de wijze waarop patchmanagement is ingericht binnen de organisatie (inclusief fallback procedure)	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

		Beheer van Technische Kwetsbaarheden	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop alle bedrijfsmiddelen in kaart zijn gebracht 2. de wijze waarop kwetsbaarheden in beeld worden gebracht 3. de maatregelen die zijn getroffen om de risico's op deze kwetsbaarheden te beperken	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beveiligingseisen voor Informatiesystemen	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop de informatiebeveiligingseisen tot stand zijn gekomen. 2. de wijze waarop informatiebeveiligingseisen worden toegepast in de levenscyclus van informatiesystemen. 3. de scope van het proces (maatwerk en standaard producten, vertrouwelijke en openbare producten, nieuwe en bestaande producten, opslag en transacties).	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beveiliging in Ontwikkelings- en Ondersteunende Processen	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop beleid en ondersteunende beveiligingsmaatregelen ten aanzien van ontwikkelprocessen tot stand zijn gekomen 2. de wijze waarop security by design is geborgd. 3. de wijze waarop wijzigingen worden uitgevoerd. 4. de inrichting van de ontwikkelomgeving. 5. de wijze waarop het testproces wordt uitgevoerd.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Overwegingen Betreffende Audits van Informatiesystemen	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de aanwezigheid en inrichting van een interne auditafdeling 2. de aanwezigheid en uitvoering van het auditplan	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Informatiebeveiliging in Leveranciersrelaties	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop beleid en ondersteunende beveiligingsmaatregelen ten aanzien van leveranciersrelaties tot stand is gekomen. 2. de wijze waarop de informatiebeveiligingseisen ten aanzien van leveranciersrelaties worden toegepast. 3. beveiligingsaspecten in leveranciersovereenkomsten. 4. de wijze waarop met onderaannemers wordt omgegaan.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

Detectie en Respons	De aanbieder neemt passende maatregelen om incidenten te kunnen detecteren, analyseren en vastleggen en om hun gevolgen zo veel mogelijk te beperken. Hij monitort structureel relevante netwerk- en informatiesystemen, legt relevante handelingen op die systemen onweerlegbaar vast en bewaart die gegevens lang genoeg om incidenten te kunnen analyseren. Hij houdt hierbij rekening met door de overheid beschikbaar gestelde relevante dreigingsinformatie. Hij hanteert procedures om op consistente en doeltreffende wijze op te treden bij incidenten.	Verslaglegging en Monitoren	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. hoe bepaald is welke systeem- en gebruikersacties vastgelegd en gemonitoord dienen te worden 2. de wijze waarop logging en monitoring ingericht is 3. de wijze waarop de integriteit van logbestanden is gewaarborgd	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Bescherming tegen Malware	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de maatregelen die getroffen zijn tegen malware	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Beheer van informatiebeveiligingsincidenten en -verbeteringen	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop beveiligingsincidenten worden beheert. 2. de rapportage van informatiebeveiligingsgebeurtenissen. 3. de rapportage van zwakke plekken in de informatiebeveiliging. 4. de wijze van classificeren en prioriteren van incidenten 5. de wijze waarop lering uit informatiebeveiligingsincidenten wordt getrokken. 6. de wijze bewijs wordt verzameld ten behoeve van disciplinaire en wettelijke actie.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
Gevolgen van Incidenten Beperken	De aanbieder zorgt voor het opstellen van een bedrijfscontinuïteitsbeleid en een crisismanagementbeleid voor de netwerk- en informatiesystemen. Onderdeel van zijn crisismanagementbeleid is ten minste een plan dat hem in staat stelt de essentiële dienst zo spoedig mogelijk te herstellen na een incident. Het crisismanagementbeleid wordt daartoe periodiek in de praktijk beoefend.	Back-up	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de aanwezigheid van een back-up beleid 2. de wijze waarop back-ups gemaakt worden 3. het testen van de back-up & recovery procedure	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*
		Informatiebeveiligingscontinuïteit	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop de eisen voor de continuïteit zijn vastgesteld. 2. de processen die waarborgen dat de continuïteit tijdens ongunstige situaties is gewaarborgd. 3. de wijze waarop de effectiviteit van beheersmaatregelen periodiek wordt geverifieerd.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

		Redundante Componenten	Ga bij de beoordeling van deze doelstelling ten minste in op: 1. de wijze waarop redundantie is geïmplementeerd om aan de beschikbaarheidseisen te voldoen.	*In te vullen door AED:* ** Waar van toepassing, een beschrijving van de huidige staat van de Governance, inclusief bestaande governance-bewijzen.* ** Waar van toepassing, een beschrijving van de huidige staat van de implementatie, inclusief bestaande bewijzen (zie voorbeelden).* ** Waar van toepassing, een algemene beschrijving hoe het kwalitatief antwoord is gekoppeld aan het kwantitatieve antwoord.*

	Volwassenheidsniveau	
Kwantitatief	**Score**	**Niveau**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**

Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**

Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**

Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**

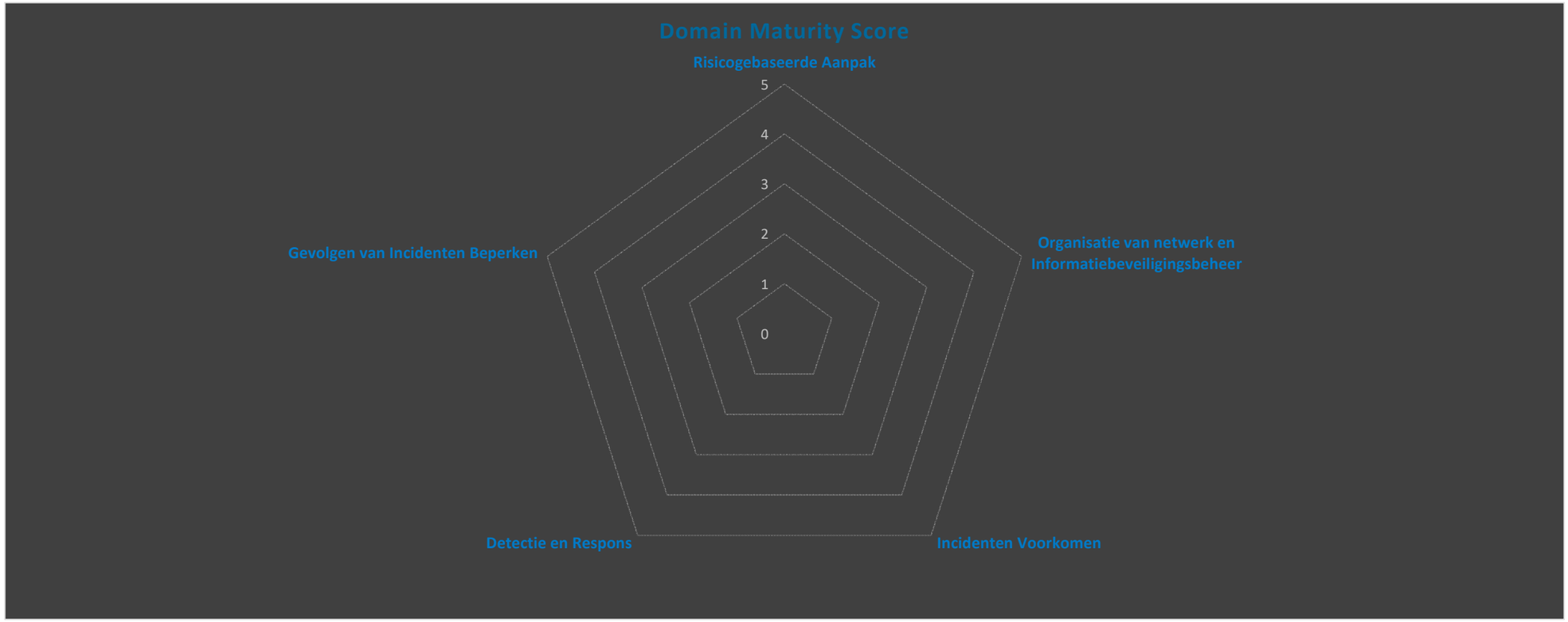
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**

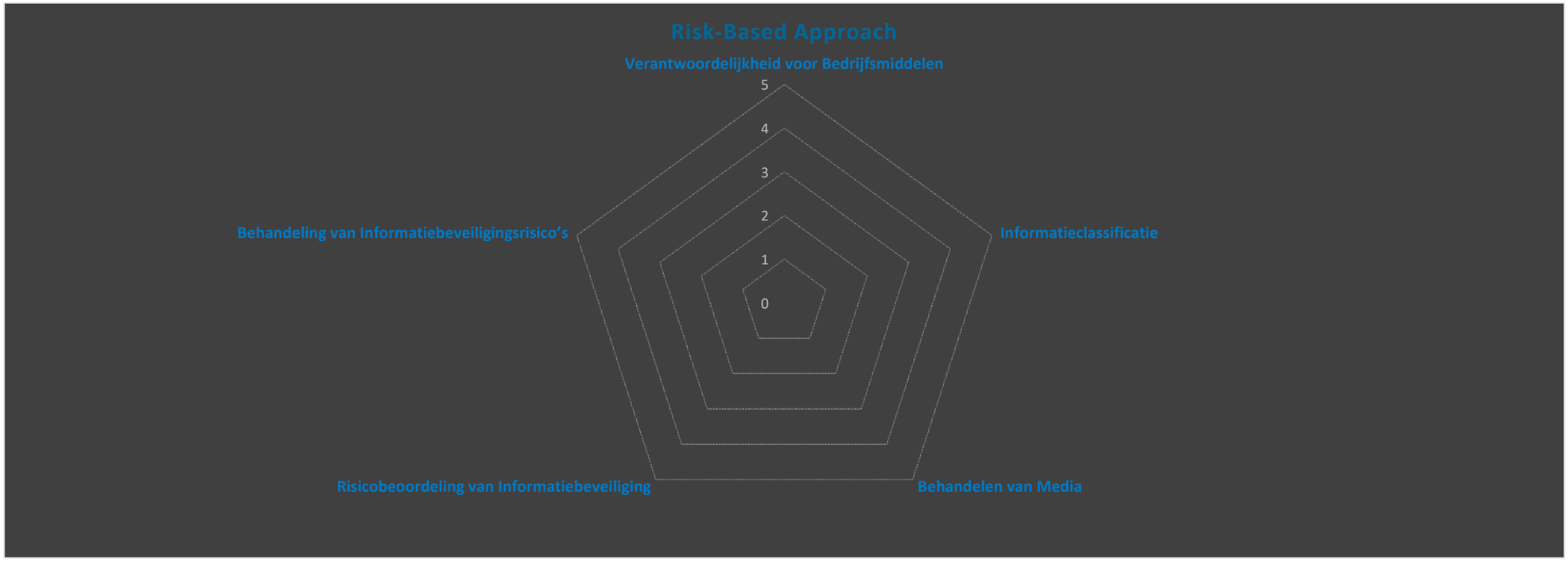
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**

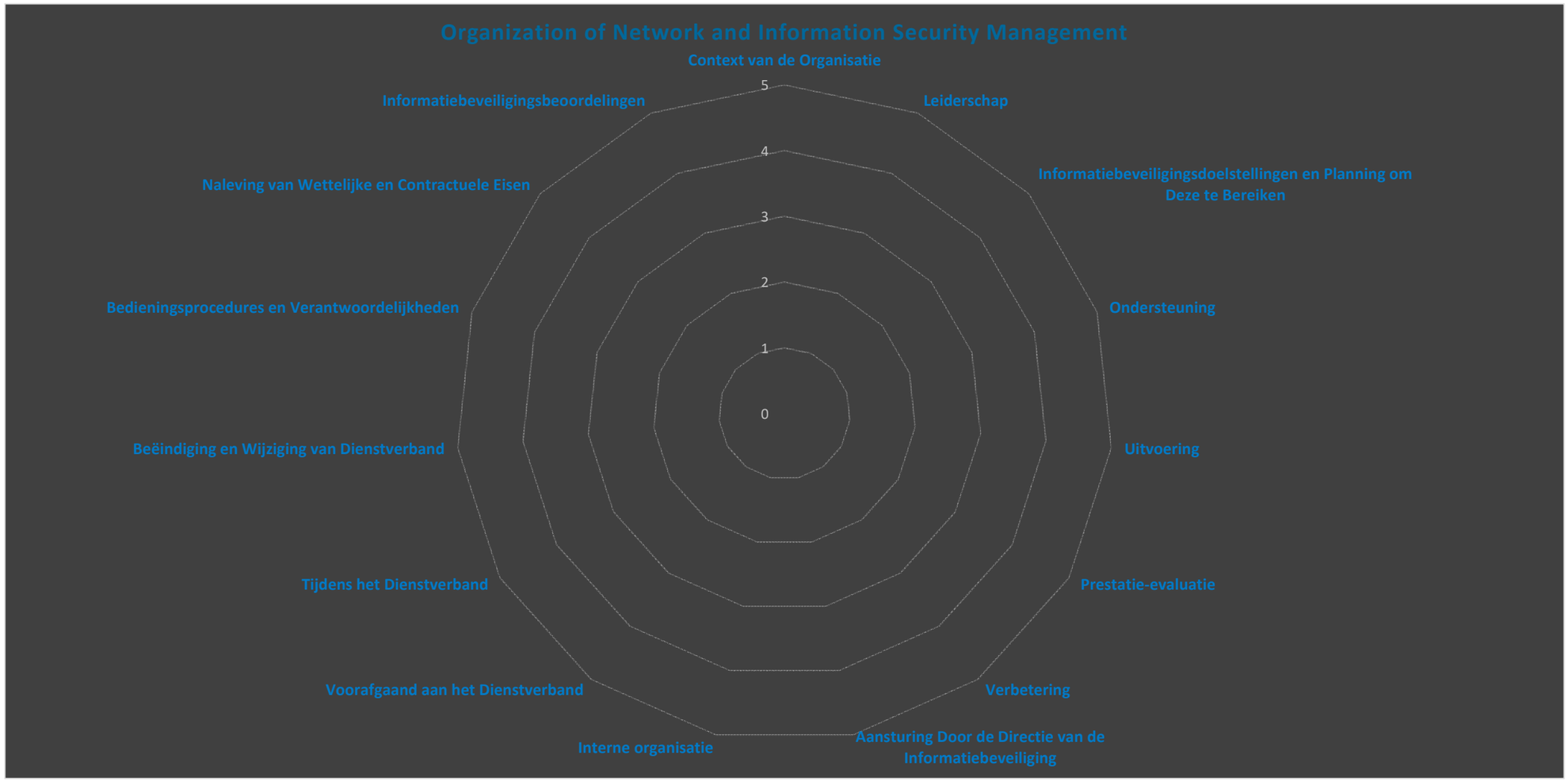
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**

Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**
Er is geen antwoord gegeven.	0	**Onbekend**

Er is geen antwoord gegeven.	0	**Onbekend**


Domain Maturity Score
Risicogebaseerde Aanpak
5
4
3
2
1
0
Organisatie van netwerk en Informatiebeveiligingsbeheer
Incidenten Voorkomen
Detectie en Respons
Gevolgen van Incidenten Beperken


Risk-Based Approach
Verantwoordelijkheid voor Bedrijfsmiddelen
5
4
3
2
1
0
Informatieclassificatie
Behandelen van Media
Risicobeoordeling van Informatiebeveiliging
Behandeling van Informatiebeveiligingsrisico's


Organization of Network and Information Security Management
Context van de Organisatie
Leiderschap
Informatiebeveiligingsdoelstellingen en Planning om Deze te Bereiken
Ondersteuning
Uitvoering
Prestatie-evaluatie
Verbetering
Aansturing Door de Directie van de Informatiebeveiliging
Interne organisatie
Voorafgaand aan het Dienstverband
Tijdens het Dienstverband
Beëindiging en Wijziging van Dienstverband
Bedieningsprocedures en Verantwoordelijkheden
Naleving van Wettelijke en Contractuele Eisen
Informatiebeveiligingsbeoordelingen
5
4
3
2
1
0

BBNI Domeinen	NIST CSF Domeinen	ISO27001	IEC 62443-2-1	IEC 62443-3-3
Risicogebaseerde Aanpak	Identify	A.8.1	4.2.3.4	SR7.8
		A.8.2	4.3.2.3.3	
		A.8.3	NA	
		6.1.2	4.2.3 4.2.3.7 4.2.3.9 4.2.3.12	
		6.1.3	5.2.1	
Organisatie van netwerk en Informatiebeveiligingsbeheer		Clause 4		
		Clause 5		
		Clause 6.2		
		Clause 7		
		Clause 8		
		Clause 9		
		Clause 10		
		A.5.1	ORG 1.1 ORG 1.2	
		A.6.1	ORG 1.1 USER 1.5 ORG 2.3	
		A.7.1	ORG 1.1 ORG 1.2	
		A.7.2	ORG 1.1 ORG 1.3 ORG 1.4	
		A.7.3	USER 1.2	
		A.12.1	ORG 1.1 CM 2.2 AVAIL 1.2 ORG 3.1	
		A.18.1	ORG 1.1 DATA 1.1 DATA 1.2 DADTA 1.7	

		A.18.2	ORG 1.1 EVENT 1.9	
Incidenten Voorkomen		A.15.2	ORG 1.1	FR-1 (All System Requirements) SR 2.1 SR 2.2 SR 2.3 SR 2.4 SR 2.5 SR 2.6 SR 2.7 FR-3 (All System Requirements except 3.7) FR-4 (All System Requirements) FR-5 (All System Requirements) SR 7.6 SR 7.7
	Protect	A.6.2	COMP 1.1 DATA 1.2	
		A.9.1	USER 1.4 USER 1.5	
		A.9.2	USER 1.4	
		A.9.3	DATA 1.1	
		A.9.4	USER 1.4 USER 1.5 USER 1.9 USER 1.13	
		A.11.1	ORG 3.1	
		A.11.2	ORG 1.1 ORG 1.3 ORG 3.1 COMP 1.1 AVAIL 1.2	
		A.10.1		
		A.13.1		
		A.13.2		
		A.14.3		
		A.12.5		
		A.12.6		
		A.14.1		
		A.14.2		
		A.12.7		
		A.15.1		
Detectie en Respons	**Detect**	A.12.4		SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.4
		A.12.2		

	Respond	A.16.1		SR 3.7 SR 6.1 SR 6.2
Gevolgen van Incidenten Beperken	**Recover**	A 12.3		SR 5.1 SR 5.2 SR 5.4 SR 7.1 SR 7.2 SR 7.3 SR 7.4 SR 7.5
		A.17.1		
		A.17.2		

Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

Team Wbni

Van

5.1.2.e
5.1.2.e

T

Datum
Mei 2021

Bijlagen
1: flowchart
2: versiebeheer

memo

Procesbeschrijving reguliere inspectie

In deze memo is het proces "reguliere inspectie" uitgeschreven. Reguliere inspecties worden ééns per twee jaar uitgevoerd. Het doel van deze inspectie is om een totaalbeeld te verkrijgen van de mate van volwassenheid van de informatiebeveiliging, waarbij middels een deelwaarneming ingezoomd wordt op een aantal beheersdoelen en rekening wordt gehouden met bevindingen uit de inventarisatie nieuwe AED's en eventueel eerder uitgevoerde inspecties. Om deze inspecties uit te voeren wordt gebruik gemaakt van de volgende documenten:

- Sjabloonbrief aankondiging inspectie;
- Self assessment;
- Volledig toetsingskader voor intern gebruik;
- Standaard rapport reguliereinspectie; en,
- Samenvatting bevindingen.

De inspecties worden door twee inspecteurs uitgevoerd: één inspecteur met auditachtergrond en de andere met een IB-achtergrond. Stem per duo af wie welke taken voor zijn rekening neemt. De planning van de inspecties vindt plaats op basis van de jaarplanning. In de bijlage worden de stappen grafisch weergegeven.

Samenvatting handelingen
Het doel is om een algemeen beeld van de mate van informatiebeveiliging van de essentiële dienst van de AED te verkrijgen. Hiervoor wordt deze gevraagd om de self assessment in te vullen, waarbij hem ook wordt gevraagd om een volwassenheidsscore aan te geven. Na bestudering van het teruggestuurde kader volgt een inspectie waarbij op een aantal beheersdoelen dieper wordt ingegaan en beoordeeld wordt of het toegekende volwassenheidsniveau correct is.

Aanmaken opslaglocatie en klaarzetten documentatie
Maak een directory aan op de buiten reikwijdte[1] waar alle stukken van de inspectie worden opgeslagen. Zet in de directory alle standaarddocumenten klaar die voor de inspectie nodig zijn en pas ze aan voor de inspectie (hernoemen, etc.). Let op dat de originele documenten ongewijzigd blijven.

[1] buiten reikwijdte

Aankondigen van de inspectie
Kondig de inspectie aan met een brief. Stel deze op, laat hem ondertekenen door het afdelingshoofd en verstuur deze per mail. Tip: licht de komst van de brief eerst mondeling toe in bijvoorbeeld het accountmanagementgesprek.

Opsturen self assessement
Neem contact op met de contactpersoon van de AED om het doel van de inspectie toe te lichten. Maak daarbij afspraken over de termijn waarbinnen de AED de self assessment ingevuld retourneert. Licht de contactpersoon in over de mogelijkheid om de assessment via het infoportal terug te zenden. Als de contactpersoon nog niet is toegevoegd in je infoportal[2] account: voeg deze toe. Bereid de contactpersoon ook voor op het vervolgtraject als de self-assessment ontvangen is.

Gebruik van informatie uit certificeringstrajecten door de AED[3]
Als de AED een (ISO) certificeringstraject heeft doorlopen dan is deze vrij om de informatie uit de certificering te gebruiken bij het invullen van het toetsingskader. Uiteraard moet het certificeringstraject in dat geval zien op de levering van de essentiële dienst. Hij kan hiertoe verwijzingen naar het auditrapport opnemen. Voorwaarde is dan wel dat het auditrapport mee wordt gestuurd als bijlage bij het ingevulde toetsingskader. Een certificering kan niet gebruikt worden ter vervanging van de reguliere inspectie.

Ontvangst self assessment en bestuderen resultaten
Bewaak de datum waarop de AED de self assessment terugstuurt naar AT. Bestudeer het ingevulde self assessment en controleer of alle onderdelen zijn ingevuld. Verzoek eventueel de AED om het self assessment volledig in te vullen.

Selecteren beheersdoelen
In deze stap worden beheersdoelen geselecteerd die tijdens de aankomende inspectie dieper worden behandeld. Op deze deelwaarneming wordt tijdens de inspectie dieper ingegaan. Tijdens de review wordt nagegaan of het volwassenheidsniveau dat de AED heeft aangegeven gestaafd kan worden met bewijsmateriaal en of de evidence de doelstelling afdekt.

De gekozen beheersdoelen worden niet alleen bepaald door de self-assessment, maar ook (onder andere) door de uitkomsten van de eerder uitgevoerde risico-analyse, actuele ontwikkelingen. Leg de keuzes die zijn gemaakt om tot de beheersdoelen te komen duidelijk vast in het volledig toetsingskader.

De AED wordt vooraf niet ingelicht over de beheersdoelen waar we dieper op ingaan tijdens de inspectie. Wel kan hem worden medegedeeld dat we op een aantal onderwerpen dieper ingaan zodat hij zich kan voorbereiden.

Licht AED in
Sluit de voorbereiding af door een afspraak te maken met de contactpersoon van de AED voor een datum waarop de review plaats gaat vinden en bevestig dit per mail. Leg in de mail nogmaals uit wat van hem verwacht wordt.

Uitvoeren review

---

[2] Als je nog geen account hebt: neem zsm contact op met 5.1.2.e .
[3] buiten reikwijdte

Denk bij het uitvoeren van de review aan de volgende aandachtspunten.

- Stel jezelf de vraag of de gekozen combinatie van evidence de doelstelling in voldoende mate afdekt;
- Beoordeel of het aangegeven volwassenheidsniveau dat de AED voor zichzelf heeft aangevinkt overeenkomt met aangetroffen evidence; en,
- Maak afspraken over eventuele acties die worden geformuleerd tijdens de inspectie.

