Bijlage 6

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Inspectierapport KPN B.V.

Zorgplicht continuïteit en bereikbaarheid 112

Colofon

Aan	Directie KPN
Van	Agentschap Telecom
Nummer	Definitief
Datum	15 juni 2018
Leden	

Inhoud

Inleiding

Agentschap Telecom stelt, bij het uitvoeren van haar missie "Agentschap Telecom waarborgt de beschikbaarheid en betrouwbaarheid van de IT- en communicatienetwerken, zodanig dat Nederland veilig en verbonden is", het maatschappelijk belang centraal. Incidenten in de telecomsector kunnen economisch en maatschappelijk veel schade aanrichten. Een aantal processen[1] binnen de telecom/ICT sector zijn eind 2017 aangemerkt als vitaal. Vitale processen zijn processen die bij uitval of verstoring tot ernstige maatschappelijke ontwrichting kunnen leiden. Met het oog op het maatschappelijk belang is het vanzelfsprekend dat de continuïteit van netwerken en/of diensten op een zo hoog mogelijk peil blijft of wordt gebracht en de maatschappelijke en economische impact van incidenten en calamiteiten tot het minimum wordt beperkt. Dit draagt bij aan het vertrouwen in de telecom/ICT sector.

Aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten (hierna: aanbieders) zijn verplicht passende technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid en integriteit van netwerken en/of diensten te beheersen. Voor aanbieders van openbare telefoniediensten geldt, bij technische verstoringen of uitval van elektriciteit, de verplichting om alle noodzakelijke maatregelen te treffen. Het doel hiervan is de continuïteit en beschikbaarheid van netwerken en/of diensten zoveel mogelijk te waarborgen.
De regelgeving