Mogelijk kan de review niet in één keer worden uitgevoerd, maak in dat geval afspraken over de vervolgaanpak.

Gebruik meerdere bronnen
Hanteer voor het reviewen van de geselecteerde beheerdoelen naast het interview met de contactpersoon altijd minimaal één extra bron voor het verzamelen van evidence. Denk aan combinaties als een interview + procesbeschrijving, een interview + schermafdruk of een interview + eigen waarneming. Bepaal op voorhand welke evidence volstaat. Verzamel alleen evidence voor de deelwaarneming.

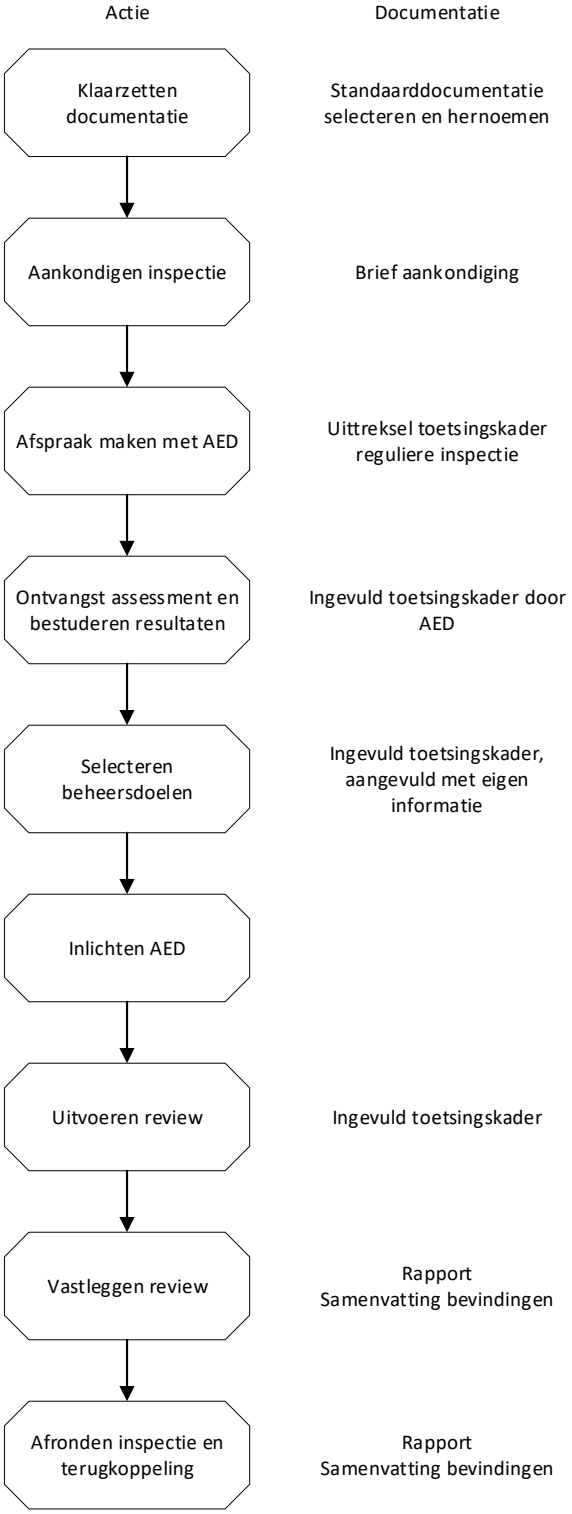
Informatiebeveiligingseisen verwerkte informatie
Tijdens deze fase wordt informatie verwerkt die op hoger niveau zijn geclassificeerd dan het standaardniveau dat wordt geleverd in de 5.1.1.b [redacted]. Houd daarom vooraf rekening hoe om te gaan met stukken die je mee wilt nemen. Met name stukken die op Stg-C zijn geclassificeerd behoeven extra aandacht. Een oplossing is om alleen die onderdelen in te zien die voor nu relevant zijn en in het verslag een verwijzing op te nemen. Het is aan de inspecteurs om een goede afweging te maken.

Herleidbaarheid
Bij gebruik van evidence duidelijke verwijzingen maken naar documenten en de relevante onderdelen in een document. Gebruik het volledig self assessment om de verwijzingen op te nemen.

Vastleggen review
Leg vervolgens de bevindingen vast in het inspectie rapport. Stem de bevindingen af met de contactpersoon. Stuur deze daartoe een samenvatting van de bevindingen en verwerk zijn commentaar. Deze wordt vastgesteld door de inspecteur. Gebruik in deze stap de sjablonen standaardrapport en samenvatting bevindingen.

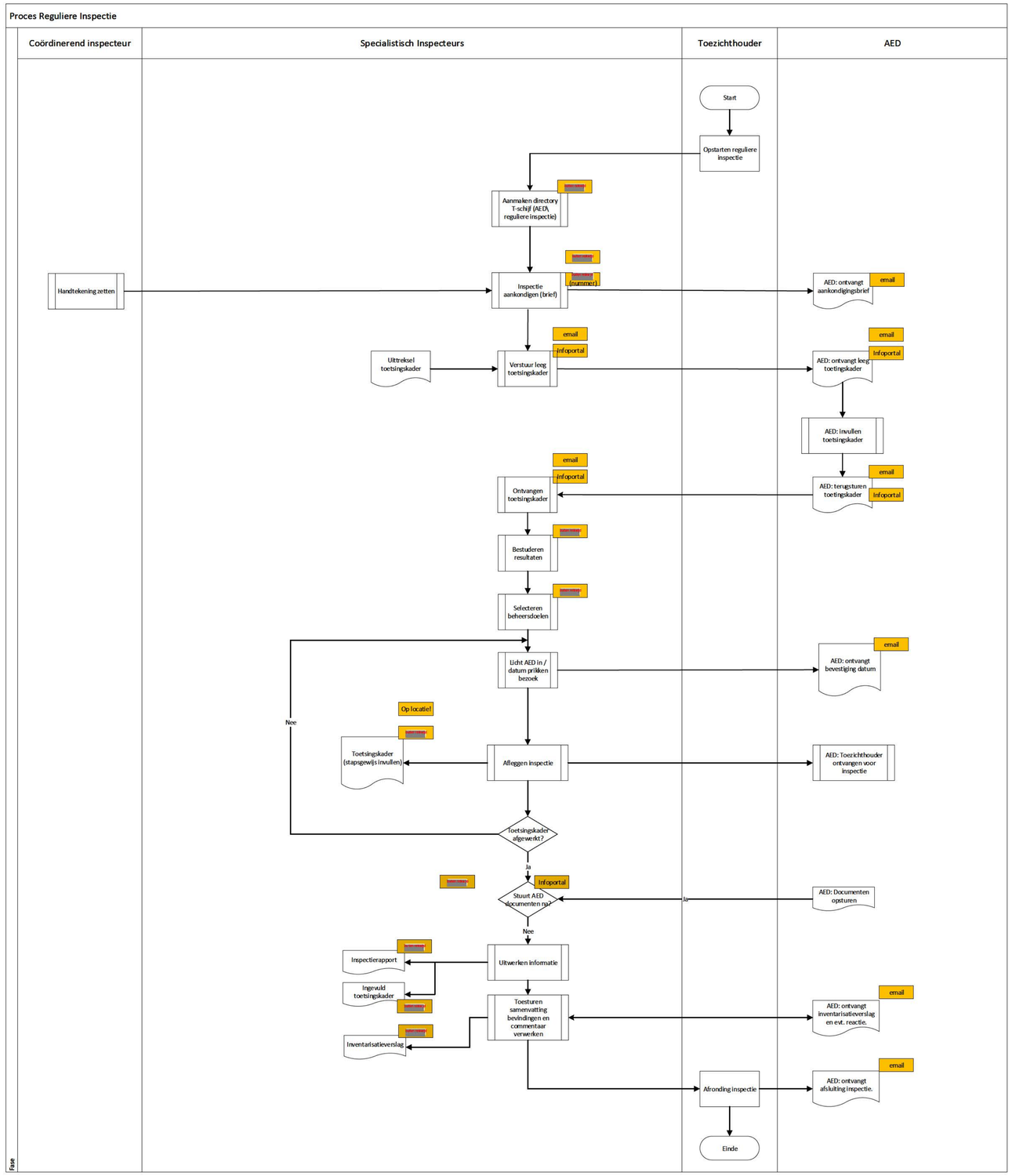
Afronden inspectie en terugkoppeling
Koppel afsluitend, na verwerken van het commentaar, de resultaten terug naar de AED. Zorg er tevens voor dat alle relevante documentatie is opgeslagen, inclusief de e-mailberichten van en naar de AED.

Bijlage: grafische weergave stappen



Bijlage: versiebeheer

Versie	Datum	Wijzigingen door	Gewijzigd
1.0	Februari 2020	5.1.2.e [redacted], 5.1.2.e [redacted] en 5.1.2.e [redacted]	Eerste opzet
1.1	April 2021	5.1.2.e [redacted] en 5.1.2.e [redacted]	Verwerken nieuwe inzichten t.a.v. self assessment en deelwaarneming
1.2	Mei 2021	5.1.2.e [redacted] en 5.1.2.e [redacted]	Verwerken standpunt t.a.v. certificering


Proces Reguliere Inspectie
Coördinerend inspecteur
Specialistisch Inspecteurs
Toezichthouder
AED
Start
Opstarten reguliere inspectie
Aanmaken directory T-schijf (AED\ reguliere inspectie)
Handtekening zetten
Inspectie aankondigen (brief)
(nummer)
AED: ontvangt aankondigingsbrief
email
Uittreksel toetsingskader
Verstuur leeg toetsingskader
Infoportal
AED: ontvangt leeg toetingskader
AED: invullen toetsingskader
AED: terugsturen toetingskader
Ontvangen toetsingskader
Bestuderen resultaten
Selecteren beheersdoelen
Licht AED in / datum prikken bezoek
AED: ontvangt bevestiging datum
Nee
Op locatie!
Toetsingskader (stapsgewijs invullen)
Afleggen inspectie
AED: Toezichthouder ontvangen voor inspectie
Toetsingskader afgewerkt?
Ja
Stuurt AED documenten na?
AED: Documenten opsturen
Nee
Inspectierapport
Uitwerken informatie
Ingevuld toetsingskader
Toesturen samenvatting bevindingen en commentaar verwerken
AED: ontvangt inventarisatieverslag en evt. reactie.
Inventarisatieverslag
Afronding inspectie
AED: ontvangt afsluiting inspectie.
Einde
Fase

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Bedrijfsnaam B.V.
T.a.v. de heer/mevrouw xxx
Straatnaam
Postcode Plaats

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.rdi nl

Contactpersoon
<naam van de lead inspecteur>
<functie>
Toezicht Wbni
T 06-<nummer>

Datum
xx-xx-20xx

Ons kenmerk
RDI
xx-20xx-x1-x

Met opmerkingen [5.1.2 e]: Opvragen bij 5.1.2 f

Betreft: Aankondiging reguliere inspectie 20xx

Geachte heer/mevrouw

<Bedrijfsnaam> is een aangewezen aanbieder van essentiële diensten (hierna: AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Rijksinspectie Digitale Infrastructuur (hierna: RDI) is vanaf 9 november 2018 toezichthouder op deze wet. Wij gaan in het toezicht graag vroegtijdig en open het gesprek met u aan. Zo worden verwachtingen over en weer duidelijk. Met deze brief kondigen wij hierbij dan ook de reguliere inspectie voor het jaar 20xx aan.

Wat is de zorgplicht?
AED's moeten passende en evenredige technische en organisatorische maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen. Om deze reden nemen zij passende maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. Verder melden AED's incidenten met aanzienlijke gevolgen bij RDI en het Nationaal Cyber Security Centrum. Dit betreft de meldplicht.

Wat houdt het toezicht in?
RDI houdt toezicht op de zorgplicht en meldplicht. <Bedrijfsnaam> valt net als andere AED's onder een actief toezichtbeleid: er vinden geplande inspecties plaats gericht op de beoordeling van het risicomanagementproces en de naar aanleiding hiervan getroffen maatregelen. Inspecties vinden risico gebaseerd plaats op basis van ontwikkelingen, signalen en incidenten. Wij benadrukken dat prioriteiten gedurende het jaar kunnen wijzigen naar aanleiding van de actualiteit.

Reguliere Inspectie 20xx
RDI onderkent twee type inspecties, namelijk thema inspecties en reguliere inspecties. Deze aankondiging betreft de twee jaarlijkse reguliere inspectie. Hierbij willen wij ons over de volle breedte van de Wbni beveiligingsdomeinen een beeld vormen over de volwassenheid van de beheerdoelstellingen.

De basis voor deze inspectie zal een self assessment zijn die door uw organisatie zelf ingevuld wordt. Vervolgens voert RDI een deelwaarneming uit om de verantwoording, inclusief de volwassenheid, van de beheerdoelstellingen te toetsen. De deelwaarneming wordt vastgesteld op basis van een risicoanalyse.

Op korte termijn nemen wij contact met u op om afspraken te maken over de planning en uitvoering van de inspectie.

Vragen?
Mocht u naar aanleiding van dit schrijven vragen hebben, kunt u zich wenden tot onze inspecteurs:

- de heer/mevrouw <naam> <functie> (<mail>) en/of
- de heer/mevrouw <naam> <functie> (<mail>).

Met vriendelijke groet,

5.1.2.e
5.1.2.e

Met opmerkingen 5.1.2.e **:** Stem het rapport af met 5.1.2.e of 5.1.2.e.
5.1.2.e zorgt voor een handtekening.

Bijlagen:
Self assessment
Handleiding Self assessment

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Bedrijfsnaam B.V.
T.a.v. de heer/mevrouw xxx
Straatnaam
Postcode Plaats

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.rdi nl

Contactpersoon
<naam van de inspecteur>
<functie>
Toezicht Wbni
T 06-<nummer>

Datum
xx-xx-20xx

Ons kenmerk
RDI
xx-20xx-x1-x

Bijlagen
-

Met opmerkingen [5.1.2.e]: Opvragen bij 5.1.2.e

Betreft: Bevindingen inspecties xxx

Geachte heer/mevrouw

<Bedrijfsnaam> is een aangewezen aanbieder van essentiële diensten (hierna: AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Dit houdt in dat <bedrijfsnaam> maatregelen neemt om incidenten te voorkomen en incidenten met aanzienlijke gevolgen meldt. Rijksinspectie Digitale Infrastructuur (hierna: RDI) is vanaf 9 november 2018 toezichthouder op deze wet. In het kader van de zorgplicht voerden wij recent een inspectie bij uw organisatie uit. Meer informatie over de inspectie kunt u vinden in de aankondigingsbrief van <datum> met kenmerk <kenmerk>. Hierbij rapporteren wij onze bevindingen.

Over welke inspectie gaat deze rapportage?
In <jaar> voerden wij een reguliere inspectie uit op basis van de ingevulde self assessment van <bedrijfsnaam>. RDI heeft op de volgende onderwerpen een deelwaarneming uitgevoerd:

- <deelwaarneming 1>
- <deelwaarneming 2>
- <deelwaarneming 3>

Wat zijn onze bevindingen?
<Omschrijf hier de bevindingen>

Met opmerkingen [5.1.2.e]: Maak een inschatting of het sanctiebureau moet worden ingeschakeld. D t zal het geval zijn indien er aanzienlijke ris co's ten aanzien van de levering van de essentiële dienst worden geconstateerd. Het sanctiebureau kan afdwingen dat opvolging moet plaatsvinden. Neem de zorgpl cht mee in je overwegen. In het geval er geen opvolging plaatsvindt, kan het sanctiebureau op later moment worden ingeschakeld.

Wat is het vervolg?
<Omschrijf hier het vervolg/eventuele afspraken>

Vragen?
Mocht u naar aanleiding van dit schrijven vragen hebben, kunt u zich wenden tot onze inspecteurs:

- de heer/mevrouw <naam> <functie> (<mail>) en/of
- de heer/mevrouw <naam> <functie> (<mail>).

Met vriendelijke groet,

5.1.2.e
5.1.2.e

Met opmerkingen [5.1.2.e]: Stem het rapport af met 5.1.2.e of 5.1.2.e.
5.1.2.e zorgt voor een handtekening.

Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

Enduris B.V.
T.a.v. de heer 5.1.2.e
Postbus 5013
4330 KA Middelburg

Hoofdafdeling Toezicht
Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.agentschaptelecom.nl

Contactpersoon
5.1.2.e
[redacted]
T 06-5.1.2.e

Datum
21-04-2020

Ons kenmerk
AT-EZ/5.1.2.e
ENDU-2020-TI-1-10

Bijlagen
-

Betreft: Aankondiging inspecties 2020

Geachte heer 5.1.2.e,

Enduris B.V. (hierna: Enduris) is aangewezen als Aanbieder van Essentiële Diensten (hierna: AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Dit houdt in dat Enduris maatregelen neemt om incidenten te voorkomen en incidenten met aanzienlijke gevolgen meldt. Agentschap Telecom (hierna: AT) is vanaf 9 november 2018 toezichthouder op deze wet. Wij gaan in het toezicht vroegtijdig en open het gesprek aan. Zo worden verwachtingen duidelijk en weet u waar u aan toe bent. In het kader van de zorgplicht kondigen wij hierbij dan ook de inspecties voor het jaar 2020 aan. Op 24 maart heeft u contact gehad met onze inspecteurs over de afronding van de inventariserende gesprekken die wij met u hebben gevoerd. In dit gesprek hebben wij, onder andere, de inspecties voor 2020 aangekondigd. In deze brief bevestigen wij de besproken onderwerpen.

Wat is de zorgplicht?
AED's moeten passende en evenredige technische en organisatorische maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen. Om deze reden nemen zij passende maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. Verder melden AED's incidenten met aanzienlijke gevolgen bij Agentschap Telecom en het Nationaal Cyber Security Centrum. Dit betreft de meldplicht.

Wat houdt het toezicht in?
Agentschap Telecom houdt toezicht op de zorgplicht en meldplicht. AED's vallen onder een actief toezichtbeleid: er vinden geplande inspecties plaats gericht op de beoordeling van het risicomanagementproces en de naar aanleiding hiervan getroffen maatregelen. Inspecties vinden risico gebaseerd plaats op basis van ontwikkelingen, signalen en incidenten. Wij benadrukken dat prioriteiten gedurende het jaar kunnen wijzigen naar aanleiding van de actualiteit.

Inspecties 2020
Op basis van voorgaande werkzaamheden (kennismaking / inventarisatie) en de actualiteit hebben wij sectorbrede- en AED-specifieke dreigingsanalyses uitgevoerd. Voor elke dreiging hebben wij het risico ingeschat. Wij zijn tot de conclusie gekomen dat het volgende onderwerp aandacht vraagt voor ons toezicht.

Risicomanagement bij overnames
Binnen de Energiesector vinden een aantal overnames plaats. Een overname is niet zonder risico's en onzekerheden. Potentiële valkuilen zoals het voortijdig weglopen van personeel en onvoldoende testen van overgenomen diensten dienen te worden beheerst. DNWG is onlangs overgenomen door Stedin. Vandaar dat wij voor dit onderwerp hebben gekozen.

Planning
U heeft telefonisch aangegeven dat de inspectie kan worden opgestart en zo veel mogelijk op afstand kan worden afgehandeld. Inmiddels hebben wij contact gehad met Stedin over hetzelfde onderwerp. Wij hebben besloten om de inspectie bij hen te beginnen en ons daarna op jullie te richten. U ontvangt van ons tijdig bericht wanneer wij de inspectie bij u willen opstarten.

Vragen?
Mocht u naar aanleiding van deze brief vragen hebben, kunt u zich wenden tot de in het brievenhoofd genoemde contactpersoon.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Toezicht Wbni

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Kick-off inspectie Risicomanagement bij overnames

GTS

Wet beveiliging netwerk- en informatiesystemen (Wbni)

Inspecteurs: 5.1.2.e en 5.1.2.e
Datum: 29-06-2020
Inspectienummer: GASU-2020-TI-1

Inhoud

1. Aankondiging inspectie
2. Wat is onze aanpak?

Aankondiging inspectie

Op 05-06-2020 kondigden wij onze inspecties voor dit jaar 2020 aan (zie brief met kenmerk AT-EZ/ 5.1.2.e).

Deze kick-off sessie is de start van de volgende inspectie:

- Risicomanagement bij overnames

Wat is onze aanpak?

Welke risico's zijn onderkend en hoe zijn deze uitgewerkt in maatregelen.

Risico → Beleid → Proces → Product

In het geval van overnames zoomen we in op de volgende onderwerpen:

- Governance
- Personeel (motivatie en kennis)
- Operationele systemen

Scope van de gesprekken zijn de cyber security risico's.

Eerst een gesprek om de problematiek in kaart te brengen, vervolgens een verdieping.

De inspectie voeren wij uit in de periode juni 2020 tot augustus 2020, naar verwachting zijn we met 2 a 3 gesprekken klaar.

Wat is onze aanpak?

<u>Uitvoering inspectie</u>
Tijdens de inspectie kunnen wij de volgende werkzaamheden uitvoeren:

- het houden van interviews;
- het beoordelen van documenten en processen;
- het reviewen van door de AED uitgevoerde controle werkzaamheden;
- het uitvoeren van eigen deelwaarnemingen;
- het uitvoeren van eigen (visuele) waarnemingen.

Agentschap Telecom biedt u een Client Portal aan waarmee u op een veilige manier informatie met ons kan delen.

Bevindingen naar aanleiding van de inspectie lichten wij aan u toe. Daarbij zult u, door middel van hoor en wederhoor, in de gelegenheid wordt gesteld om desgewenst een nadere toelichting te geven en/of aanvullende informatie aan te leveren.

Wat is onze aanpak?

Afronding inspectie
Op basis van onze werkzaamheden stellen wij een rapportage op. Indien nodig maken wij nadere afspraken over een vervolgtraject. U ontvangt deze rapportage ter informatie.

Wij maken inspectierapporten niet openbaar.

Ten aanzien van de Wet openbaarheid van bestuur (Wob) geldt voor de Wbni een uitzondering: vertrouwelijke gegevens die herleidbaar zijn tot een AED zijn niet op te vragen.

Vragen?

Agentschap Telecom
Ministerie van Economische Zaken

Nederlandse Gasunie N.V.
T.a.v. de heer 5.1.2.e
Postbus 19
9700 MA Groningen
(Verstuurd per mail)

Hoofdafdeling Toezicht
Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.agentschaptelecom.nl

Contactpersoon
5.1 2 e
[redacted]
T 06-5.1.2.e

Datum
20-05-2020

Ons kenmerk
AT-EZ/5.1 2.e
GASU-2020-TI-1-10

Bijlagen
-

Betreft: Aankondiging inspecties 2020

Geachte heer 5.1.2.e ,

Gasunie is een aangewezen aanbieder van essentiële diensten (hierna: AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Dit houdt in dat Gasunie maatregelen neemt om incidenten te voorkomen en incidenten met aanzienlijke gevolgen meldt. Agentschap Telecom (hierna: AT) is vanaf 9 november 2018 toezichthouder op de Wbni. Wij gaan in het toezicht vroegtijdig en open het gesprek aan. Zo worden verwachtingen duidelijk en weet u waar u aan toe bent. Onlangs heeft u contact gehad met onze inspecteurs over de afronding van de eerste ronde inventariserende gesprekken die wij met u hebben gevoerd. In dit gesprek hebben wij, onder andere, de inspecties voor 2020 aangekondigd. In deze brief bevestigen wij de besproken onderwerpen.

Wat zijn de zorgplicht en meldplicht?
AED's nemen passende en evenredige technische en organisatorische maatregelen om hun netwerk- en informatiesystemen te beveiligen. Om deze reden nemen zij maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. Verder melden AED's incidenten met aanzienlijke gevolgen bij AT en het Nationaal Cyber Security Centrum. Dit betreft de meldplicht.

Wat houdt het toezicht in?
AT houdt toezicht op de zorgplicht en meldplicht. AED's vallen onder een actief toezichtbeleid: er vinden geplande inspecties plaats gericht op de beoordeling van het risicomanagementproces en de naar aanleiding hiervan getroffen maatregelen. Inspecties vinden risico gebaseerd plaats op basis van ontwikkelingen, signalen en incidenten. Wij benadrukken dat prioriteiten gedurende het jaar kunnen wijzigen naar aanleiding van de actualiteit.

Inspecties 2020
Op basis van voorgaande werkzaamheden en de actualiteit hebben wij sectorbrede- en AED specifieke dreigingsanalyses uitgevoerd. Voor elke dreiging hebben wij het risico ingeschat. Wij zijn tot de conclusie gekomen dat de volgende twee onderwerpen aandacht vragen voor ons toezicht.

Risicomanagement bij overnames
Binnen de Energiesector vinden een aantal overnames plaats. Een overname is niet zonder risico's en onzekerheden. Potentiële valkuilen zoals het voortijdig weglopen van personeel en onvoldoende testen van overgenomen diensten dienen te worden beheerst. Op dit moment loopt een overname traject waarbij Zebra Gasnetwerk B.V. wordt overgenomen door Gasunie. Vandaar dat wij dit onderwerp voor Gasunie en vervolgens Zebra hebben gekozen.

Detectie, logging en monitoring
Het is in de praktijk zo goed als onmogelijk om indringers buiten de deur te houden met alleen preventieve maatregelen. Goede maatregelen zijn noodzakelijk om onder andere hackaanvallen te detecteren en netwerk- en informatiesystemen dienen faciliteiten te bieden voor logging en monitoring. Randvoorwaardelijk voor deze activiteiten is een betrouwbare inrichting van asset management, segmentering van systemen en een aansluiting op het incident management proces.

Planning
U heeft telefonisch aangegeven dat de inspectie op het thema risicomanagement bij overnames kan worden opgestart en zo veel mogelijk op afstand kan worden afgehandeld. Op korte termijn geven wij graag een presentatie, met een nadere toelichting, aan medewerkers van Gasunie die bij de overname zijn betrokken.

Voor de inspectie detectie, logging en monitoring nemen wij op een later tijdstip contact met u op om deze in de plannen.

Vragen?
Mocht u naar aanleiding van deze brief vragen hebben, kunt u zich wenden tot de in het brievenhoofd genoemde contactpersoon.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Toezicht Wbni

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

40

Kick-off inspectie Risicomanagement bij overnames

Stedin

Wet beveiliging netwerk- en informatiesystemen (Wbni)

Inspecteurs: 5.1.2.e en 5.1.2.e
Datum: 12-05-2020
Inspectienummer: STED-2020-TI-1

Inhoud

1. Aankondiging inspectie
2. Wat is onze aanpak?

Aankondiging inspectie

Op 28-4-2020 kondigden wij onze inspecties voor dit jaar 2020 aan (zie brief met kenmerk AT-EZ/5.1.2.e).

Deze kick-off sessie is de start van de volgende inspectie:

- Risicomanagement bij overnames

Wat is onze aanpak?

Welke risico's zijn onderkend en hoe zijn deze uitgewerkt in maatregelen.

Risico → Beleid → Proces → Product

In het geval van overnames zoomen we in op de volgende twee onderwerpen:

- Personeel (motivatie en kennis)
- Operationele systemen

Eerst een gesprek om de problematiek in kaart te brengen, vervolgens een verdieping.

De inspectie voeren wij uit in de periode mei 2020 tot juli 2020, naar verwachting zijn we met 2 a 3 gesprekken klaar.

Wat is onze aanpak?

<u>Uitvoering inspectie</u>
Tijdens de inspectie kunnen wij de volgende werkzaamheden uitvoeren:

- het houden van interviews;
- het beoordelen van documenten en processen;
- het reviewen van door de AED uitgevoerde controle werkzaamheden;
- het uitvoeren van eigen deelwaarnemingen;
- het uitvoeren van eigen (visuele) waarnemingen.

Agentschap Telecom biedt u een Client Portal aan waarmee u op een veilige manier informatie met ons kan delen.

Bevindingen naar aanleiding van de inspectie lichten wij aan u toe. Daarbij zult u, door middel van hoor en wederhoor, in de gelegenheid wordt gesteld om desgewenst een nadere toelichting te geven en/of aanvullende informatie aan te leveren.

Wat is onze aanpak?

Afronding inspectie
Op basis van onze werkzaamheden stellen wij een rapportage op. Indien nodig maken wij nadere afspraken over een vervolgtraject. U ontvangt deze rapportage ter informatie.

Wij maken inspectierapporten niet openbaar.

Ten aanzien van de Wet openbaarheid van bestuur (Wob) geldt voor de Wbni een uitzondering: vertrouwelijke gegevens die herleidbaar zijn tot een AED zijn niet op te vragen.

Vragen?

Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

Stedin Netbeheer B.V.
T.a.v. mevrouw 5.1.2.e
Postbus 49
3000 AA Rotterdam
(Verstuurd per mail)

Hoofdafdeling Toezicht
Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.agentschaptelecom.nl

Contactpersoon
5.1.2.e
T 06-5.1.2.e

Datum
21-04-2020

Ons kenmerk
AT-EZ/5.1.2.e
STED-2020-TI-1-10

Bijlagen
-

Betreft: Aankondiging inspecties 2020

Geachte mevrouw 5.1.2.e ,

Stedin Netbeheer B.V. (hierna: Stedin) is aangewezen als Aanbieder van Essentiële Diensten (hierna: AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Dit houdt in dat Stedin maatregelen neemt om incidenten te voorkomen en incidenten met aanzienlijke gevolgen meldt. Agentschap Telecom (hierna: AT) is vanaf 9 november 2018 toezichthouder op de Wbni. Wij gaan in het toezicht vroegtijdig en open het gesprek aan. Zo worden verwachtingen duidelijk en weet u waar u aan toe bent. Onlangs heeft u contact gehad met onze inspecteurs over de afronding van de inventariserende gesprekken die wij met u hebben gevoerd. In dit gesprek hebben wij, onder andere, de inspecties voor 2020 aangekondigd. In deze brief bevestigen wij de besproken onderwerpen.

Wat is de zorgplicht onder de Wbni?
AED's moeten passende en evenredige technische en organisatorische maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen. Om deze reden nemen zij passende maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. Verder melden AED's incidenten met aanzienlijke gevolgen bij Agentschap Telecom en het Nationaal Cyber Security Centrum. Dit betreft de meldplicht.

Wat houdt het toezicht van in?
AT houdt toezicht op de zorgplicht en meldplicht. AED's vallen onder een actief toezichtbeleid: er vinden geplande inspecties plaats gericht op de beoordeling van het risicomanagementproces en de naar aanleiding hiervan getroffen maatregelen. Inspecties vinden risicogebaseerd plaats op basis van ontwikkelingen, signalen en incidenten. Wij benadrukken dat prioriteiten gedurende het jaar kunnen wijzigen naar aanleiding van de actualiteit.

Inspecties 2020
Op basis van voorgaande werkzaamheden (kennismaking / inventarisatie) en de actualiteit hebben wij sectorbrede- en AED-specifieke dreigingsanalyses uitgevoerd. Voor elke dreiging hebben wij het risico ingeschat. Wij zijn tot de conclusie gekomen dat de volgende onderwerpen aandacht vragen voor ons toezicht.

Risicomanagement bij overnames
Binnen de Energiesector vinden een aantal overnames plaats. Een overname is niet zonder risico's en onzekerheden. Potentiële valkuilen zoals het voortijdig weglopen van personeel en onvoldoende testen van overgenomen diensten dienen te worden beheerst. DNWG is onlangs overgenomen door Stedin. Vandaar dat wij voor dit onderwerp hebben gekozen.

Detectie, logging en monitoring
Het is in de praktijk zo goed als onmogelijk om indringers buiten de deur te houden met alleen preventieve maatregelen. Goede maatregelen zijn noodzakelijk om onder andere hackaanvallen te detecteren en netwerk- en informatiesystemen dienen faciliteiten te bieden voor logging en monitoring. Randvoorwaardelijk voor deze activiteiten is een betrouwbare inrichting van asset management, segmentering van systemen en een aansluiting op het incident management proces.

Planning
U heeft telefonisch aangegeven dat de inspectie op het thema risicomanagement bij overnames kan worden opgestart en zo veel mogelijk op afstand kan worden afgehandeld. Op korte termijn ontvangt u van ons een presentatie met een nadere toelichting. Deze presentatie lichten we graag toe met medewerkers van Stedin die bij de overname zijn betrokken.

Voor de inspectie detectie, logging en monitoring nemen wij op een later tijdstip contact met u op om deze in de plannen.

Vragen?
Mocht u naar aanleiding van deze brief vragen hebben, kunt u zich wenden tot de in het brievenhoofd genoemde contactpersoon.

Met vriendelijke groet,

5.1.2.e

5.1.2.e

Toezicht Wbni

Toetsingskader

Onderwerp	Subonderwerp		Doelstelling	Goodpractice
6.1 Maatregelen om risico's te beperken en kansen te benutten				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	6.1.1	Algemeen	Bij het plannen voor het managementsysteem voor informatiebeveiliging moet in de context van de organisatie de risico's en kansen worden vastgesteld en aangepakt **(scope overname).**	1. De wijze waarop maatregelen om de risico's te beperken en kansen ten aanzien van de overname te benutten tot stand komen (methodiek). 2. De wijze waarop de maatregelen ten aanzien van de overname in het bestaande risicomanagement proces zijn geïntegreerd (proces). 3. De wijze waarop de doeltreffendheid van deze maatregelen ten aanzien van de overname worden geëvalueerd (evaluatie).
	6.1.2	Risicobeoordeling van informatiebeveiliging	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen **(scope overname).**	1. Risicocriteria ten aanzien van de overname zijn vastgesteld en worden onderhouden. 2. Risico's ten aanzien van de overname zijn onderkend en hebben een risico eigenaar. 3. Risico's ten aanzien van de overname zijn gecategoriseerd op basis van kans en impact. 4. Risico's ten aanzien van de overname zijn geprioriteerd voor risicobehandeling.
	6.1.3	Behandeling van informatiebeveiligingsrisico's	De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren en toepassen **(scope overname).**	**1. Maatregelen voor de beheersing van het risico ten aanzien van de overname zijn vastgelegd.** 2. Een behandelplan voor de beheersing van het risico ten aanzien van de overname is vastgelegd. 3. De risico eigenaren keuren het behandelplan goed en accepteren de restrisico's.

6.1.3.1 Maatregelen voor de beheersing van het risico ten aanzien van de overname zijn vastgelegd.				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	A.6.1	Interne organisatie	Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen **(scope overname).**	1. Rollen en verantwoordelijkheden 2. Scheiding van taken
	A.7.3	Beëindiging en wijziging van dienstverband	Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband **(scope overname).**	1. Beëindiging of wijziging van verantwoordelijkheden van het dienstverband.
	A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren **(scope overname).**	1. Inventariseren van bedrijfsmiddelen. 2. Eigendom van bedrijfsmiddelen. 3. Teruggeven van bedrijsmiddelen.
	A.12.1	Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen **(scope overname).**	1. Procedures en werkinstructies
	A14.1	Analyse en specificatie van informatiebeveiligingseisen	Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus **(scope overname).**	1. Totstandkoming beveiligingseisen. 2. Tussen beide partijen overeengekomen beveiligingseisen. 3. Acceptatiecriteria voor overdracht.
	A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen	Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen. **(scope overname).**	1. Testproces
	A.15.2	Beheer van dienstverlening van leveranciers	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven. **(scope overname).**	1. Overdracht en beëindigen contracten

A.12 Beveiliging bedrijfsvoering				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	A.12.1	Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. **(scope overname).**	12.1.2 Wijzigingenbeheer: - identificeren en registreren - plannen en testen - bepalen impact - goedkeuringsprocedure - verificatie voldoen aan eisen - communiceren - uitwijkprocedure/rollback - noodveranderingsproces - vastlegging verantwoordelijkheden en procedures

Toetsingskader				In te vullen door de inspecteur													
Onderwerp	**Subonderwerp**	**Doelstelling**	**Goodpractice**	Aandachtspunten voor de inspecteur	Interview	Eigen waarneming	Beleid, procedure of instructie	Schermafdruk	Documentatie	Deelwaarneming	Interview verslag	Verslag overige evidence (eigen waarneming, beleid, procedure of instructie, schermafdruk en documentatie)	Afgerond?	Afgestemd met AED	Vereist volwassenheidsniveau	Volwassenheid volgen inspecteur	Eventuele acties naar aanleiding van de inspectie
6.1 Maatregelen om risico's te beperken en kansen te benutten			**Ga bij de beoordeling van deze doelstelling ten minste in op:**														
	6.1.1 Algemeen	Bij het plannen voor het managementsysteem voor informatiebeveiliging moet in de context van de organisatie de risico's en kansen worden vastgesteld en aangepakt **(scope overname).**	1. de wijze waarop maatregelen om de risico's te beperken en kansen ten aanzien van de overname te benutten tot stand komen (methodiek). 2. de wijze waarop de maatregelen ten aanzien van de overname in het bestaande risicomanagement proces zijn geïntegreerd (proces). 3. de wijze waarop de doeltreffendheid van deze maatregelen ten aanzien van de overname worden geëvalueerd (evaluatie).	1. Vraag na welke best practice wordt gebruikt (bv COSO) 2. Stakeholder analyse	■	□	■	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Zie tab 6.1 Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
	6.1.2 Risicobeoordeling van informatiebeveiliging	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen **(scope overname).**	1. Risicocriteria ten aanzien van de overname zijn vastgesteld en worden onderhouden. 2. Risico's ten aanzien van de overname zijn onderkend en hebben een risico eigenaar. 3. Risico's ten aanzien van de overname zijn gecategoriseerd op basis van kans en impact. 4. Risico's ten aanzien van de overname zijn geprioriteerd voor risicobehandeling.	1. Interviewen AED's die de overname doet	■	□	■	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
	6.1.3 Behandeling van informatiebeveiligingsrisico's	De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren en toepassen **(scope overname).**	**1. Maatregelen voor de beheersing van het risico ten aanzien van de overname zijn vastgelegd.** 2. Een behandelplan voor de beheersing van het risico ten aanzien van de overname is vastgelegd. 3. De risico eigenaren keuren het behandelplan goed en accepteren de restrisico's.	1. Vraag na welk systeem wordt gebruikt voor de risicobeheersing (bv Bwise)? 2. Interviewen AED's die de overname doet 3. Vraag de risico-analyse op en beoordeel.	■	□	□	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
6.1.3.1 Maatregelen voor de beheersing van het risico ten aanzien van de overname zijn vastgelegd.			**Ga bij de beoordeling van deze doelstelling ten minste in op:**														
	A.6.1 Interne organisatie	Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen **(scope overname).**	1. Rollen en verantwoordelijkheden 2. Scheiding van taken	1. Overgang van oude naar nieuwe rollen 2. Programma documentatie (Prince)	■	□	□	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
	A.7.3 Beëindiging en wijziging van dienstverband	Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband **(scope overname).**	1. Beëindiging of wijziging van verantwoordelijkheden van het dienstverband.	1. Kennisoverdracht van IT omgeving 2. Motivatie	■	□	□	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
	A.8.1 Verantwoordelijkheid voor bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren **(scope overname).**	1. Inventariseren van bedrijfsmiddelen. 2. Eigendom van bedrijfsmiddelen. 3. Teruggeven van bedrijsmiddelen.	1. Componenten 2. Verbindingen	■	□	□	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
	A.12.1 Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen **(scope overname).**	1. Procedures en werkinstructies	1. Hoe is de kennisoverdracht (werkwijze) gewaarborgd.	■	□	□	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
	A14.1 Analyse en specificatie van informatiebeveiligingseisen	Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus **(scope overname).**	A14.1.1 Analyse en specificatie van informatiebeveiligingseisen: 1. Totstandkoming beveiligingseisen. 2. Tussen beide partijen overeengekomen beveiligingseisen. 3. Acceptatiecriteria voor overdracht.		■	□	■	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:					
	A.14.2 Beveiliging in ontwikkelings- en ondersteunende processen	Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen. **(scope overname).**	1. Testproces	1. Vraag na welke best practice wordt gebruikt (bv TMAP) 2. Parallel draaien	■	□	■	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
	A.15.2 Beheer van dienstverlening van leveranciers	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven. **(scope overname).**	1. Overdracht en beëindigen contracten	1. Overdracht door leveranciers 2. Medewerking leveranciers	■	□	□	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:
A.12 Beveiliging bedrijfsvoering			**Ga bij de beoordeling van deze doelstelling ten minste in op:**														
	A.12.1 Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. **(scope overname).**	12.1.2 Wijzigingenbeheer: - identificeren en registreren - plannen en testen - bepalen impact - goedkeuringsprocedure - verificatie voldoen aan eisen - communiceren - uitwijkprocedure/rollback - noodveranderingsproces - vastlegging verantwoordelijkheden en procedures	Check transitieplan	■	□	□	□	■	□	Datum: Gesproken met: Samenvatting gesprek: Bevindingen inspecteur: Eventuele management reactie:	Verwijzing naar evidence: Bevindingen inspecteur: Eventuele management reactie:	Nee	□	3		Omschrijving: Actiehouder: Deadline:

Agentschap Telecom
Ministerie van Economische Zaken

Zebra Gasnetwerk B.V.
T.a.v. de heer 5.1.2.e
Postbus 24
4600 AA Bergen op Zoom
(Verstuurd per mail)

Hoofdafdeling Toezicht
Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.agentschaptelecom.nl

Contactpersoon
5.1.2.e
T 06-5.1.2.e

Datum
20-05-2020

Ons kenmerk
AT-EZ/ 5.1.2.e
ZEBR-2020-TI-1-10

Bijlagen
-

Betreft: Aankondiging inspecties 2020

Geachte heer 5.1.2.e ,

Zebra Gasnetwerk B.V. (hierna: Zebra) is een aangewezen aanbieder van essentiële diensten (hierna: AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Dit houdt in dat Zebra maatregelen neemt om incidenten te voorkomen en incidenten met aanzienlijke gevolgen meldt. Agentschap Telecom (hierna: AT) is vanaf 9 november 2018 toezichthouder op deze wet. Wij gaan in het toezicht vroegtijdig en open het gesprek aan. Zo worden verwachtingen duidelijk en weet u waar u aan toe bent. Onlangs heeft u contact gehad met onze inspecteurs over de afronding van de eerste ronde inventariserende gesprekken die wij met u hebben gevoerd. In dit gesprek hebben wij, onder andere, de inspecties voor 2020 aangekondigd. In deze brief bevestigen wij de besproken onderwerpen.

Wat zijn de zorgplicht en meldplicht?
AED's moeten passende en evenredige technische en organisatorische maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen. Om deze reden nemen zij passende maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. Verder melden AED's incidenten met aanzienlijke gevolgen bij AT en het Nationaal Cyber Security Centrum. Dit betreft de meldplicht.

Wat houdt het toezicht in?
AT houdt toezicht op de zorgplicht en meldplicht. AED's vallen onder een actief toezichtbeleid: er vinden geplande inspecties plaats gericht op de beoordeling van het risicomanagementproces en de naar aanleiding hiervan getroffen maatregelen. Inspecties vinden risico gebaseerd plaats op basis van ontwikkelingen, signalen en incidenten. Wij benadrukken dat prioriteiten gedurende het jaar kunnen wijzigen naar aanleiding van de actualiteit.

Inspecties 2020
Op basis van voorgaande werkzaamheden en de actualiteit hebben wij sectorbrede- en AED specifieke dreigingsanalyses uitgevoerd. Voor elke dreiging hebben wij het risico ingeschat. Wij zijn tot de conclusie gekomen dat de volgende onderwerpen aandacht vragen voor ons toezicht.

Risicomanagement bij overnames
Binnen de Energiesector vinden een aantal overnames plaats. Een overname is niet zonder risico's en onzekerheden. Potentiële valkuilen zoals het voortijdig weglopen van personeel en onvoldoende testen van overgenomen diensten dienen te worden beheerst. Op dit moment loopt een overname traject waarbij Zebra Gasnetwerk B.V. wordt overgenomen door Gasunie. Vandaar dat wij voor dit onderwerp voor de Gasunie en vervolgens Zebra hebben gekozen.

Planning
U heeft telefonisch aangegeven dat de inspectie kan worden opgestart en zo veel mogelijk op afstand kan worden afgehandeld. Inmiddels hebben wij contact gehad met Gasunie over hetzelfde onderwerp. Wij hebben besloten om de inspectie bij hen te beginnen en ons daarna tot Zebra te wenden. U ontvangt van ons tijdig bericht wanneer wij de inspectie bij u willen opstarten.

Vragen?
Mocht u naar aanleiding van deze brief vragen hebben, kunt u zich wenden tot de in het brievenhoofd genoemde contactpersoon.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Toezicht Wbni

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Kick-off inspectie Risicomanagement bij overnames

Zebra

Wet beveiliging netwerk- en informatiesystemen (Wbni)

Inspecteurs: 5.1.2.e en 5.1.2.e
Datum: 06-07-2020
Inspectienummer: ZEBR-2020-TI-1-10

Inhoud

1. Aankondiging inspectie
2. Wat is onze aanpak?

Aankondiging inspectie

Op 20-05-2020 kondigden wij onze inspecties voor dit jaar 2020 aan (zie brief met kenmerk AT-EZ/5.1.2.e [redacted]).

Deze kick-off sessie is de start van de volgende inspectie:

- Risicomanagement bij overnames

Wat is onze aanpak?

Welke risico's zijn onderkend en hoe zijn deze uitgewerkt in maatregelen.

Risico → Beleid → Proces → Product

In het geval van overnames zoomen we in op de volgende onderwerpen:

- Governance
- Personeel (motivatie en kennis)
- Operationele systemen

Scope van de gesprekken zijn de cyber security risico's.

Eerst een gesprek om de problematiek in kaart te brengen, vervolgens een verdieping.

De inspectie voeren wij uit in de periode september 2020 tot november 2020, naar verwachting zijn we met 2 a 3 gesprekken klaar.

Wat is onze aanpak?

<u>Uitvoering inspectie</u>
Tijdens de inspectie kunnen wij de volgende werkzaamheden uitvoeren:

- het houden van interviews;
- het beoordelen van documenten en processen;
- het reviewen van door de AED uitgevoerde controle werkzaamheden;
- het uitvoeren van eigen deelwaarnemingen;
- het uitvoeren van eigen (visuele) waarnemingen.

Agentschap Telecom biedt u een Client Portal aan waarmee u op een veilige manier informatie met ons kan delen.

Bevindingen naar aanleiding van de inspectie lichten wij aan u toe. Daarbij zult u, door middel van hoor en wederhoor, in de gelegenheid wordt gesteld om desgewenst een nadere toelichting te geven en/of aanvullende informatie aan te leveren.

Wat is onze aanpak?

<u>Afronding inspectie</u>
Op basis van onze werkzaamheden stellen wij een rapportage op. Indien nodig maken wij nadere afspraken over een vervolgtraject. U ontvangt deze rapportage ter informatie.

Wij maken inspectierapporten niet openbaar.

Ten aanzien van de Wet openbaarheid van bestuur (Wob) geldt voor de Wbni een uitzondering: vertrouwelijke gegevens die herleidbaar zijn tot een AED zijn niet op te vragen.

Vragen?

Proces dossierreview:
1. 5.1.2.e voert de dossierreview ten behoeve van de volledigheid uit.
2. 5.1.2.e voeren de dossierreview ten behoeve van de inhoud uit.
3. Het rapport wordt na afronding van alle punten uit 1 en 2 ondertekend door 5.1.2.e (via 5.1.2.e.
4. Na ondertekening en versturen rapport rond 5.1.2.e haar dossierreview af.

Nr	Sub	Onderwerp	Bevindingen reviewer	Reactie inspecteurs
ALGEMEEN				
1	a	De checklist 'volledigheid' (dossierreview door 5.1.2.e) is uitgevoerd (voor zo ver als mogelijk).		
	b	Punten uit de dossierreview van 5.1.2.e zijn afgehandeld.		
UITVOERING				
2	a	Bevindingen zijn eenduidig vastgelegd (het is duidelijk wat de bevindingen zijn).		
	b	Bevindingen zijn aantoonbaar gewogen (wat neem je wel/niet op in het rapport, zie ook onderstaande tabel vanaf regel 20).		
	c	Bevindingen zijn met evidence onderbouwd (verwijzing naar gespreksverslag of andere evidence).		
RAPPORTAGE				
3	a	Bevindingen zijn in het rapport overgenomen (zie 1b).		
	b	Het rapport bevat naast negatieve bevindingen (verbeterpunten) ook een beknopte omschrijving van wat goed gaat (in control), zodat de leze de bevinding kan duiden.		
	c	De geformuleerde actie en planning van een AED op een bevindingen is in het rapport opgenomen.		
4	a	Het rapport bevat geen adviezen.		
	b	Het rapport bevat geen oordelen.		
	c	Het rapport bevat geen conclusie.		
	d	Het rapport bevat geen subjectieve teksten.		

Tabel bij 2b.

	Onderkend AED	Onderkend AT
Weinig impact	Wel opnemen Geen feedback Geen monitoring	Wel opnemen Wel / geen feedback Monitoring account mngt
Veel impact	Wel opnemen Wel feedback Monitoring d.m.v…..	Wel opnemen Wel feedback Monitoring d.m.v…..

Laat de checklist na afronding van de inspectie invullen door 5.1.2.e.
Op basis van de ingevulde checkllist leggen de inspecteurs een reactie in dit document vast.
Te allen tijde moet het dossier minimaal voldoen aan de **vetgedrukte** onderwerpen.

Nr	Sub	Onderwerp	Bevindingen reviewer	Reactie inspecteurs
ALGEMEEN				
1	a	De directory van het dossier is omschreven conform de naamgevingsconventie (202x xx x omschrijving)		
2	a	Het dossier kent de volgende structuur*: 001 Planning 002 Uitvoering 003 Rapportage		
PLANNING				
3	a	In de directory 001 Planning zijn minimaal de volgende documenten opgenomen: **- een ondertekende aankondigingsbrief met RP2000 nummer** - de presentatie voor de kick-off meeting - het te gebruiken toetsingskader **- bewijs dat de aankondigingsbrief is verzonden naar de AED**		
	b	De documenten zijn op de templates van het dummy dossier gebaseerd.		
	c	De documenten bevatten de juiste naamgevingsconventie.		
UITVOERING				
4	a	In de directory 002 Uitvoering zijn minimaal de volgende documenten opgenomen: - het ingevulde toetsingskader - de afstemming van de bevindingen		
	b	De documenten zijn op de templates van het dummy dossier gebaseerd.		
	c	De documenten bevatten de juiste naamgevingsconventie.		
	d	Het ingevulde toetsingskader (of aanvullend document) bevat per norm: - een samenvatting van de resultaten van de uitgevoerde werkzaamheden (interview aangevuld met review documentatie, walkthrough, etc) - een verwijzing naar evidence.		
	e	**Uit de afstemming van de bevindingen (of aanvullend document) blijkt dat 'hoor en wederhoor' met de AED heeft plaatsgevonden.**		
RAPPORTAGE				
5	a	In de directory 003 Rapportage zin minimaal de volgende documenten opgenomen: **- de ondertekende eindrapportage met RP2000 nummer** **- bewijs dat de eindrapportage is verzonden naar de AED**		
	b	Het document is op de templates van het dummy dossier gebaseerd.		
	c	Het document bevat de juiste naamgevingsconventie.		

* Tip: maak eventueel een (of meerdere) map 'Archief' aan om concept versies in op te slaan. Zo is het direct duidelijk wat de definitieve versies van docementen zijn.

BCM Thema inspectie

Laatste update

12-06-2022

Te bespreken

- Wijzigingen in proces
- Status docs
- Kick-off PPT

Handelingen

- Opsturen aankondigingsbrief
- Direct daarna: plannen kick-off
- Voor kick-off: uittreksel van toetsingskader opsturen
- Uitvoeren kick-off: inspectie bespreken
- Voor inspectie:
  - Selectie BIA (inzien totaal en selecteren)
  - Terugsturen naar AT ingevuld toetsingskader door AED
- Inspectie (minimaal 2 x)
- Interne vergelijking resultaten
- Bevindingen bespreken met AED’s

Status producten

- Dummy dossier met NL producten klaar
- Brief NL af => Engelse vertaling aangevraagd
- Normenkader NL af => Engelse versie aangevraagd
- PPT Kickoff NL af => vertalen?
- Toelichting NL af

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Kick-off inspectie Business Continuity management

<AED>

Wet beveiliging netwerk- en informatiesystemen (Wbni)

Inspecteurs: <insp1> <insp2>
Datum: DD-MM-YVYY
Inspectienummer: XXXX-2022-TI-1-BCM

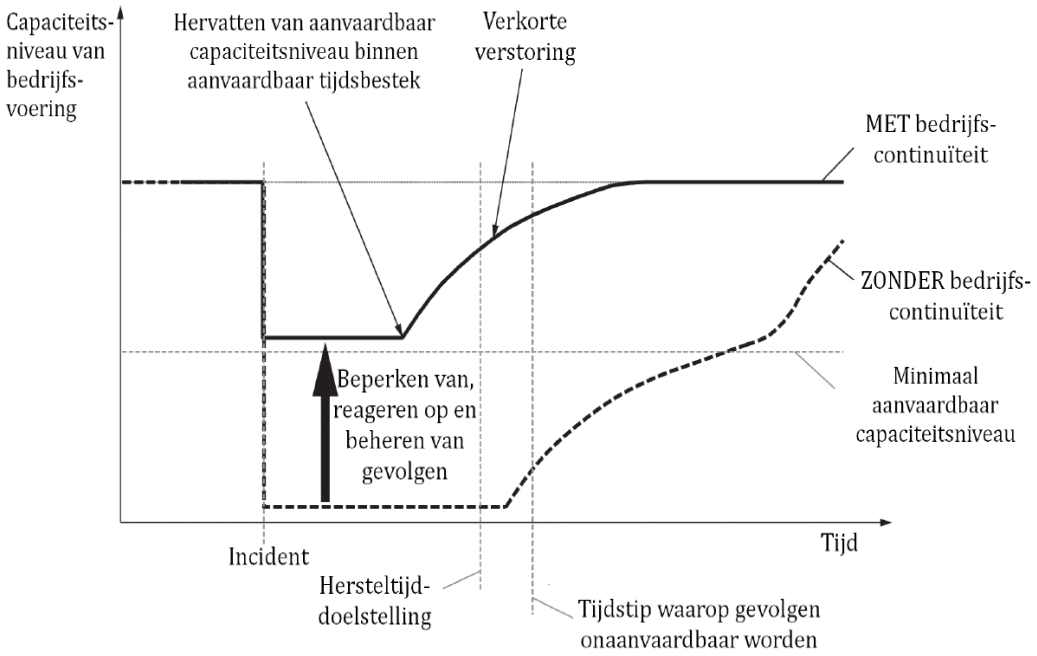
Inhoud

1. Definitie BCM
2. Gehanteerde scope
3. Aanpak
4. Toetsingskader
5. Afspraken

Definitie van BCM

- “De managementprocessen die de continuïteit van de kritische processen van een organisatie waarborgen. De processen zijn erop gericht om de impact van een verstoring te beperken en zo snel mogelijk weer een acceptabel dienstenniveau te bereiken.”
- In dit kader gaat het om de kritische processen, die nodig zijn voor de levering van de essentiële dienst.

- Plaatje uit ISO22313



Gehanteerde scope

In scope zijn de processen, componenten en diensten, die gebruikt worden om de continuïteit bieden aan de levering essentiële dienst te leveren.

Voor BCM zijn ook de onderliggende afhankelijkheden voor een goede werking van de componenten en diensten van belang

- Netwerk- en informatie systemen(ICT)
- Bediening en Beheer (personen)
- Fysieke locatie van systemen en personen incl stroomvoorziening (Loc)
- Leveranciers (Supply chain)

Aanpak

Er worden minimaal 3 sessie gepland:

- Twee sessies voor inspectie
    1. Doorlopen normenkader
    2. Doorlopen processen op basis van BIA en recent incident/test
- Een sessie voor bespreken bevindingen

<u>Voorbereiding</u>

Om de inspectie voor te bereiden vragen we u alvast het toetsingskader in te vullen. Van belang is welke documenten (inclusief pagina/ paragraaf) relevant zijn per control doelstelling.

Samen met de inspecteur wordt gekozen of er eveneens vooraf een onderbouwing van de bestaande controls per doelstelling wordt ingevuld.

Daarnaast wordt u gevraagd voorafgaand aan de inspecties een lijst met BIAs op te sturen.

Aanpak (uitvoering)

<u>Uitvoering inspectie</u>
Tijdens de inspectie kunnen wij de volgende werkzaamheden uitvoeren:

- het houden van interviews;
- het beoordelen van documenten en processen;
- het reviewen van door de AED uitgevoerde controlewerkzaamheden;
- het uitvoeren van eigen visuele/deelwaarnemingen.

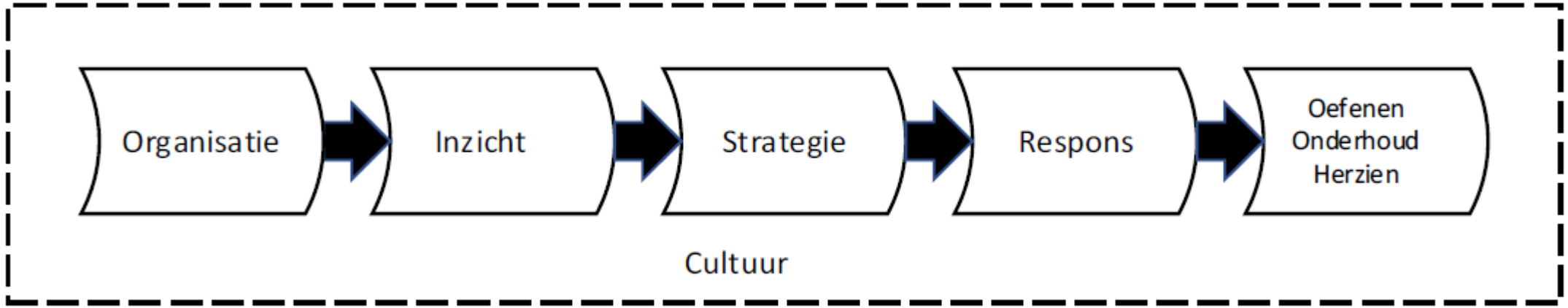
Het toetsingskader is gebaseerd op de ISO-normen voor BCM (ISO 22301 en ISO22313) en gestructureerd naar ISO27001. Tijdens de inspectie wordt vastgesteld of de getroffen maatregelen passend en evenredig zijn.

Bevindingen naar aanleiding van de inspectie lichten wij aan u toe. Daarbij zult u, door middel van hoor en wederhoor, in de gelegenheid wordt gesteld om desgewenst een nadere toelichting te geven en/of aanvullende informatie aan te leveren.

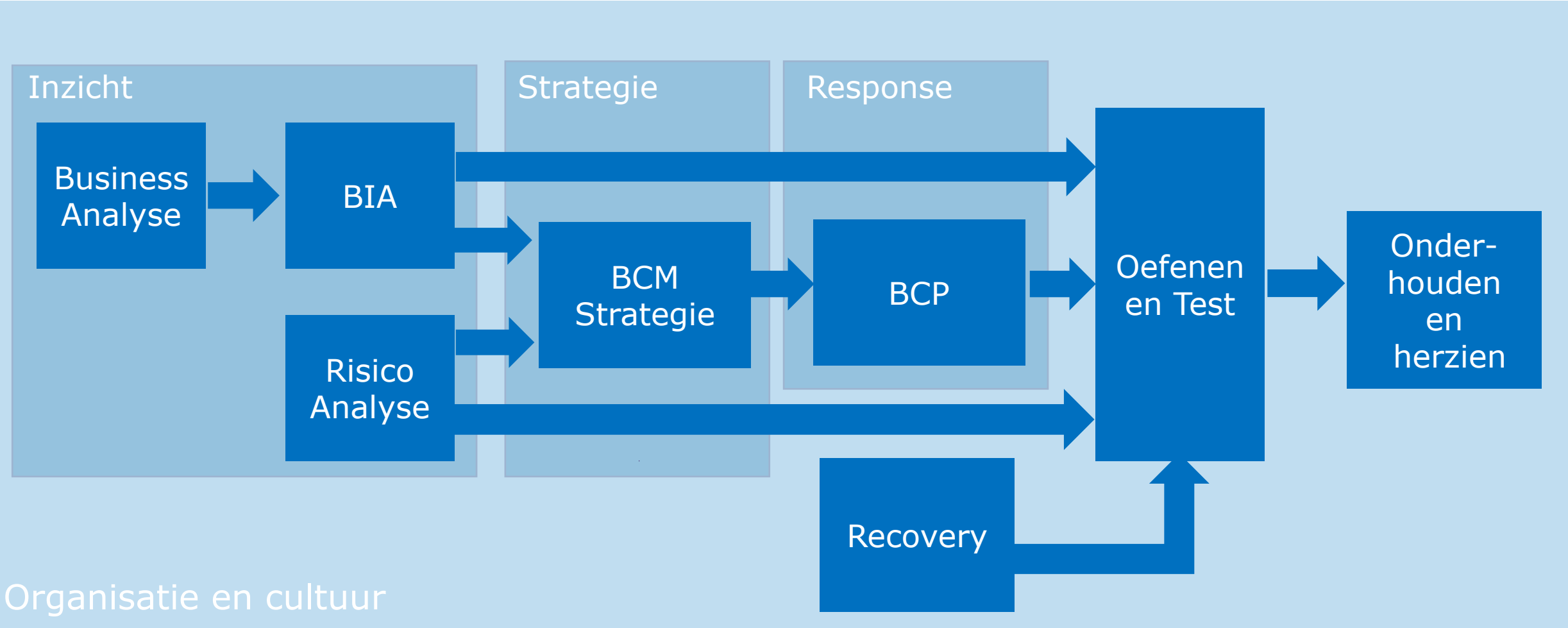
Toetsingskader

- Controls zorgen dat control doelstellingen worden gerealiseerd
- Per control doelstelling zijn er aandachtspunten en soorten documentatie
- AT maakt per control doelstelling een afweging van de mate waarin doelstelling wordt gerealiseerd
- AT analyseert de samenhang tussen de verschillende BCM onderdelen

Aanpak (analyse onderdelen)



Aanpak (analyse samenhang)



Aanpak: afronding

<u>Afronding inspectie</u>
Op basis van onze werkzaamheden stellen wij een rapportage op. Indien nodig maken wij nadere afspraken over een vervolgtraject. U ontvangt deze rapportage ter informatie.

Wij maken inspectierapporten niet openbaar.

Ten aanzien van de Wet openbaarheid van bestuur (Wob) geldt voor de Wbni een uitzondering: vertrouwelijke gegevens die herleidbaar zijn tot een AED zijn niet op te vragen.

Afspraken

- Data voor inspectie
- Inzage lijst BIA’s
- Retourneren toetsingskader en documentatie

Vragen?

Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

Aan: Wbni team

Van
5.1 2.e
T

Datum
11-5-2022

Bijlagen
-

memo

Betreft: Toelichting BCM

Inleiding

Business Continuity Management binnen de organisatie zal de organisatie niet alleen in staat stellen haar dienstverlening te verzekeren ondanks een onderbreking van één of meerdere processen of activiteiten, daarnaast levert het proces nog andere voordelen op. Zo zorgt het er onder meer voor dat voldaan kan worden aan wettelijke en reglementaire verplichtingen (zoals in dit geval de Wbni), sterkt het de geloofwaardigheid en reputatie van de organisatie, is het personeel opgeleid en voorbereid om efficiënt te reageren en kan het personeel worden ingeschakeld in andere teams. Daarnaast levert het in detail bekijken van processen soms ook voordelen uit onverwachte hoek op door het zichtbaar maken van knelpunten binnen de organisatie.

Definitie van BCM
Er bestaat vaak verwarring tussen de begrippen ‘Business Continuity Management’ (BCM) en ‘Business Continuity Plan (BCP).

BCM
Business Continuity Management is een proces waarbij de organisatie de nodige maatregelen treft om ongeacht de omstandigheden de continuïteit van de meest kritische processen te garanderen. In geval van een onderbreking van een of meerdere van deze processen moet de organisatie in staat zijn snel en kordaat op te treden opdat deze activiteiten binnen de kortst mogelijke termijn kunnen worden hersteld.

BCP
Een Business Continuity Plan omschrijft hoe men dat concreet gaat doen en is daarmee een product van Business Continuity Management. Het Business Continuity Plan is een geheel van procedures, afspraken en contactinformatie die gebruikt wordt op het ogenblik dat een onderbreking daadwerkelijk plaatsvindt.

Relatie met andere disciplines
Er bestaat een nauw verband tussen Business Continuity Management, crisismanagement, risicomanagement, interne controle en interne audit. Deze worden verduidelijkt binnen de onderdelen van BCM.

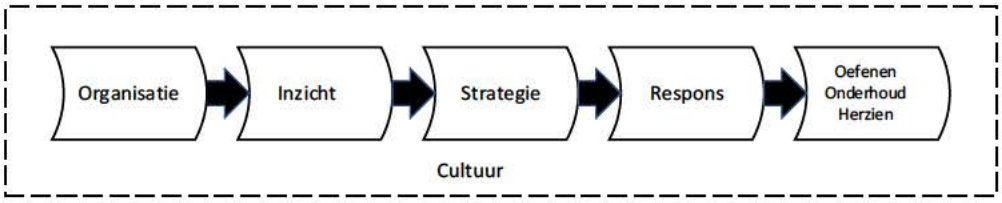
BCM Standaarden
Er bestaan verschillende internationale standaarden en richtlijnen inzake BCM. Het biedt een theoretisch raamwerk dat kan dienen als ondersteuning voor organisaties die een Business Continuity Management programma in hun organisatie wensen te installeren.

Er kan worden vastgesteld dat deze documenten in grote lijnen hetzelfde weergeven, hier en daar wat anders geformuleerd. Het is dan ook niet zo dat wanneer de organisatie kiest om een bepaalde norm te volgen de resultaten tegenovergesteld zouden zijn dan wanneer zij gebruik zouden maken van een andere norm.

Hierbij kan ook nog worden opgemerkt dat deze richtlijnen en normen enkel aangeven wat de stappen zijn die ondernomen moeten worden om een Business Continuity Management te installeren, maar weinig informatie bevatten over het 'hoe' de verschillende stappen in de praktijk moeten worden omgezet.

De onderdelen van BCM

BCM kan in de volgende onderdelen worden onderverdeeld:



Onderdeel 1: het BCM-programma

Het is van belang dat er een duidelijk kader beschreven wordt voor de implementatie van een Business Continuity Management. Zo is het onder meer nodig dat de doelstellingen van het project duidelijk zijn, de rollen en verantwoordelijkheden worden beschreven, dat er gecommuniceerd wordt over het project, enz. Al deze elementen komen aan bod in dit onderdeel.

Beleid
Eén van de belangrijkste randvoorwaarden voor een succesvolle implementatie van Business Continuity Management is de ondersteuning van het topmanagement. Het is daarom aanbevolen dat het topmanagement op een formele wijze een beleidsverklaring (BCM Policy) ondertekent.

Rollen en verantwoordelijkheden
Projectstructuur
Als er wordt gestart met BCM, zal dit worden gedaan in de vorm van een project. In de projectorganisatie treft men de rollen en verantwoordelijkheden alsook de werkwijze die gevolgd zal worden aan. Als BCM volwassener is dan verlaat het doorgaans de projectstructuur en neemt het een permanente structuur aan.

Permanente structuur
BCM is geen tijdelijk gegeven. De opgemaakte plannen moeten voortdurend bijgewerkt worden in functie van de wijzigingen binnen de organisatie. Het is daarom sterk aan te raden een permanente structuur voor BCM binnen de organisatie te voorzien.

Crisisstructuur
Anderzijds moet er ook nagedacht worden over welke de rol dan moet zijn van deze permanente structuur in geval van een ernstige onderbreking waarbij het noodzakelijk is het Business Continuity Plan effectief op te starten. Aangezien deze personen het plan door en door kennen zou het onverstandig zijn in een noodsituatie hun kennis niet in te zetten. Afhankelijk van de cultuur die binnen de organisatie heerst, moet de exacte rol van deze personen in geval van een noodsituatie worden gedefinieerd.

Onderdeel 2: Inzicht verkrijgen in de organisatie

Het tweede onderdeel in het BCM-proces is het verkrijgen van een goed inzicht in de eigen organisatie, de werking van de bedrijfsprocessen, de mensen en de middelen die voor de uitvoering van de processen nodig zijn, de onderlinge afhankelijkheden tussen de processen, de impact van een onderbreking van de processen op de organisatie en de bedreigingen waarmee de organisatie kan worden geconfronteerd. Hier worden de fundamenten gelegd voor het verdere verloop van het proces. Om te weten hoe en op wat men zich moet/kan voorbereiden, en welke de middelen zijn die ter beschikking moeten worden gehouden, moet men de processen in detail gaan bekijken.

Business Analyse
Bij het uitvoeren van een Business Analyse worden alle elementen (input, output, doelstelling, middelen,…) van het proces in kaart gebracht, inclusief de eventuele afhankelijkheden van het proces met andere processen.

Business Impact Analyse
Het uitvoeren van een Business Impact Analyse bestaat uit een analyse van de impact (in termen van gevolgschade) van een onderbreking van de sleutelprocessen van de organisatie en het verloop ervan in de tijd, ongeacht de oorzaak van de onderbreking. In deze fase is het met andere woorden de bedoeling een inschatting te maken van de impact van een uitval van de processen binnen de organisatie. Dit zal niet alleen helpen bepalen welke de volgorde zal zijn waarin de activiteiten zullen moeten worden hersteld. Deze informatie zal ook het management toelaten met kennis van zaken te beslissen in welke BCM maatregelen te investeren. Processen waarvan een onderbreking een zeer grote impact heeft zullen logischerwijze sneller moeten worden hersteld dan processen waarvan de impact van een onderbreking klein is.

Resultaat BA en BIA
Aan het einde van de Business Impact Analyse dient men per proces over de volgende informatie te beschikken:

- Een rangschikking van de sleutelprocessen volgens prioriteit in het kader van bedrijfscontinuïteit (en cf. Wbni).
- De RTO (recovery point objective) en RPO (recovery point objective) voor elk sleutelproces.
- Lijsten van belangrijke leveranciers, systemen, en vitale data.
- Ramingen van de kwalitatieve en kwantitatieve impact van een gebeurtenis in functie van de duur van de verstoring (b.v. 24 uren, 48 uren, 5 dagen, enz.)
- Een overzicht van wat nodig is voor het herstellen van sleutelprocessen in functie van de duur van de verstoring.
- De informatie verkregen uit de Business analyse en de Business Impact Analyse is belangrijke input voor het Business Continuity Plan, met name de beschrijving welke acties wanneer moet gebeuren in geval van onderbreking van een proces.

Risico-analyse
Een volgende stap in het verkrijgen van een goed inzicht in de organisatie is het uitvoeren van een risicoanalyse. De Risicoanalyse is een analyse betreffende de *mogelijke bedreigingen* die kunnen leiden tot een onderbreking van de processen van de organisatie, de waarschijnlijkheid van hun voorkomen en de impact ervan op de organisatie. Er zijn twee uiteenlopende visies te onderscheiden:

Uitgebreide risico-analyse
Enerzijds is er de visie waarbij vertrokken wordt vanuit een inventarisatie van alle mogelijke risico's en het maken van een inschatting van de impact van de diverse risico's op de organisatieprocessen. In functie van de 'kans van optreden van het

risico' en de 'impact' dat het risico teweeg brengt wordt de strategie bepaald en wordt gekeken welke maatregelen/acties ondernomen moeten worden.

Scenario's
Anderzijds is er de visie waarbij wordt geponeerd dat het niet steeds noodzakelijk is om in het kader van Business Continuity Management een uitgebreide risicoanalyse uit te werken. Het is wel belangrijk dat er periodiek (zeg 1 keer per jaar) een risicoanalyse plaatsvindt, maar het voeren van een risicoanalyse is geen absolute voorwaarde om het Business Continuity Management proces binnen de organisatie te kunnen implementeren. Een meer pragmatische aanpak is het vertrekken van een door het management gedefinieerd prioritair risico, of beter nog vanuit een 'worstcase scenario'. In dit geval wordt niet vertrokken vanuit de mogelijke risico's, dan wel wordt aandacht besteed aan de mogelijke gevolgen voor de organisatie ongeacht de dreiging. De mogelijke gevolgen kunnen de volgende zijn:

- gebrek aan faciliteiten of gebrek aan toegang tot de faciliteiten (gebouwen, lokalen,…)
- gebrek aan vitale data
- gebrek aan ICT-infrastructuur
- gebrek aan Human Resources/personeel

Een valkuil is het maken van een plan dat specifiek gericht is op één risico (vb. corona). Het is beter één globaal plan te hebben dat verschillende risico's afdekt dan per specifiek risico een bijlage te ontwikkelen aan het globaal plan.

Onderdeel 3: BCM strategie

Op basis van de goedgekeurde resultaten van de Business Impact Analyse en de mogelijke gevolgen van een onderbreking (gebrek aan personeel, data, ICT en infrastructuur) hetzij eventueel de resultaten van de risicoanalyse (afhankelijk van de methodologie die wordt gevolgd) dienen maatregelen te worden geformuleerd die ervoor moeten kunnen zorgen dat:

- de waarschijnlijkheid van een onderbreking wordt verminderd;
- de periode van de onderbreking kan worden ingekort; de impact van de onderbreking op de kritische activiteiten beperkt is.

In het kader van de BIA werd de RPO en RTO bepaald. In deze fase komt het er op aan maatregelen te formuleren die hieraan tegemoet kunnen komen. Het spreekt voor zich dat hoe korter de RTO, hoe 'hotter' de strategie. Daarnaast moet er bij het bepalen van de maatregelen eveneens rekening worden gehouden met de al bestaande maatregelen.

Onderdeel 4: BCM respons

BCM-Respons is het antwoord dat een organisatie voorbereid heeft om een incident dat zich voordoet te kunnen beheersen en de impact ervan op de werkprocessen te minimaliseren. De maatregelen die door het management in het vorige onderdeel werden goedgekeurd moeten worden uitgewerkt zodat de organisatie in geval van onderbreking van een bepaald proces snel en efficiënt kan reageren.

Het geheel aan procedures met betrekking tot de eerste reactie in navolging van een incident, wordt het Incident Management Plan (IMP) genaamd. Het Business Continuity Plan (BCP) bestaat uit het in gang zetten van processen en het vrijmaken van middelen opdat de organisatie de continuïteit van de meest kritische processen kan blijven garanderen. In het Business Recovery Plan worden die zaken geregeld waarmee kan worden terug gegaan naar 'business as usual'.

Incident Management Plan
Het Incident Management Plan dient in een eenvoudige en makkelijk op te stellen structuur te voorzien, die de organisatie in staat stelt:

- de aard en de reikwijdte van het incident te bevestigen;
- controle te nemen over de situatie;
- te communiceren met stakeholders; en,
- Deze structuur moet ook de geschikte business continuity respons opstarten.

Het is niet de bedoeling nieuwe procedures en plannen uit te werken. Het is juist de bedoeling de reeds bestaande procedures en documenten (evacuatieprocedures, contactgegevens hulp- en interventiediensten, etc.) samen te brengen, de eventuele lacunes te identificeren om daaromtrent verdere afspraken te maken.

Business Continuity Plan
Het Business Continuity Plan geeft in detail weer wat, wie, hoe en wanneer welke acties moet ondernemen zodat de continuïteit van de kritische activiteiten binnen de organisatie kan gegarandeerd worden, hetzij de betrokken activiteiten zo snel als mogelijk opnieuw opgestart kunnen worden.

Het Business Continuity Plan bestaat met andere woorden uit een geheel door het management goedgekeurde reactieve maatregelen. Het beschrijft de wijze waarop een organisatie reageert op het ogenblik dat een risico zich daadwerkelijk manifesteert.

Business Recovery Plan
Het Herstelplan of Business Recovery Plan beschrijft de activiteiten die ondernomen moeten worden om terug te keren naar 'business as usual'. Het plan geeft de recovery targets of milestones aan na een volledige of gedeeltelijke opschorting van bepaalde activiteiten. Het spreekt voor zich dat het van belang is eerst de continuïteit van de meest kritische activiteiten te plannen en voor te bereiden alvorens maatregelen te gaan nemen om volledig terug te keren naar 'business as usual'.

Onderdeel 5: Oefenen Onderhouden Herzien

Het volstaat niet om een Incident Management Plan, een Business Continuity Plan en een Business Recovery Plan in de kast te hebben liggen. De plannen hebben maar hun nut als deze gekend zijn, actueel zijn en regelmatig geoefend worden. Er dient met andere woorden eveneens een oefenprogramma ontwikkeld en geïmplementeerd worden binnen de organisatie.

Het oefenen van de procedures en maatregelen in de plannen moeten verzekeren of de naar aanleiding van de Business Impact Analyse geïdentificeerde doelen gehaald kunnen worden en de kritieke activiteiten binnen de vooropgestelde tijd hersteld kunnen worden.

Het is van belang dat de grote lijnen van het oefenbeleid van de organisatie eveneens worden opgenomen in de globale BCM-beleidsverklaring. Niet alleen de verantwoordelijkheden, de methodologie en het tijdsschema dat gevolgd zal worden dient opgenomen te worden. Daarnaast moet de beleidsverklaring omschrijven welke soort oefeningen georganiseerd zullen worden en in welke volgorde. Het oefenbeleid wordt goedgekeurd door het management.

De doelstellingen van het organiseren van oefeningen zijn onder meer:
- Het personeel vertrouwd te maken met de inhoud van de plannen;
- De kwaliteit van de plannen te testen (zijn de gegevens volledig, actueel, coherent?);
- Na te gaan of de individuen vermeld in het plan op de hoogte zijn van hun rol en in staat zijn hun verantwoordelijkheden op te nemen;
- Na te gaan of de procedures vermeld in het plan haalbaar en realistisch zijn;
- Na te gaan of de vooropgestelde herstelobjectieven realistisch zijn; en,
- De plannen aan te passen in functie van de verbeterpunten die werden vastgesteld tijdens de oefeningen.

Het oefenen van de plannen dient als een onderdeel van BCM te worden gezien. Het is daarom ook belangrijk dat een op maat van de organisatie afgestemd oefenbeleid gevalideerd wordt door het management. Idealiter zouden de plannen jaarlijks getest moeten worden. Het is echter niet steeds noodzakelijk het volledige plan te testen. Er kunnen evenwel oefeningen georganiseerd worden van een

verschillende moeilijkheidsgraad en omvang of met betrekking tot slechts een gedeelte van de organisatie of processen. Het resultaat van de oefeningen dient als input voor eventuele aanpassingen van het plan.

Soorten oefeningen

Moeilijkheid	Soort oefening	Omschrijving
Eenvoudig	Table top	Bepaalde delen van het plan of bepaalde procedures worden in groep nagekeken, doorlopen en besproken.
Medium	Table top met scenario	Bepaalde delen van het plan of bepaalde procedures worden in groep nagekeken, doorlopen en besproken aan de hand van een of meerdere scenario's. De procedures worden niet in 'real-time' toegepast.
	Simulatie	Een onderbreking van een of meerdere processen wordt zo waarheidsgetrouw mogelijk nagebootst waardoor de procedures in het plan worden getest. Aan de hand van een scenario wordt de onderlinge samenwerking en rolverdeling op de proef gesteld, het omgaan met gebrekkige informatie en het besluitvormingsproces wordt geoefend.
Complex	Globale oefening	Oefening die zo dicht mogelijk aanleunt bij de realiteit en die het plan in zijn geheel test. Een onderbreking wordt in 'real-time' nagebootst. De procedures worden effectief in gang gezet en toegepast. Opgelet: er dient steeds een inschatting te worden gemaakt van de kosten, de impact van de oefening en de risico's voor de normale werking.

Onderdeel 6: inbedden in de organisatiecultuur

Om succesvol te zijn moet het BCM gedragen worden door zoveel mogelijk personen binnen de organisatie. Het management (zowel top- als

middenmanagement) spelen een essentiële rol bij het in kaart brengen van de kritische processen.

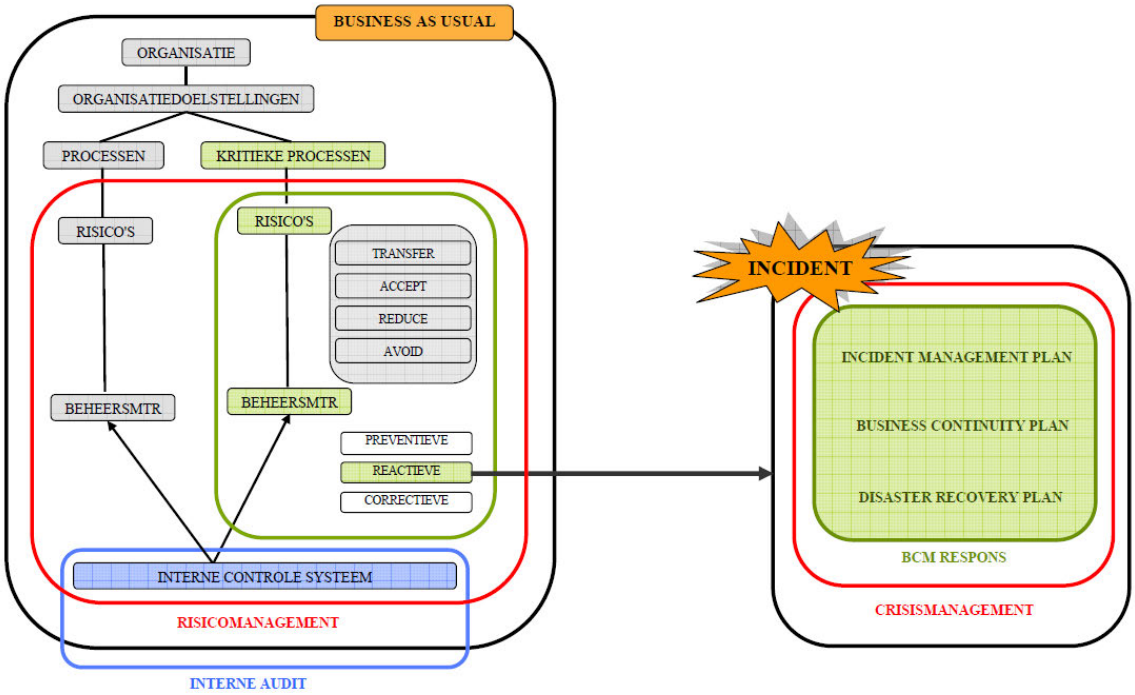
Zoveel mogelijk personeelsleden moeten overtuigd zijn van het feit dat ze een belangrijke rol te spelen hebben om de continuïteit van de activiteiten van de organisatie te kunnen waarborgen. Het is daarom belangrijk voldoende aandacht te besteden aan bewustwording- en opleidingsprogramma's voor het personeel.

Enerzijds moeten alle personeelsleden geïnformeerd worden over de inhoud van de plannen en moet iedereen zich bewust zijn van zijn/haar individuele verantwoordelijkheden. Anderzijds is het aan te bevelen dat personeel met directe BCM-verantwoordelijkheden specifieke opleidingen volgen.

BCM moet ook blijvend onder de aandacht worden gehouden door bijvoorbeeld het verspreiden van een interne nieuwsbrief, informatie op het intranet, bespreking hiervan in teammeetings, het gebruiken van een logo,... Voor nieuwe personeelsleden kan het BCM-beleid van de organisatie eventueel geïntegreerd worden in het opleidings- of onthaalprogramma. Andere mogelijkheden om een draagvlak te creëren kunnen zijn:

- Workshops of discussiegroepen rond het thema organiseren
- Artikelen publiceren met betrekking tot oefeningen en vergaderingen van de Task Force: communicatie over de werkzaamheden
- Opleidingen organiseren
- Nieuwsbrief
- Een pagina op intranet
- Bezoek aan de alternatieve locatie

Bijlage 1: Het verband tussen Business Continuity Management, Crisismanagement, Risicomanagement, Interne controle en Interne audit.



Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

50

Team Wbni

Van
5.1.2.e

Review:

T

Datum
Mei 2022

Bijlagen
1: Flowchart
2: versiebeheer

memo

Procesbeschrijving thematische inspectie (BCM)

In deze memo is het proces "thema-inspectie" uitgeschreven. Om de inspecties uit te voeren wordt gebruik gemaakt van de volgende documenten:

- Brief aankondiging inspectie;
- Presentatie Kick-off (aankondiging);
- Uittreksel van toetsingskader thema-inspectie, dit is de versie die naar de AED wordt gestuurd (in het toetsingskader is dit onderdeel blauw gemarkeerd);
- Volledig toetsingskader[1] voor intern gebruik;
- Sjabloon voor gespreksverslagen;
- Template thema-inspectie (rapport en ppt); en,
- Directorystructuur

De inspecties worden door twee inspecteurs uitgevoerd: een auditor en een specialist. Stem per duo af wie welke taken voor zijn rekening neemt. In de bijlage worden de stappen grafisch weergegeven.

Samenvatting handelingen
Het doel van de thema-inspectie is om een diepgaand beeld van een onderdeel van de informatiebeveiliging van de essentiële dienst van de AED te verkrijgen.

Voor de kick-off ontvangt de AED een aankondigingsbrief en het uittreksel van het toetsingskader.

Tijdens de kick-off wordt de werkwijze gepresenteerd.

Na de kick-off wordt de AED gevraagd om zich met een verkorte versie van het toetsingskader zich voor te bereiden op de inspectie. Het uittreksel geeft het thema op de hoofdonderwerpen weer. Voor de inspectie wordt het uittreksel ingevuld geretourneerd aan AT. Tevens wordt in overleg met AED een BIA gekozen.

Vervolgens wordt in samenwerking met de AED het thema behandeld tijdens de daadwerkelijke inspecties. Stel per onderwerp de vragen die zijn opgenomen in

[1] Deze procesbeschrijving veronderstelt dat het kader reeds is opgesteld.

het toetsingskader en volg de stappen uit het toetsingskader. Het eerste deel van de inspectie doorloopt de onderdelen uit het toetsingskader. Het tweede deel van de inspectie gaat dieper in op de BIA en op een crisissituatie of een oefening.

Vervolgens wordt de inspectie uitgewerkt en volgt een interne analyse waarbij de resultaten van vergelijkbare organisaties worden geanalyseerd. Dat leidt tot een terugkoppeling in de vorm van een inspectierapport en een presentatie.

Aanmaken opslaglocatie en klaarzetten documentatie
Maak een directory aan op de T-schijf waar alle stukken van de inspectie worden opgeslagen. Zet in de directory alle templates klaar die voor de inspectie nodig zijn en pas ze aan voor de inspectie. Maak hiervoor gebruik van het dummy dossier[2] en volg de aanwijzingen. Let op dat de lege templates ongewijzigd blijven.

Aankondigen van de inspectie
Kondig de inspectie aan met een brief. Stel deze op, laat hem ondertekenen door het afdelingshoofd (via 5.1.2.e + RP2000 nummer) en verstuur deze per mail. Gebruik de volgnummers die zijn opgenomen in "instructie kenmerk documenten".[3] Neem contact op met de AED om een afspraak te maken om het doel van de inspectie op kantoor toe te lichten. Stuur het uittreksel van het toetsingskader op.

Inlezen
Lees jezelf in voor de inspectie. Gebruik hiervoor informatie uit eerdere inspecties, inventarisatiegesprekken etc.

Kick-off thema-inspectie
Gebruik een presentatie om de werkwijze toe te lichten.

Behandel tijdens de kick-off het uittreksel van het toetsingskader. Licht tijdens het gesprek toe wat het doel van de inspectie is en wat van de AED verwacht wordt. Zorg er voor dat de AED het toetsingskader invult en terugstuurt voor de inspectie. Verzoek de AED om de evidence op te sturen. Maak vervolgafspraken om de daadwerkelijke inspectie uit te voeren. Er zijn waarschijnlijk minimaal twee inspecties nodig. Reserveer ook tijd (bij hen op kantoor) om documenten in te zien voor het geval ze niet alles op willen sturen.

Voorbereiden inspectie
In het interne toetsingskader zijn tabbladen opgenomen waarin is opgenomen wat het doel is per deelonderwerp en wat de aandachtspunten voor de inspecteur zijn. Bestudeer de onderwerpen en vul het toetsingskader zo ver mogelijk in adhv de teruggestuurde documenten van de AED.

Ga na of de AED een lijst met BIA's heeft overlegd en kies een BIA om tijdens de inspectie verder op in te gaan. Kies een BIA die een duidelijke link met de essentiële dienst heeft.

Uitvoeren inspectie

---

[2] buiten reikwijdte

[3] buiten reikwijdte

Gebruik een gespreksverslag (sjabloon uit het dummy dossier) om het interview in weer te geven. Vervolgens wordt het toetsingskader door de inspecteurs ingevuld. We gaan uit van twee sessies. In de eerste sessie wordt het BCM doorlopen, in de tweede sessie wordt dieper ingegaan op de BIA en het incident.

Denk bij het uitvoeren van de inspectie aan de volgende aandachtspunten:

- Stel jezelf de vraag of de aangeleverde evidence de doelstelling in voldoende mate afdekt; en,
- Maak afspraken over eventuele acties die worden geformuleerd tijdens de inspectie.

Stem de gespreksverslagen af met de AED voor hoor-wederhoor.

Hieronder wordt dieper ingegaan op het verzamelen van de evidence, enkele richtlijnen over de informatiebeveiliging van de verwerkte informatie, volwassenheidsscores en de uitzonderingen.

Verzamelen evidence
Verzamel voor de inspectie van de beheersdoelen relevante evidence. Bepaal op voorhand welke evidence volstaat, zoals vastgelegd in de voorbereiding. De evidence wordt vooraf afgestemd met de AED. Uitgangspunt is dat altijd minimaal 2 bronnen worden gebruikt. Dit houdt in dat naast het interview nog bijvoorbeeld een procedure of schermafdruk wordt opgevraagd. De evidence wordt bij voorkeur voor de inspectie opgestuurd naar AT via het infoportal.

Informatiebeveiligingseisen verwerkte informatie
Tijdens deze fase wordt informatie verwerkt die op een hoger niveau is geclassificeerd dan het standaardniveau dat wordt geleverd in de 5.1.1.b [redacted] Houd daarom vooraf rekening hoe om te gaan met stukken die je mee wilt nemen. Met name stukken die op Stg-C zijn geclassificeerd behoeven extra aandacht. Voor deze categorie stukken is het een oplossing om alleen die onderdelen in te zien die voor nu relevant zijn en in het verslag een verwijzing op te nemen. Werk met eenduidige verwijzingen zodat in een later stadium geen onduidelijkheid kan ontstaan als evidence toch moet worden opgevraagd, bijvoorbeeld in het geval van handhaving.

Volwassenheidsscores
De inspecties richten zich op beveiligingsmaatregelen die naar verwachting, zeker bij de energiesector, niet zijn te vergelijken in verband met de complexiteit van die maatregelen. Bij wijze van experiment is daarom besloten dat bij de drie partijen uit de digitale infrastructuur wordt geprobeerd om volwassenheidsscores aan te geven. Bij netbeheer wordt dit in eerste instantie niet gedaan.

Uitzonderingen
Hoe ga je om met informatie die niet tot de inspectie horen? Dit kan zijn in de volgende situaties:

- Je krijgt informatie die buiten de scope van de inspectie valt.
- AED laat "per ongeluk" informatie zien die niet van toepassing is van de inspectie; maar wel belastend kan zijn.

Neem dit eventueel op als bijvangst en overweeg om dit mee te nemen in de jaarlijkse risico analyse. Let op: dit is maatwerk voor elke specifieke situatie.

Hoe ga je om met een hoge risk appetite van een AED of een AED die niet wil meewerken? Dit is maatwerk. Belangrijk om met partij in gesprek te blijven en intern AT een groep samen stellen om dit te bespreken.

Vastleggen inspectie
Leg vervolgens de bevindingen vast in het standaardrapport.

Interne analyse
Maak een vergelijking van de resultaten van de inspectie met de vergelijkbare organisaties en kijk of er een rode draad is te vinden in de bevindingen en op welke punten we willen terugkoppelen naar de AED. Hanteer voor de analyse van bevindingen de volgende uitgangspunten:

	Onderkend AED	Onderkend AT
Weinig impact	Wel opnemen Geen feedback Geen monitoring	Wel opnemen Wel / geen feedback Monitoring account mngt
Veel impact	Wel opnemen Wel feedback Monitoring d.m.v…..	Wel opnemen Wel feedback Monitoring d.m.v…..

Afstemming bevindingen
Stem de bevindingen via een concept van de bevindingenrapportage af. Eventueel kun je op hoofdlijnen verwijzen naar good/best practices die de AED zelf verder dient te onderzoeken.

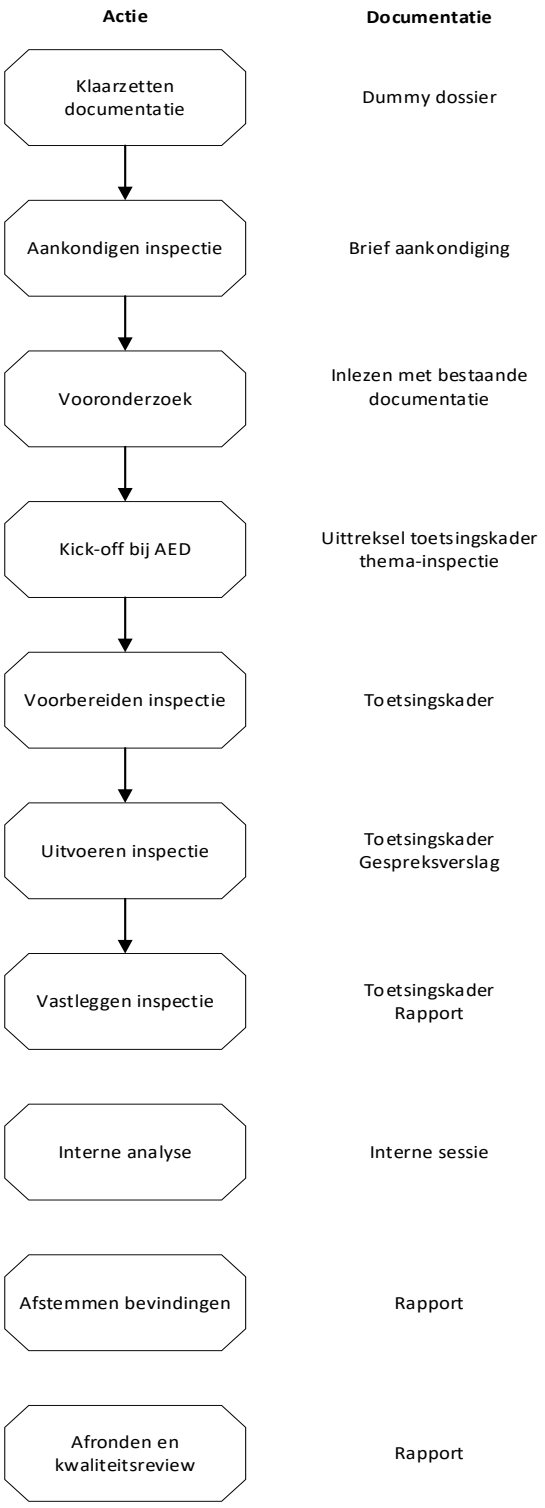
Gebruik het template standaardrapport voor de eindrapportage.

Afronden inspectie en kwaliteitsreview
Koppel afsluitend, na verwerken van het commentaar, de resultaten terug naar de AED. Zorg er tevens voor dat alle relevante documentatie is opgeslagen, inclusief de e-mailberichten van en naar de AED.

Opvolging van acties vindt plaats via het accountmanagement gesprek. Evidence van de opzet en bestaan wordt opgevraagd en in het dossier opgenomen. Indien er dringende acties zijn, dan wordt direct na verstrijken van de deadline de opvolging vastgesteld. De AED bepaalt zelf de actie en de deadlines. Ga in discussie met de AED als de actie niet juist of volledig is of als de deadline niet reëel is.

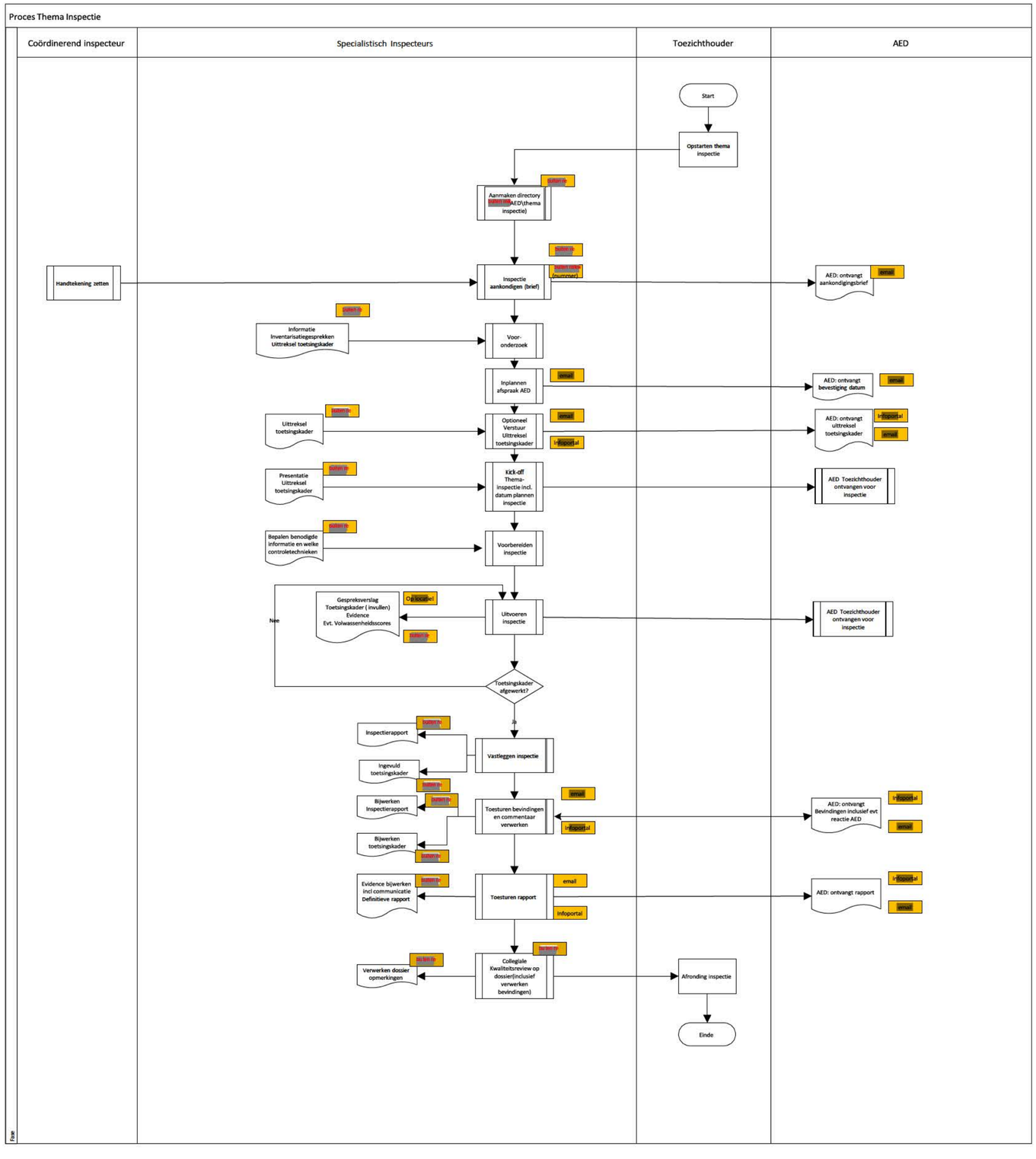
Tot slot wordt een kwaliteitsreview op het dossier uitgevoerd door de 5.1.2.e [redacted]. De inspecteurs geven haar daarvoor het teken dat zij de review uit kan gaan voeren. De kwaliteitsreview richt zich op de juiste directorystructuur, de naamgevingen, de volledigheid van de stukken etc. De rapportage wordt inhoudelijk door een 5.1.2.e [redacted] beoordeeld. Daarna vindt ondertekening door de 5.1.2.e [redacted] plaats. De verantwoordelijkheid voor een correcte afhandeling blijft bij de inspecteurs liggen die de inspectie hebben uitgevoerd.

Bijlage: flow-chart thema-inspectie



Bijlage 2: versiebeheer

Versie	Auteur	Datum	Wijziging
1.0	5.1.2.e	03-2020	
1.1	5.1.2.e	2-6-2021	Naar aanleiding van evaluatie inspectie proces. Zie de samenvatting van het evaluatieproces voor de wijzigingen.
1.2	5.1.2.e		Aangepast voor BCM
1.3	5.1.2.e	26-10-2023	Aanpassing BCM op verzoek van 5.1.2.e verwijderd.


Proces Thema Inspectie
Coördinerend inspecteur
Specialistisch Inspecteurs
Toezichthouder
AED
Start
Opstarten thema inspectie
Aanmaken directory AED\thema inspectie)
Handtekening zetten
Inspectie aankondigen (brief)
AED: ontvangt aankondigingsbrief
email
Informatie Inventarisatiegesprekken Uittreksel toetsingskader
Voor-onderzoek
Inplannen afspraak AED
AED: ontvangt bevestiging datum
Uittreksel toetsingskader
Optioneel Verstuur Uittreksel toetsingskader
AED: ontvangt uittreksel toetsingskader
infoportal
Presentatie Uittreksel toetsingskader
Kick-off Thema-inspectie incl. datum plannen inspectie
AED Toezichthouder ontvangen voor inspectie
Bepalen benodigde informatie en welke controletechnieken
Voorbereiden inspectie
Gespreksverslag Toetsingskader (invullen) Evidence Evt. Volwassenheidsscores
Uitvoeren inspectie
Nee
Toetsingskader afgewerkt?
Ja
Inspectierapport
Vastleggen inspectie
Ingevuld toetsingskader
Bijwerken Inspectierapport
Toesturen bevindingen en commentaar verwerken
AED: ontvangt Bevindingen inclusief evt reactie AED
Bijwerken toetsingskader
Evidence bijwerken incl communicatie Definitieve rapport
Toesturen rapport
AED: ontvangt rapport
Verwerken dossier opmerkingen
Collegiale Kwaliteitsreview op dossier(inclusief verwerken bevindingen)
Afronding inspectie
Einde
Fase

Business Continuity Management Toetsingskader

		Control Objective / Doelstelling	Best practice controls/ beheersmaatregelen (*afwijken van deze controls/beheersmaatregelen is mogelijk, uiteindelijk is het van belang dat het control objective / doelstelling geborgd wordt).	Aandachtspunten bij nagaan invulling maatregel	Mogelijke evidence bij de te verwachte control / beheersmaatregelen (*afwijken van deze controls/beheersmaatregelen is mogelijk, uiteindelijk is het van belang dat het control objective / doelstelling maar geborgd wordt).
Onderdeel 1: BCM organisatie (ISO A17.1.1)	Organisatie	Het management van een organisatie geeft aan dat BCM prioriteit heeft en doelstellingen, rollen en verantwoordelijkheden worden duidelijk geformuleerd.	In een formeel vastgesteld document, ondertekend door topmanagement, in de vorm van een BCM-beleidsverklaring. In dit document worden doelstellingen, rollen en verantwoordelijkheden geformuleerd.	In het beleidsdocument is, onder andere, het volgende aan te treffen: - De definitie van Business Continuity Management volgens de organisatie; - De Business Continuity doelstellingen van de organisatie (welke resultaten worden verwacht?); - Het toekennen van taken, verantwoordelijkheden en bevoegdheden binnen BCM proces - De beschikbaarheid van personeel en middelen (tijd/budget); - Versiecontrole en documentbeheer van de beleidsverklaring;	BCM-beleidsstuk
Onderdeel 2: inzicht in de organisatie (ISO A17.1.1)	Business Analyse	Het in kaart brengen van de belangrijkste processen (scope: Wbni) van de organisatie.	Overzicht met processen die een onderdeel vormen van de essentiële dienst en daarmee in aanmerking komen voor BCM.	- Overzicht met processen. - De essentiële dienst moet worden vertegenwoordigd door de opsomming van de processen. - Afhankelijkheden van andere processen. - Incl. uitbestede diensten.	Lijst met de belangrijkste processen + overwegingen bij aandachtspunten (scope: Wbni) van de organisatie.
	Business Impact Analyses	Analyse van de impact van een onderbreking van de eerder geïdentificeerde processen van de organisatie en het verloop ervan in de tijd, inclusief de vereisten de aan de processen worden gesteld.	Er is een actuele Business Impact Analyse (BIA) uitgevoerd voor processen, met een inschatting van de impact van een verstoring op de bedrijfsvoering en vastgestelde hersteldoelstellingen.	De BIA identificeert per proces o.a. - classificatie op de BIV; - vertaling soort schade of verlies naar classificatie; - hoe de schade kan escaleren; - De afhankelijkheid van vaardigheden, faciliteiten, systemen en derde partijen om dit proces te continueren; - De tijd waarin gedeeltelijk (meest essentiële processen/systemen) en volledig herstel plaats moet vinden; - Het bepalen van herstelprioriteiten (RPO / RTO) voor elke service dat gevalideerd is door de business.	BIA waarin de aandachtspunten zijn opgenomen. (overzicht met BIA's vooraf opsturen)
	Dreigingsanalyse	Uit de risicoanalyse volgt een lijst met relevant bedreigingen die impact hebben op de kritische processen van de essentiele dienst.	Meest gebruikte methode is scenario-analyses. (“klassieke” risico-analyse kan ook)	Toets of relevante dreigingen zijn meegenomen. In het geval er scenario's zijn opgesteld kan rekening worden gehouden met het volgende: - afhankelijkheden van de medewerkers en informatie en communicatiesystemen. - afhankelijkheid van basisvoorzieningen (locatie, elektriciteit, etc.) - externe service providers, welke specifieke risico's deze afhankelijkheid inhoudt voor de continuïteit van de kritieke processen en op welke wijze de continuïteit hiervoor is georganiseerd. Lijst met scenario's met onderbouwing waarom deze scenario relevant zijn. De BA, BIA en de dreigingsanalyse vormt de basis voor de BCM strategie. Periodieke update van het dreigingsprofiel.	Risico-analyse, (all hazard) dreigingsanalyse, etc.
Onderdeel 3: BCM strategie (ISO A17.1.2)	Strategie	Op basis van voorgaande stappen en de mogelijke gevolgen van een verstoring in combinatie met de resultaten van de risicoanalyse dienen maatregelen te worden geformuleerd en geïmplementeerd die ervoor moeten kunnen zorgen dat: - de duur van de vermindere dienstverlening kan worden ingekort; - de impact van de verstoring op de kritische processen beperkt wordt.	Een door het management goedgekeurd document met de te nemen maatregelen en bewijs van de uitvoering van deze maatregelen.	Uit de BIA zijn de eisen in termen van RPO/RTO van de processen gekomen. In deze stap moeten deze eisen worden omgezet in maatregelen. Per relevant business proces: - De activiteiten identificeren om de RPO/RTO te halen. - De kosten baten (inclusief maatschappelijke impact) analyse van de verschillende soorten response (bijv. koppelingen afsluiten, OT isoleren). - Na keuze van het management omzetten van het opmaken van een plan van aanpak - Implementatie en opvolging van het plan van aanpak.	Document waarin de eisen uit de BIA zijn omgezet in maatregelen en geïmplementeerd
Onderdeel 4: BCM respons (ISO A17.1.2)	Incident management	Het Incident Management dient in een eenvoudige en makkelijk op te stellen structuur te voorzien, die de organisatie in staat stelt om de geschikte business continuity response op te starten.	Een incident management plan met onder andere: - de aard en de reikwijdte van het incident vaststellen; - controle te nemen over de situatie; - te communiceren met stakeholders; Uit deze stap moet direct volgen wat de impact van de verstoring (is er sprake van crisis?) is en welke onderdelen van de organisatie moeten worden ingeschakeld.	In het plan is verder opgenomen: - Doelstelling en scope van het plan - De rollen en verantwoordelijkheden - Escalatieprocedure: het opstarten van het plan (hoe, door wie, wanneer, ...) - De documenteigenaar - Essentiële contactgegevens (contactlijsten) Niet het hele incident management proces wordt behandeld, alleen dat deel waarin de onderdelen (BCP, recovery, evt. crisismgmt) van het BCM worden opgestart.	Incident Management Plan waarin verwezen wordt naar relevante onderdelen van de organisatie zoals het BCP en crisis management.
	Business Continuity & Crisismanagement	Het moet tot in detail duidelijk zijn wie, hoe en wanneer welke acties moet ondernemen zodat de continuïteit van de kritische processen binnen de organisatie zo snel mogelijk kunnen worden hersteld.	De organisatie heeft een plan waarin staat beschreven wie (rol), hoe en wanneer welke acties ondernomen moeten worden om de continuïteit van de kritische processen zo snel mogelijk te kunnen herstellen. In het Business Continuity Plan staat o.a.: - Doelstelling en scope van het plan - De rollen en verantwoordelijkheden - Het opstarten van het plan (hoe, door wie, wanneer) - De documenteigenaar - Essentiële contactgegevens - draaiboek met de te ondernemen activiteiten voor herstel acties - consequentie van mogelijke keuzen (uitwijk, afschakeling dienst,) Het BCP maakt gebruik van onderdelen van het crisismanagement. Deze constructie heeft als doel om de impact op de gehele organisatie zoin te doen afnemen.	Escalatieprocedure / opstarten BCP - Essentiële contactgegevens: Verantwoordelijken voor het afkondigen van het Business Continuity Plan - Structuur, rollen en verantwoordelijkheden (mandaat) van het crisismanagement team. - Opsomming van de kritieke sleutelprocessen met het telkens daarbij de RPO/RTO, alsook de rangschikking van de processen en activiteiten (incl uitbestede processen). - Afhankelijkheden van andere processen (met de respectievelijke RTO en contactpersonen. (bijvoorbeeld het IT-proces) - Personeel nodig voor de uitvoering van de kritieke sleutelprocessen (contactgegevens, rollen en verantwoordelijkheden,alsook eventueel logistiek, HR en juridische Zaken, ..) - Vitale data nodig voor de uitoefening van het proces en de vindplaats ervan (of van de back-up) - Faciliteiten (bijvoorbeeld vergaderzalen, persruimte, ... voor het geval de sleutelactiviteiten naar een alternatieve locatie dienen te worden verplaatst. - Lijst met kritieke leveranciers of andere dienstverleners - Andere relevante informatie: - Communicatiestrategie (t.a.v. personeel, partners/belanghebbenden, leveranciers, media, ...) - Registratie van communicatie (logboek) - Formulieren: templates logboek/incidentenlogboek	Business Continuity Plan
	Business Recovery	De organisatie heeft vooraf nagedacht om weer terug te keren naar business as usual, (hgv een incident. (Terugkeer IT, locatie, terugkeren van island mode)	Een Business Recovery Plan met: - Doelstelling en scope van het plan - De rollen en verantwoordelijkheden - Het opstarten van het plan (hoe, door wie, wanneer) - De documenteigenaar	Het Herstelplan of Business Recovery Plan beschrijft de activiteiten die ondernomen moeten worden om terug te keren naar 'business as usual'. Het plan geeft de recovery targets of milestones aan na een volledige of gedeeltelijke opschorting van bepaalde activiteiten.	Business Recovery Plan
Onderdeel 5: Oefenen, onderhouden en herzien (ISO A17.1.3)	Oefenen	Oefeningen worden gehouden om: - Personeel vertrouwd te maken met de plannen; - De kwaliteit van de plannen te testen; - Controleren of mensen voldoende getraind zijn om te weten wat zij moeten doen; - Na te gaan of de procedures en hersteltijden haalbaar zijn; - De plannen te kunnen verbeteren	Van eenvoudig (tabletop) tot uitgebreid (organisatie overstijgend).	Het type oefening dat wordt gedaan is afhankelijk van de doelstelling. Daarom moeten deze oefeningen goed voorbereid zijn. De volgende stappen kunnen worden onderscheiden: - Plannen; - Ontwikkelen; - Oefenen; - Evaluatie; - Implementatie. Ga per stap (zie tabblad fase oefening) na in hoeverre hier invulling aan is gegeven. Kritische leveranciers dienen meegenomen te worden in deze plannen.	Oefenbeleid Oefenplannen Verslagen van oefeningen Logboeken
	Onderhouden en herzien	Het BCM proces stappen wordt onderhouden.	Het BCM documentatie wordt onderhouden en op een zorgvuldige manier gecommuniceerd. Elke oefening en crisis wordt geevaluaeerd, verbeterpunten opgeschreld en worden tijdig opgelost.	Het BCM wordt geevaluaeerd en bijgewerkt naar aanleiding van: - Oefening en de geïdentificeerde verbeterpunten. - In werking treden van BCM plan na een incident. - Een wijziging van de gebruikte producten of diensten van de organisatie (incl. leveranciers). - Een wijziging van beleid, processen of procedures. - Jaarlijkse herziening	Documentatie historie (+aanleiding) van het BCM en een distributielijst. Evaluatie verslagen en actiepunten Inzage incident (indien niet aanwezig oefening)
Onderdeel 6: Organisatiecultuur (ISO 17.1.3)	Organisatiecultuur	De organisatie zorgt voor gedragenheid en kennis van BCM onder haar personeel.	BCM bewustwording en opleiding dienen geborgd te worden binnen de organisatie.	Onder andere: - Workshops - Interne communicatie - Opleidingen & trainingen - Campagnes - Publicaties (oefeningen en crisis)	Trainingsplan, register van trainingen. Voorbeelden van campagnes en publicaties

Good practice:	In een formeel vastgesteld document, ondertekend door topmanagement, in de vorm van een BCM-beleidsverklaring. In dit document worden doelstellingen, rollen en verantwoordelijkheden geformuleerd.		
Aandachtspunten:	In het beleidsdocument is, onder andere, het volgende aan te treffen: - De definitie van Business Continuity Management volgens de organisatie; - De Business Continuity doelstellingen van de organisatie (welke resultaten worden verwacht?); - Het toekennen van taken, verantwoordelijkheden en bevoegdheden binnen BCM proces - De beschikbaarheid van personeel en middelen (tijd/budget); - Versiecontrole en documentbeheer van de beleidsverklaring;		
Aandachtspunten voor inspecteurs	Doorgaans gepubliceerd in beleidsdocument. Denk aan periodiciteit (niet te oud).		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Good practice:	Overzicht met processen die een onderdeel vormen van de essentiële dienst en daarmee in aanmerking komen voor BCM.		
Aandachtspunten:	- Overzicht met processen. - De essentiële dienst moet worden vertegenwoordigd door de opsomming van de processen. - Afhankelijkheden van andere processen. - Incl. uitbestede diensten.		
Aandachtspunten voor inspecteurs:	Overzicht met processen, kan onderdeel zijn van een BIA, rampenplan etc. Gaat met name over de Wbni-scope (alle digitale netbeheerderstaken) van het BCM.		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Good practice:	Er is een actuele Business Impact Analyse (BIA) uitgevoerd voor processen, met een inschatting van de impact van een verstoring op de bedrijfsvoering en vastgestelde hersteldoelstellingen.		
Aandachtspunten:	De BIA identificeert per proces o.a. - classificatie op de BIV; - vertaling soort schade of verlies naar classificatie; - hoe de schade kan escaleren; - De afhankelijkheid van vaardigheden, faciliteiten, systemen en derde partijen om dit proces te continueren; - De tijd waarin gedeeltelijk (meest essentiële processen/systemen) en volledig herstel plaats moet vinden; - Het bepalen van herstelprioriteiten (RPO / RTO) voor elke service dat gevalideerd is door de business.		
Aandachtspunten voor inspecteurs:	BIA beoordelen (zie D8) adhv vereisten, inclusief RTO en RPO. Werkwijze: - Vooraf opsturen van een lijst met uitgevoerde BIA door AED. - Voor de eerste inspectie kiest AT 1 sample van een uitgevoerde BIA. - AT communiceert dit aan AED en wil een toelichting van een uitgevoerde BIA tijdens de inspectie.		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Good practice:	Meest gebruikte methode is scenario-analyses. ("klassieke" risico-analyse kan ook)		
Aandachtspunten:	Toets of relevante dreigingen zijn meegenomen. In het geval er scenario's zijn opgesteld kan rekening worden gehouden met het volgende: - afhankelijkheden van de medewerkers en informatie en communicatiesystemen. - afhankelijkheid van basisvoorzieningen (locatie, elektriciteit, etc.) - externe service providers, welke specifieke risico's deze afhankelijkheid inhoudt voor de continuïteit van de kritieke processen en op welke wijze de continuïteit hiervoor is georganiseerd. Lijst met scenario's met onderbouwing waarom deze scenario relevant zijn. De BA, BIA en de dreigingsanalyse vormt de basis voor de BCM strategie. Periodieke update van het dreigingsprofiel.		
Aandachtspunten voor inspecteurs:	Opzet: Hoe is de analyse tot stand gekomen? Welke bronnen zijn gebruikt (ncsc etc.)? Worden zowel externe als interne dreigingen hierin meegenomen? Hoe vaak wordt geupdate? Zie E9 voor aandachtspunten. Extra aandachtspunten: Zijn scenario's als vulnerability, pandemie (Log4J/ Corona), wegvallen van kritieke leveranciers (VDL) onderkend? In hoeverre is het BCP plan in werking getreden (Log4J/ Corona)? evt meenemen met onderdeel crisismanagement. Zijn er aspecten wat niet voorzien is en wat zijn de leerpunten en actiepunten hierop.		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Good practice:	Een door het management goedgekeurd document met de te nemen maatregelen en bewijs van de uitvoering van deze maatregelen.		
Aandachtspunten:	Uit de BIA zijn de eisen in termen van RPO/RTO van de processen gekomen. In deze stap moeten deze eisen worden omgezet in maatregelen. Per relevant business proces: - De activiteiten identificeren om de RPO/RTO te halen. - De kosten baten (inclusief maatschappelijke impact) analyse van de verschillende soorten response (bijv. koppelingen afsluiten, OT isoleren). - Na keuze van het management omzetten van het opmaken van een plan van aanpak - Implementatie en opvolging van het plan van aanpak.		
Aandachtspunten voor inspecteurs	Zal in grote mate afhangen van de werkwijze van de AED. Toets vooral of de eerder gemaakte analyses terugekomen en doelstellingen worden gehaald door de genomen maatregelen. Zijn de gedefinieerde maatregelen daadwerkelijk geïmplementeerd? Indien niet het geval afwijkingsrapport of evt planning wanneer ze het hebben geimplementeerd. Zie verder hieronder voorbeelden van maatregelen opgenomen die uit deze exercitie kunnen komen)		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

BCM maatregelen	De organisatie heeft effectieve maatregelen genomen om de impact bij een eventuele verstoring te beperken.	De organisatie dient haar kritieke processen uit te kunnen wijken naar een andere fysieke locatie	ISO/IEC 22313: 2020, 8.4 NIST 800-34	Beschrijving in BCP plan van uitwijklocaties. Uitwijktesten
		Enkelvoudige verstoringen met hoge impact (Netwerk en informatievoorziening en stroomvoorziening) kunnen binnen korte tijd opgevangen worden.	ISO 22301??? NIST 800-34	UPS, Aggregaat, Redundante netwerkvoorziening Testresultaten
		De backup strategie houdt rekening met hersteltijd, beschikbaarheid en integriteit van de backups (inclusief testen)	ISO/IEC 27002: 2017, 12.3.1 IEC 62243 2-1 system development & maintenance NIST 800-34	Backup strategie Backup testmethode
		De organisatie heeft maatregelen genomen om de beschikbaarheid van kritisch personeel tijdens crisissituaties te waarborgen.		inventarisatie kritische functies (vlootschouw) plan bij uitval personeel of pandemie
		Voor kritische leveranciers zijn additionele maatregelen genomen om de beschikbaarheid van producten en diensten te garanderen		maatregel als leverancier uitvalt (bijv reserve componenten, contractuele afspraken, dual vendor,..)

Good practice:	Een incident management plan met onder andere: - de aard en de reikwijdte van het incident vaststellen; - controle te nemen over de situatie; - te communiceren met stakeholders; Uit deze stap moet direct volgen wat de impact van de verstoring (is er sprake van crisis?) is en welke onderdelen van de organisatie moeten worden ingeschakeld.		
Aandachtspunten:	In het plan is verder opgenomen: - Doelstelling en scope van het plan - De rollen en verantwoordelijkheden - Escalatieprocedure: het opstarten van het plan (hoe, door wie, wanneer, …) - De documenteigenaar - Essentiële contactgegevens (contactlijsten) Niet het hele incident management proces wordt behandeld, alleen dat deel waarin de onderdelen (BCP, recovery, evt. crisismgmt) van het BCM worden opgestart.		
Aandachtspunten voor inspecteurs	Het incident management wordt getoetst op selectiecriteria (worden de juiste onderdelen opgestart?) en hoe wordt de ernst van het incident bepaald. Is IM centraal geregeld? Het is buiten scope om de "brandweerfunctie" te toetsen, dwz de reactie om het incident te bestrijden.		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Good practice:	De organisatie heeft een plan waarin staat beschreven wie (rol), hoe en wanneer welke acties ondernomen moeten worden om de continuïteit van de kritische processen zo snel mogelijk te kunnen herstellen. In het Business Continuity Plan staat o.a.: - Doelstelling en scope van het plan - De rollen en verantwoordelijkheden - Het opstarten van het plan (hoe, door wie, wanneer) - De documenteigenaar - Essentiële contactgegevens - draaiboek met de te ondernemen activiteiten voor herstel acties - consequentie van mogelijke keuzen (uitwijk, afschakeling dienst,) Het BCP maakt gebruik van onderdelen van het crisismanagement. Deze constructie heeft als doel om de impact op de gehele organisatie zsm te doen afnemen. Uit deze stap moet direct volgen wat de impact van de verstoring (is er sprake van crisis?) is en welke onderdelen van de organisatie moeten worden ingeschakeld.		
Aandachtspunten:	Escalatieprocedure / opstarten BCP - Essentiële contactgegevens: Verantwoordelijken voor het afkondigen van het Business Continuity Plan - Structuur, rollen en verantwoordelijkheden (mandaat) van het crisismanagement team. - Opsomming van de kritieke sleutelprocessen met het telkens daarbij de RPO/RTO, alsook de rangschikking van de processen en activiteiten (incl uitbestede processen). - Afhankelijkheden van andere processen (met de respectievelijke RTO en contactpersonen. Bijvoorbeeld het IT-proces) - Personeel nodig voor de uitvoering van de kritieke sleutelprocessen (contactgegevens, rollen en verantwoordelijkheden,alsook eventueel logistiek, HR en Juridische Zaken, …) - Vitale data nodig voor de uitoefening van het proces en de vindplaats ervan (of van de back-up) - Faciliteiten (bijvoorbeeld vergaderzalen, persruimte, ... voor het geval de sleutelactiviteiten naar een alternatieve locatie dienen te worden verplaatst. - Lijst met kritieke leveranciers of andere dienstverleners - Andere relevante informatie: - Communicatiestrategie (t.a.v. personeel, partners/belanghebbenden, leveranciers, media, …) - Registratie van communicatie (logboek) - Formulieren: templates logboek/incidentenlogboek		
Aandachtspunten voor inspecteurs	BCP toetsen op aandachtspunten en onderzoek of de maatregelen de doelstelling afdekken. BCP heeft overlap met de crisisorganisatie. Bij een crisis (brand oid) hoeft niet altijd het BCP opgestart te worden. Beschikbaarheid: zijn deze ook beschikbaar tijdens crisis?		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Good practice:	Een Business Recovery Plan met: - Doelstelling en scope van het plan - De rollen en verantwoordelijkheden - Het opstarten van het plan (hoe, door wie, wanneer) - De documenteigenaar		
Aandachtspunten:	Het Herstelplan of Business Recovery Plan beschrijft de activiteiten die ondernomen moeten worden om terug te keren naar 'business as usual'. Het plan geeft de recovery targets of milestones aan na een volledige of gedeeltelijke opschorting van bepaalde activiteiten.		
Aandachtspunten voor inspecteurs	Is voorbereid op de verscheidenheid aan schades en situaties die zich voor kunnen doen?		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Good practice:	Van eenvoudig (tabletop) tot uitgebreid (organisatie overstijgend).		
Aandachtspunten:	Het type oefening dat wordt gedaan is afhankelijk van de doelstelling. Daarom moeten deze oefeningen goed voorbereid zijn. De volgende stappen kunnen worden onderscheiden: - Plannen; - Ontwikkelen; - Oefenen; - Evaluatie; - Implementatie. Ga per stap (zie tabblad fase oefening) na in hoeverre hier invulling aan is gegeven. Kritische leveranciers dienen meegenomen te worden in deze plannen.		
Aandachtspunten voor inspecteurs	Zie hieronder "fases oefening" om de aandachtspunten na te gaan. Dekt het geheel aan de tests en oefeningen de belangrijkste processen en risico's af?		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

De fasen van een oefening / test

Fase 1: plannen	- Inschatting maken van de huidige kennis en het vermogen binnen de organisatie om effectief en efficiënt te reageren op een onderbreking; - Definiëren van de scope van de oefening (welk deel van het plan wordt getest?); - De globale doelstelling van de oefening (wat wil men bereiken?); - Samenstelling van het team dat de oefening zal voorbereiden (oefenbegeleiders); - Identificeren van de specifieke doelstellingen (Specifiek, Meetbaar, Aanvaardbaar, Realistisch en Tijdsgebonden) van de oefeningen, de context en de deelnemers.
Fase 2: Ontwikkelen	- Het opmaken van het oefenscenario; - Een algemene lijst met de belangrijkste activiteiten (vb. activeren BCP, opstarten back-up procedure, communicatie aan het personeel…) die tijdens de oefening moeten plaatsvinden. Dit moet overeenstemmen met de gestelde doelen van de oefening; - Opsomming van de acties die per activiteiten moeten worden uitgevoerd; - Indien nodig (afhankelijk van de omvang en het type van oefening) een inschatting maken van het risico dat gepaard gaat met de oefening en eventueel de nodige voorzorgsmaatregelen nemen; - Identificeren van de benodigdheden voor de oefening: administratieve ondersteuning, zalen, oefenmateriaal, eventueel transport, plannen, …); - Een evaluatiemechanisme ontwikkelen (Hoe zal de oefening worden geëvalueerd?); - Voorzien in de nodige mechanismen voor de sturing en begeleiding van de oefening (observatoren, evaluatoren,..); - Voorbereiden en communiceren van de instructies voor de deelnemers aan de oefening; - Het verkrijgen van goedkeuring en ondersteuning van het management.
Fase 3: Oefening	De oefening wordt gestuurd en ondersteund door een of meerdere begeleiders. Het is van belang dat deze mensen opgeleid worden om een oefening te organiseren, sturen en begeleiden, zodat zij duidelijk weten wat hun taken zijn.
Fase 4: Evaluatie	- Onmiddellijk na de oefening een eerste korte debriefing en feedback organiseren voor de deelnemers; - Op het laatst enkele weken na de oefening, het organiseren van een groepsdiscussie waarin aanbevelingen voor de aanpassingen van het plan worden opgesomd; - Opmaken van een schriftelijk rapport van de eindconclusies van de oefening en opstellen van een actieplan.
Fase 5: Post-oefening	- Communiceren van de resultaten van de oefening aan het management; - Goedkeuring van het actieplan door het management; - Organiseren van follow-up sessies voor de deelnemers aan de oefening; - Implementatie van de wijzigingen in de plannen (Business Continuity Plan, Incident Management Plan en eventueel Business Recovery Plan).

Good practice:	Het BCM wordt onderhouden en op een zorgvuldige manier gecommuniceerd. Elke oefening en crisis wordt geevalueerd, verbeterpunten opgesteld en worden tijdig opgelost.		
Aandachtspunten:	Het BCM wordt geevalueerd en bijgewerkt naar aanleiding van: - Oefening en de geidentificeerde verbeterpunten. - In werking treden van BCM plan na een incident. - Een wijziging van de gebruikte producten of diensten van de organisatie (incl. leveranciers). - Een wijziging van beleid, processen of procedures. - Jaarlijkse herziening		
Aandachtspunten voor inspecteurs	Verzoek om uitleg van het laatste grootste incident adhv een logboek waarin het BCM wordt doorgenomen. In het geval dat er geen incident beschikbaar is dan verzoek om de laatste oefening door te nemen (adhv het logboek)		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Good practice:	BCM bewustwording en opleiding dienen geborgd te worden binnen de organisatie.		
Aandachtspunten:	Onder andere: - Workshops - Interne communicatie - Opleidingen & trainingen - Campagnes - Publicaties (oefeningen en crisis)		
Aandachtspunten voor inspecteurs	Gaat om de globale indruk of invulling wordt gegeven aan bewustwording en training. Wees terughoudend met details opvragen.		
Datum:			
Gesproken met:			
Inspecteurs:			
Samenvatting:		**Evidence:**	
Overall indruk over de beheersing van Control doelstelling. Op basis of beheermaatregelen effectief zijn of niet. Vervolgens beargumenteren waarom het wel of niet tot een bevinding leidt waarbij er rekening gehouden moet worden met het risico.			

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Agentschap Telecom

Voor een **veilig verbonden** Nederland

<INSP>,<INSP>

BEVINDINGEN EN VERVOLGAANPAK
Thematische Inspectie <ONDERWERP>

<DATUM>

Agenda

Afgeronde onderwerpen

- <norm nr/hfdstuk> <norm>

Onderwerpen waarbij nadere toelichting nodig is

- <norm nr/hfdstuk> <norm>

Onderwerpen met bevindingen

- <norm nr/hfdstuk> <norm >

Reactie bevindingen en vervolgaanpak

- Reactie op bevindingen
- Acties en planning
- Vervolg

Afgeronde onderwerpen

- <norm nr/hfdstuk> <norm naam>
- <norm nr/hfdstuk> <norm naam>

Voor deze inspectie hebben we geen openstaande vragen meer op deze onderwerpen.

Onderwerpen nadere toelichting nodig

<norm nr/hoofdstuknr><norm>
Vraag 1
Vraag 2

<norm nr/hoofdstuknr><norm>
Vraag 1
Vraag 2

Bevindingen

<norm nr/hoofdstuknr><norm>

- <Punt 1>
- <Punt 2>

Feedback	
Actie:	<In te vullen door AED>
Planning:	<In te vullen door AED>

<norm nr/ hoofdstuknr><norm>

- <Punt 1>
- <Punt 2>

Feedback	
Actie:	<In te vullen door AED>
Planning:	<In te vullen door AED>

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Vervolgstappen

1. AT: Updaten presentatie en mailen naar <AED>
2. <AED>: Invullen feedback in presentatie en mailen naar AT
3. AT: Opstellen eindrapportage en mailen naar <AED>

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Bedrijfsnaam B.V.
T.a.v. de heer/mevrouw xxx
Straatnaam
Postcode Plaats

Hoofdafdeling Toezicht
Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.agentschaptelecom.nl

Contactpersoon
<naam van de inspecteur>
<functie>
Toezicht Wbni
T 06-<nummer>

Datum
xx-xx-20xx

Ons kenmerk
AT-
xx-20xx-x1-x

Met opmerkingen 5.1.2.e **]:** Opvragen bij 5.1.2 e

Bijlagen
-

Betreft: Bevindingen inspecties xxx

Geachte heer/mevrouw

<Bedrijfsnaam> is een aangewezen aanbieder van essentiële diensten (AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (Wbni). Dit houdt in dat <bedrijfsnaam> maatregelen neemt om incidenten te voorkomen en incidenten met aanzienlijke gevolgen meldt. Agentschap Telecom is vanaf 9 november 2018 toezichthouder op deze wet. In het kader van de zorgplicht voerden wij recent een inspectie bij uw organisatie uit. Meer informatie over de inspectie kunt u vinden in de aankondigingsbrief van <datum> met kenmerk <kenmerk>. Hierbij rapporteren wij onze bevindingen.

Over welke inspectie gaat deze rapportage?
In <jaar> voerden wij de volgende inspectie uit:

<kopieer vanuit het risico model>
<kopieer vanuit het risico model>

Met opmerkingen 5.1.2.e **]:** Maak een inschatting of het sanctiebureau moet worden ingeschakeld. Dit zal het geval zijn indien er aanzienlijke risico's ten aanzien van de levering van de essentiële dienst worden geconstateerd. Het sanctiebureau kan afdwingen dat opvolging moet plaatsvinden. Neem de zorgplicht mee in je overwegen. In het geval er geen opvolging plaatsvindt, kan het sanctiebureau op later moment worden ingeschakeld.

Wat zijn onze bevindingen en wat is het vervolg?

Op basis van de inspectie-werkzaamheden heeft Agentschap Telecom op dit moment gee
verdere vragen over de (sub)onderwerpen <x, y en z>. Hiermee is bovengenoemde insp
voor deze (sub)onderwerpen afgerond. Ten aanzien van de volgende (sub)onderwerpen c
<bedrijfsnaam> aanvullende passende en evenredige technische en/of organisatorische
maatregelen te treffen om haar digitale weerbaarheid te verhogen:

1. <(sub)onderwerp[1] | bevinding 1 | reactie van de AED | wijze waarop AT de opvo
   vaststelt>

Met opmerkingen 5.1.2.e **:** Let op: Indien een toezichtstraject afstevent op een bestuurlijke boete en dus van toezicht naar bestraffing verschuift is het belangrijk om voorafgaand aan het verder opvragen van informatie bij een statutaire bestuurder de cautie te geven voor wilsafhankelijke informatie.

De cautie houdt in dat aan de betrokkene wordt medegedeeld dat hij niet verplicht is tot antwoorden. Wilsafhankelijk informatie betreft kortgezegd informatie die de bestuurder niet voorhanden heeft op papier of digitaal maar op ons verzoek vervaardigt. Als de cautie niet is gegeven kan dat later tot bewijsuitsluiting leiden. De cautie hoeft niet aan medewerkers van de organisatie/rechtspersoon te worden gegeven, omdat zij optreden als getuige.

Met opmerkingen 5.1.2.e Neem in deze rapportage alleen afgestemde bevindingen op. Leg de afstemming van de bevindingen vast in het toetsingskader of een gespreksverslag.

[1] ISO27001 referentie nummer

2. <(sub)onderwerp | bevinding 2 | reactie van de AED | wijze waarop AT de opvolging vaststelt>

<of>

Op basis van de gehouden interviews en ontvangen documenten heeft Agentschap Telecom op dit moment geen verdere vragen. Hiermee is bovengenoemde inspectie afgerond.

Vragen?
Mocht u naar aanleiding van dit schrijven vragen hebben, kunt u zich wenden tot onze inspecteurs:

- de heer/mevrouw <naam> <functie> (<mail>) en/of
- de heer/mevrouw <naam> <functie> (<mail>).

Met vriendelijke groet,

5.1.2.e [redacted]

Met opmerkingen 5.1.2.e **:** Stem het rapport af met 5.1.2.e [redacted] orgt voor een handtekening.

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Bedrijfsnaam B.V.
T.a.v. de heer/mevrouw xxx
Straatnaam
Postcode Plaats

Hoofdafdeling Toezicht
Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.agentschaptelecom.nl

Contactpersoon
<naam van de lead inspecteur>
<functie>
Toezicht Wbni
T 06-<nummer>

Datum
xx-xx-20xx

Ons kenmerk
AT-
xx-2022-VI-1

Met opmerkingen 5.1.2.e: Opvragen bij 5.1.2 e

Bijlagen
Onderdelen BCM

Betreft: Aankondiging thema-inspectie 2022

Geachte heer/mevrouw xxx,

Hierbij ontvangt u de aankondiging van een thema-inspectie in het kader van de Wbni zorgplicht.[1] Het onderwerp van deze inspectie wordt Business Continuity Management (BCM). In deze brief leest u hoe wij tot deze keuze zijn gekomen, een korte inleiding over BCM en de planning die wij voor ogen hebben.

Achtergrond
Eind vorig jaar hebben wij dit onderwerp bij u onder de aandacht gebracht. Wij hebben het onderwerp BCM risicogebaseerd gekozen op basis van een intern uitgevoerde analyse.

Inleiding BCM
BCM is een belangrijk onderwerp. Het is onvermijdelijk is dat er situaties ontstaan die zijn veroorzaakt door grote verstoringen of andere dreigende situaties zoals een pandemie of grootschalig kwetsbaarheid. Organisaties dienen in deze gevallen voorbereid te zijn om de impact van die gebeurtenissen op de essentiële dienst te beperken. Dit onderwerp komt aan bod in de bijlage van het Besluit Beveiliging Netwerk- en informatiesystemen (BBNI[2]) onder punt 5: Gevolgen van incidenten beperken.

Agentschap Telecom hanteert onderstaande definitie voor BCM:[3]

"De managementprocessen die de continuïteit van de kritische processen[4] van een organisatie waarborgen. De processen zijn erop gericht om de impact van een verstoring te beperken en zo snel mogelijk weer een acceptabel dienstenniveau te bereiken."

[1] Uw organisatie is een Aanbieder van Essentiële Diensten (AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (Wbni).
[2] https://wetten.overheid.nl/BWBR0041520/2021-06-01
[3] Deze is afgeleid van de definitie van ENISA en aangevuld met ISO22301.
In dit kader gaat het om de kritische processen, die nodig zijn voor de levering van de essentiële dienst

Om de inspectie uit te voeren maken wij gebruik van een toetsingskader. In het toetsingskader worden zes hoofdonderdelen onderscheiden, welke in de bijlage kort worden toegelicht.

Planning
Om de inspectie uit te voeren maken we gebruik van de volgende contactmomenten:

- Kick-off: toelichting scope, toetsingskader en aanpak;
- Inspecties: naar verwachting twee sessies van 2 uur; en,
- Afronding: terugkoppeling resultaten en vervolgacties.

De inspecties worden uitgevoerd in Q3 en Q4 2022 en vinden op locatie plaats.

Binnenkort neemt uw contactpersoon contact met u op voor een afspraak van de kick-off.

Vragen?
Mocht u naar aanleiding van deze brief vragen hebben, kunt u zich wenden tot de in het briefhoofd genoemde contactpersoon.

Met vriendelijke groet,

Met opmerkingen 5.1.2.e: Handtekening door 5.1.2.e verzorgd

5.1.2.e

Bijlage: onderdelen BCM
Hieronder een korte toelichting per deelonderwerp.

Organisatie
- Beleid
- Rollen en verantwoordelijkheden

Inzicht
- Business analyse
- Business Impact Analyse (AT kiest één BIA uit een overzicht)
- Risico analyse

BCM-strategie
- Bepalen van de strategie aan de hand van de eerder vastgestelde RPO en RTO van de diverse processen

BCM-respons
- Incident management (beperkte scope)
- Business Continuity Plan (koppeling met crisisorganisatie)
- Business Recovery Plan

Oefenen – onderhouden – herzien
- Oefenen: inzage in de plannen en uitgevoerde testen.
- Onderhoud – herzien: de triggers die ervoor zorgen dat het BCM actueel blijft (adhv een incident)

Organisatiecultuur
- Opleidingen
- Workshops
- Publicaties
- Etc.

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Kick-off Thema inspectie GTS

Wet beveiliging netwerk- en informatiesystemen (Wbni)

Inspecteurs: 5.1.2.e , 5.1.2.e
Datum: xx Juni 2021
Inspectienummer: GTS-TI-10

Inhoud

1. Aankondiging inspectie
2. Wat is onze scope
3. Wat is onze aanpak
4. Afspraken rond Corona
5. Komende sessie
6. Normenkader

Aankondiging inspectie

Op 20-05-2020 kondigden wij onze inspecties voor het jaar 2020 aan (zie brief met kenmerk AT-EZ/[redacted]).
Teneinde inspectie Overname en detectie, monitoring en logging (DML) niet te laten overlappen is DML verplaatst naar 2021

Deze kick-off sessie is de start van de volgende inspectie(s):

- Thema inspectie detectie, monitoring en logging (DML)

Wat is onze scope?

Naast het hoofdonderwerp Detectie Monitoring en Logging wordt er ook in gegaan op segmentatie, assetmanagement (configuratiemanagement) en incident management. Segmentatie en assetmanagement zijn ondersteunend aan DML en incidentmanagement voor de opvolging. Er wordt beperkt aandacht besteed aan assetmanagement en incident Management (tenzij..).

In scope zijn de diensten en componenten die gebruikt worden om de continuïteit van de essentiële dienst te leveren. Dat betekent dus de OT omgeving inclusief de Beschermingslaag (perimeter) en de bijbehorende beheeromgeving en ondersteunende diensten.

Wat is onze aanpak?

Welke risico’s zijn onderkend en hoe zijn deze uitgewerkt in maatregelen.

Risico → Beleid → Proces → Product

Er worden een aantal dagdelen gepland worden bestaande uit een deel gesprekken en een deel voor de inzage van (gevoelige) documenten. Tijdens de inzage kan additionele toelichting gewenst zijn (standby). Mochten er nog zaken onduidelijk zijn dan kunnen er nog gesprekken in gepland worden.

Dit houdt in dat er minimaal 2 sessies van ca 2 uur elk gepland kunnen worden:
1) Assetmanagement & Segmentatie
3) Detectie Monitoring en Logging & Incident management

Om de inspectie voor te bereiden vragen we u alvast een aantal documenten te delen. Dit zal met name gaan om relevante beleidsdocumenten. Daarnaast vragen we u als voorbereiding op de gesprekken dat er toegang verkregen kan worden tot relevante systemen en documenten.

Wat is onze aanpak?

<u>Uitvoering inspectie</u>
Tijdens de inspectie kunnen wij de volgende werkzaamheden uitvoeren:

- het houden van interviews;
- het beoordelen van documenten en processen;
- het reviewen van door de AED uitgevoerde controle werkzaamheden;
- het uitvoeren van eigen visuele/deelwaarnemingen.

Het normenkader is gebaseerd op ISO27001. Tijdens de inspectie wordt vastgesteld of de getroffen maatregelen passend en evenredig zijn en steunen waar mogelijk op certificeringen.

Agentschap Telecom biedt u een Client Portal aan waarmee u op een veilige manier informatie met ons kan delen.

Bevindingen naar aanleiding van de inspectie lichten wij aan u toe. Daarbij zult u, door middel van hoor en wederhoor, in de gelegenheid wordt gesteld om desgewenst een nadere toelichting te geven en/of aanvullende informatie aan te leveren.

Wat is onze aanpak?

<u>Afronding inspectie</u>
Op basis van onze werkzaamheden stellen wij een rapportage op. Indien nodig maken wij nadere afspraken over een vervolgtraject. U ontvangt deze rapportage ter informatie.

Wij maken inspectierapporten niet openbaar.

Ten aanzien van de Wet openbaarheid van bestuur (Wob) geldt voor de Wbni een uitzondering: vertrouwelijke gegevens die herleidbaar zijn tot een AED zijn niet op te vragen.

Classificatie

	Classificatie 1 (Behandelen binnen AT als ongerubriceerd)	Classificatie 2 (Behandelen binnen AT als departementaal vertrouwelijk)	Classificatie 3 (Behandelen binnen AT als staatsgeheim confidentieel)
Voorbeelden	Mail, openbare informatie en een uittreksel KvK	Beleid en procedures	Pentestrapport met actieve bevindingen en een netwerk- of architectuurplaat
Distributie	5.1.1.b		Alleen in te zien bij de AED*.
Opslag			Alleen in te zien bij de AED*

* Tenzij aanvullende maatregelen in overleg met AED akkoord zijn.

Deze classificatie is gebaseerd op de "Handleiding Rubricering":
http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/szw_2/organisatie_14/szw_5/overszw/een_veilig_szw/informatiebeveiliging_4/Handleiding_rubricering_v28-09-2015.pdf

Hoe gaan we om met COVID?

<u>Inspecties on-site</u>
Deze inspecties werken alleen maar als deze op locatie worden uitgevoerd. Als dat niet mogelijk is vanwege beleid of locatie dan moeten we daar een oplossing voor bedenken. Het is belangrijk om te beschikken over een locatie waar afstand gehouden kan worden.

De alom bekende zaken zijn van toepassing:
1) Niet deelnemen met klachten;
2) Hygiene regels;
3) Afstand;
4) Registratie.

Als er nog regels zijn vanuit NAM dan horen we die graag. Dit speelt met name als er zaken meegenomen moeten worden als mondkapjes of handschoenen.

Mogelijke data

Nog een drietal sessies te plannen

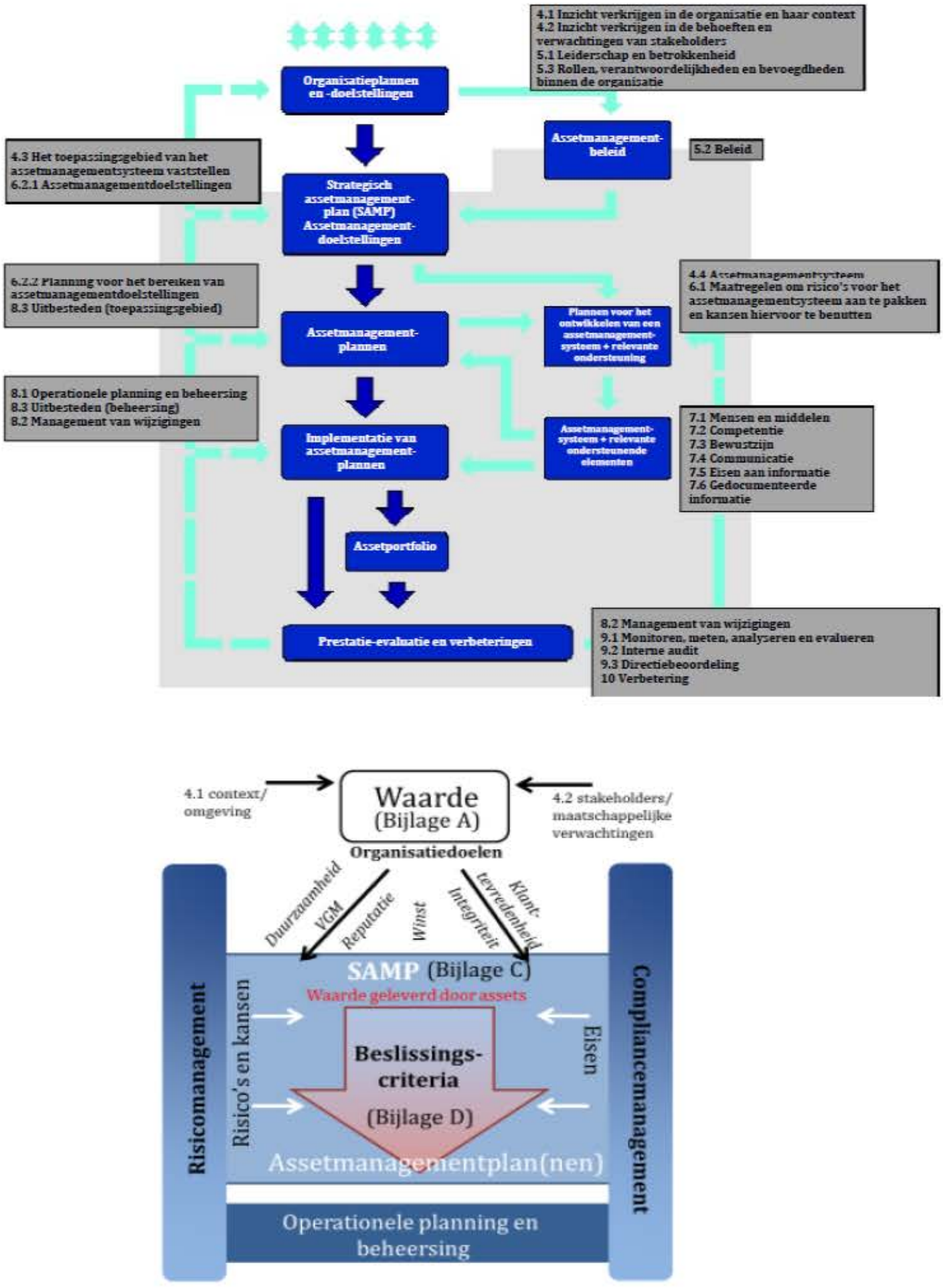
Sessie 1: Assetmanagement en segmentatie
Sessie 2: DML en incidentmanagement
Sessie 3: Afronding en evaluatie

Vragen?

Toetsingskader

Onderwerp	Subonderwerp		Doelstelling	Goodpractice
Assetmanagement				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	8.1.1	Inventariseren van bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.	Een organisatie behoort bedrijfsmiddelen die relevant zijn in de levenscyclus van informatie te identificeren en hun belang te documenteren. De levenscyclus van informatie behoort aanmaak, verwerking, opslag, overdracht, verwijdering en vernietiging te omvatten. Documentatie behoort te worden onderhouden in speciale of bestaande inventarislijsten indien van toepassing.
	8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.	Voor elk van de geïdentificeerde bedrijfsmiddelen behoort het eigenaarschap te worden toegekend.
	8.2.1	Classificatie van informatie	Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Classificaties en de bijbehorende beschermende beheersmaatregelen voor informatie behoren rekening te houden met de zakelijke behoeften om informatie te delen of te beperken, en met wettelijke eisen. Andere bedrijfsmiddelen dan informatie kunnen ook worden geclassificeerd in overeenstemming met de classificatie van informatie die is opgeslagen in, verwerkt door of anderszins behandeld of beschermd door het bedrijfsmiddel.
Segmentering				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	13.1.3	Scheiding in netwerken	De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.	Groepen van informatiediensten, gebruikers en systemen behoren in netwerken te worden gescheiden Een van de methoden om de beveiliging van grote netwerken te beheren is ze te verdeelen in gescheiden netwerkdomeinen. De perimeter van elk domein behoort goed te worden gedefinieerd.
	14.1.2	Toepassingen op openbare netwerken beveiligen	Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.	Informatie die deel uitmaakt van uitwisselingsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen fraudeuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.
Detectie, monitoring, logging				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
DL	A.12.4.1	Gebeurtenissen registreren	Gebeurtenissen vastleggen en bewijs verzamelen.	Logbestanden van gebeurtenissen behoren, voor zover relevant, te bevatten: a) gebruikersidentificaties; b) systeemactiviteiten; c) data, tijdstippen en details van belangrijke gebeurtenissen, bijv. in- en uitloggen; d) identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie; e) registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem; f) registratie van geweigerde en geweigerde gegevens en andere pogingen om toegang te verkrijgen tot bronnen van informatie; g) systeemconfiguratieveranderingen; h) gebruik van speciale bevoegdheden; i) gebruik van systeemhulpmiddelen en -toepassingen; j) bestanden die zijn geopend en het type toegang dat is verkregen; k) netwerkadressen en -protocollen; l) alarmen die worden afgegeven door het toegangsbeveiligingssysteem; m) activering en deactivering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen; n) vertragingen van transacties die door gebruikers in toepassingen zijn uitgevoerd. Logbestanden van gebeurtenissen vormen de basis van geautomatiseerde monitorsystemen die
DL	A.12.4.2	Beschermen van informatie in logbestanden	Gebeurtenissen vastleggen en bewijs verzamelen.	Beheersmaatregelen behoren gericht te zijn op het beschermen van informatie in logbestanden tegen onbevoegde veranderingen en tegen operationele problemen met de logvoorziening, met inbegrip van: a) veranderingen aan de soorten berichten die worden vastgelegd; b) bewerken of verwijderen van logbestanden; c) overschrijden van de opslagcapaciteit van de media met de logbestanden, waardoor gebeurtenissen niet meer kunnen worden vastgelegd of eerder vastgelegde gebeurtenissen worden overschreven. Als onderdeel van het beleid voor het bewaren van verslagen of in verband met eisen om bewijsmateriaal te verzamelen en bewaren kan het nodig zijn om bepaalde auditlogbestanden te archiveren (zie 16.1.7).
DL	A.12.4.3	Logbestanden van beheerders en operators.	Gebeurtenissen vastleggen en bewijs verzamelen.	Houders van een speciaal account zijn mogelijk in staat om de logbestanden op informatieverwerkende faciliteiten die onder hun directe beheer staan te manipuleren. Daarom is het nodig de logbestanden te beschermen en te beoordelen om te handhaven dat speciale gebruikers rekenschap afleggen.
DL	A.12.4.4	Klocksynchronisatie	Gebeurtenissen vastleggen en bewijs verzamelen.	Externe en interne eisen voor weergave, synchronisatie en nauwkeurigheid van tijd behoren te worden gedocumenteerd. Dergelijke eisen kunnen wettelijke, regelgevende of contractuele eisen zijn, nakoming van normen of eisen voor interne monitoring. Er behoort een standaard referentietijd voor gebruik binnen de organisatie te worden gedefinieerd. De aanpak van de organisatie om een referentietijd op basis van externe bron(nen) te verkrijgen en hoe interne klokken betrouwbaar te synchroniseren behoren te worden gedocumenteerd en geïmplementeerd.
L	A.18.1.3	Beschermen van registraties	Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.	Om te voldoen aan deze doelstellingen met betrekking tot het veiligstellen van registraties behoren binnen een organisatie de volgende stappen te worden genomen: a) er behoren richtlijnen te worden verstrekt voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie; b) er behoort een bewaarschema te worden opgesteld waarin registraties en de periode dat ze moeten worden bewaard, zijn vastgelegd; c) er behoort een inventarisoverzicht van bronnen van belangrijke informatie te worden bijgehouden.
M	A.16.1.7	Verzamelen van bewijsmateriaal	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.	Bij het omgaan met bewijs ten behoeve van disciplinaire en wettelijke actie behoren interne procedures te worden ontwikkeld en gevolgd.
Incidentmanagement				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	A.16.1.4	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.	Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Het contactpunt behoort elke informatiebeveiligingsgebeurtenis te beoordelen op basis van de overeengekomen classificatieschema voor gebeurtenissen en incidenten (betreffende informatiebeveiliging, en te besluiten of de gebeurtenis behoort te worden geclassificeerd als informatiebeveiligingsincident. Classificeren en prioriteren van incidenten kan helpen de impact en omvang van een incident te bepalen. In gevallen waarin de organisatie beschikt over een responsteam voor informatiebeveiligingsincidenten (ISIRT), kunnen de beoordeling en het besluit worden doorgeleurd naar het ISIRT voor beveiliging of herbeoordeling. Resultaten van de beoordeling en het besluit behoren in detail in een verslag te

Toetsingskader				
Onderwerp	**Subonderwerp**		**Doelstelling**	**Goodpractice**
Assetmanagement				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	8.1.1	Inventariseren van bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.	Een organisatie behoort bedrijfsmiddelen die relevant zijn in de levenscyclus van informatie te identificeren en hun belang te documenteren. De levenscyclus van informatie behoort aanmaak, verwerking, opslag, overdracht, verwijdering en vernietiging te omvatten. Documentatie behoort te worden onderhouden in speciale of bestaande inventarislijsten indien van toepassing.
	8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.	Voor elk van de geïdentificeerde bedrijfsmiddelen behoort het eigenaarschap te worden toegekend.
	8.2.1	Classificatie van informatie	Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Classificaties en de bijbehorende beschermende beheersmaatregelen voor informatie behoren rekening te houden met de zakelijke behoeften om informatie te delen of te beperken, en met wettelijke eisen. Andere bedrijfsmiddelen dan informatie kunnen ook worden geclassificeerd in overeenstemming met de classificatie van informatie die is opgeslagen in, verwerkt door of anderszins behandeld of beschermd door het bedrijfsmiddel.
Segmentering				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	13.1.3	Scheiding in netwerken	De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden Een van de methoden om de beveiliging van grote netwerken te beheren is ze te verdelen in gescheiden netwerkdomeinen. De perimeter van elk domein behoort goed te worden gedefinieerd.
	14.1.2	Toepassingen op openbare netwerken beveiligen	Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.	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.
Detectie, monitoring, logging				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
DL	A.12.4.1	Gebeurtenissen registreren	Gebeurtenissen vastleggen en bewijs verzamelen.	Logbestanden van gebeurtenissen behoren, voor zover relevant, te bevatten: a) gebruikersidentificaties; b) systeemactiviteiten; c) data, tijdstippen en details van belangrijke gebeurtenissen, bijv. in- en uitloggen. d) identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie; e) registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem; f) registratie van goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie. g) systeemconfiguratieveranderingen; h) gebruik van speciale bevoegdheden; i) gebruik van systeemhulpmiddelen en -toepassingen; j) bestanden die zijn geopend en het type toegang dat is verkregen; k) netwerkadressen en -protocollen; l) alarmen die worden afgegeven door het toegangsbeveiligingssysteem.
DL	A.12.4.2	Beschermen van informatie in logbestanden	Gebeurtenissen vastleggen en bewijs verzamelen.	Beheersmaatregelen behoren gericht te zijn op het beschermen van informatie in logbestanden tegen onbevoegde veranderingen en tegen operationele problemen met de logvoorziening, met inbegrip van: a) veranderingen aan de soorten berichten die worden vastgelegd; b) bewerken of verwijderen van logbestanden; c) overschrijden van de opslagcapaciteit van de media met de logbestanden, waardoor gebeurtenissen niet meer kunnen
DL	A.12.4.3	Logbestanden van beheerders en operators.	Gebeurtenissen vastleggen en bewijs verzamelen.	Houders van een speciaal account zijn mogelijk in staat om de logbestanden op informatieverwerkende faciliteiten die onder hun directe beheer staan te manipuleren. Daarom is het nodig
DL	A.12.4.4	Kloksynchronisatie	Gebeurtenissen vastleggen en bewijs verzamelen.	Externe en interne eisen voor weergave, synchronisatie en nauwkeurigheid van tijd behoren te worden gedocumenteerd. Dergelijke eisen kunnen wettelijke, regelgevende of contractuele eisen zijn, naleving van normen of eisen voor interne monitoring. Er behoort een standaard referentietijd voor gebruik binnen de organisatie te worden gedefinieerd. De aanpak van de organisatie om een referentietijd op basis van externe bron(nen) te verkrijgen en hoe interne klokken betrouwbaar te synchroniseren behoren te worden gedocumenteerd en geïmplementeerd.
L	A.18.1.3	Beschermen van registraties	Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.	Om te voldoen aan deze doelstellingen met betrekking tot het veiligstellen van registraties behoren binnen een organisatie de volgende stappen te worden genomen: a) er behoren richtlijnen te worden verstrekt voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie; b) er behoort een bewaarschema te worden opgesteld waarin registraties en de periode dat ze moeten
M	A.16.1.7	Verzamelen van bewijsmateriaal	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.	Bij het omgaan met bewijs ten behoeve van disciplinaire en wettelijke actie behoren interne procedures te worden ontwikkeld en gevolgd.
Incidentmanagement				**Ga bij de beoordeling van deze doelstelling ten minste in op:**
	A.16.1.4	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de	Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Het contactpunt behoort elke informatiebeveiligingsgebeurtenis te beoordelen op basis van de overeengekomen classificatieschema voor gebeurtenissen en incidenten betreffende informatiebeveiliging, en te besluiten of de gebeurtenis behoort te worden geclassificeerd als informatiebeveiligingsincident. Classificeren en prioriteren van incidenten kan helpen de impact en omvang van een incident te bepalen. In gevallen waarin de organisatie beschikt over een responsteam voor informatiebeveiligingsincidenten (ISIRT),



Figuur D.1 — Besluitvormingskader voor assetmanagement

Laat de checklist na afronding van de inspectie invullen door 5.1.2.e.
Op basis van de ingevulde checkllist leggen de inspecteurs een reactie in dit document vast.
Te allen tijde moet het dossier minimaal voldoen aan de **vetgedrukte** onderwerpen.

Nr	Sub	Onderwerp	Bevindingen reviewer	Reactie inspecteurs
ALGEMEEN				
1	a	De directory van het dossier is omschreven conform de naamgevingsconventie (202x xx x omschrijving)	akkoord	
2	a	Het dossier kent de volgende structuur*: 001 Planning 002 Uitvoering 003 Rapportage	akkoord	
PLANNING				
3	a	In de directory 001 Planning zijn minimaal de volgende documenten opgenomen: **- een ondertekende aankondigingsbrief met RP2000 nummer** - de presentatie voor de kick-off meeting - het te gebruiken toetsingskader **- bewijs dat de aankondigingsbrief is verzonden naar de AED**	akkoord	Bewijs is de mail met bevestiging van portal dat documenten zijn gedownload: ["Bestandsoverdracht oa aankondiging inspectie DML is gedownload.msg"] Daarin genoemd de brief met kenmerk AT-EZ/5.1.2.e [GASU-2020-TI-1-10 Aankondiging inspectie.pdf] waar voor GTS de onderwerpen zijn gecombineerd Risico bij Overname en DML. Ook indirect bewijs: Verslag 20210623 Accountmanagementgesprek GTS - AT definitief.pdf verklaard actiepunt 3: de verzending van de aankondigingsbrief gereed.
	b	De documenten zijn op de templates van het dummy dossier gebaseerd.	akkoord	
	c	De documenten bevatten de juiste naamgevingsconventie.	akkoord	
UITVOERING				
4	a	In de directory 002 Uitvoering zijn minimaal de volgende documenten opgenomen: - het ingevulde toetsingskader - de afstemming van de bevindingen	Toestingskader aangetroffen Afstemming lijkt mondeling te hebben plaatsgevonden	Schriftelijk en mondeling toegelicht, zie 4e. Vragen zijn bescherven in [Voorbereiding GTS DML]. Bevindingen zijn beschreven in de rapporten (het kader is voor intern gebruik), alsmede de Presentatie van bevindingen en uiteindelijke afstemming via review verslag
	b	De documenten zijn op de templates van het dummy dossier gebaseerd.	akkoord	
	c	De documenten bevatten de juiste naamgevingsconventie.	akkoord	
	d	Het ingevulde toetsingskader (of aanvullend document) bevat per norm: - een samenvatting van de resultaten van de uitgevoerde werkzaamheden (interview aangevuld met review documentatie, walkthrough, etc) - een verwijzing naar evidence.	akkoord	
	e	**Uit de afstemming van de bevindingen (of aanvullend document) blijkt dat 'hoor en wederhoor' met de AED heeft plaatsgevonden.**	akkoord	
RAPPORTAGE				
5	a	In de directory 003 Rapportage zin minimaal de volgende documenten opgenomen: **- de ondertekende eindrapportage met RP2000 nummer** **- bewijs dat de eindrapportage is verzonden naar de AED**	akkoord	
	b	Het document is op de templates van het dummy dossier gebaseerd.	akkoord	
	c	Het document bevat de juiste naamgevingsconventie.	akkoord	

* Tip: maak eventueel een (of meerdere) map 'Archief' aan om concept versies in op te slaan. Zo is het direct duidelijk wat de definitieve versies van docementen zijn.

Agentschap Telecom
Ministerie van Economische Zaken

Nederlandse Gasunie N.V.
T.a.v. de heer 5.1.2.e
Postbus 19
9700 MA Groningen
(Verstuurd per mail)

Hoofdafdeling Toezicht
Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.agentschaptelecom.nl

Contactpersoon
5.1 2 e
Toezicht Wbni
T 06-5.1.2.e

Datum
20-05-2020

Ons kenmerk
AT-EZ/5.1 2.e
GASU-2020-TI-1-10

Bijlagen
-

Betreft: Aankondiging inspecties 2020

Geachte heer 5.1.2.e ,

Gasunie is een aangewezen aanbieder van essentiële diensten (hierna: AED) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Dit houdt in dat Gasunie maatregelen neemt om incidenten te voorkomen en incidenten met aanzienlijke gevolgen meldt. Agentschap Telecom (hierna: AT) is vanaf 9 november 2018 toezichthouder op de Wbni. Wij gaan in het toezicht vroegtijdig en open het gesprek aan. Zo worden verwachtingen duidelijk en weet u waar u aan toe bent. Onlangs heeft u contact gehad met onze inspecteurs over de afronding van de eerste ronde inventariserende gesprekken die wij met u hebben gevoerd. In dit gesprek hebben wij, onder andere, de inspecties voor 2020 aangekondigd. In deze brief bevestigen wij de besproken onderwerpen.

Wat zijn de zorgplicht en meldplicht?
AED's nemen passende en evenredige technische en organisatorische maatregelen om hun netwerk- en informatiesystemen te beveiligen. Om deze reden nemen zij maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. Verder melden AED's incidenten met aanzienlijke gevolgen bij AT en het Nationaal Cyber Security Centrum. Dit betreft de meldplicht.

Wat houdt het toezicht in?
AT houdt toezicht op de zorgplicht en meldplicht. AED's vallen onder een actief toezichtbeleid: er vinden geplande inspecties plaats gericht op de beoordeling van het risicomanagementproces en de naar aanleiding hiervan getroffen maatregelen. Inspecties vinden risico gebaseerd plaats op basis van ontwikkelingen, signalen en incidenten. Wij benadrukken dat prioriteiten gedurende het jaar kunnen wijzigen naar aanleiding van de actualiteit.

Inspecties 2020
Op basis van voorgaande werkzaamheden en de actualiteit hebben wij sectorbrede- en AED specifieke dreigingsanalyses uitgevoerd. Voor elke dreiging hebben wij het risico ingeschat. Wij zijn tot de conclusie gekomen dat de volgende twee onderwerpen aandacht vragen voor ons toezicht.

Risicomanagement bij overnames
Binnen de Energiesector vinden een aantal overnames plaats. Een overname is niet zonder risico's en onzekerheden. Potentiële valkuilen zoals het voortijdig weglopen van personeel en onvoldoende testen van overgenomen diensten dienen te worden beheerst. Op dit moment loopt een overname traject waarbij Zebra Gasnetwerk B.V. wordt overgenomen door Gasunie. Vandaar dat wij dit onderwerp voor Gasunie en vervolgens Zebra hebben gekozen.

Detectie, logging en monitoring
Het is in de praktijk zo goed als onmogelijk om indringers buiten de deur te houden met alleen preventieve maatregelen. Goede maatregelen zijn noodzakelijk om onder andere hackaanvallen te detecteren en netwerk- en informatiesystemen dienen faciliteiten te bieden voor logging en monitoring. Randvoorwaardelijk voor deze activiteiten is een betrouwbare inrichting van asset management, segmentering van systemen en een aansluiting op het incident management proces.

Planning
U heeft telefonisch aangegeven dat de inspectie op het thema risicomanagement bij overnames kan worden opgestart en zo veel mogelijk op afstand kan worden afgehandeld. Op korte termijn geven wij graag een presentatie, met een nadere toelichting, aan medewerkers van Gasunie die bij de overname zijn betrokken.

Voor de inspectie detectie, logging en monitoring nemen wij op een later tijdstip contact met u op om deze in de plannen.

Vragen?
Mocht u naar aanleiding van deze brief vragen hebben, kunt u zich wenden tot de in het brievenhoofd genoemde contactpersoon.

Met vriendelijke groet,

5.1.2.e
[redacted]
Toezicht Wbni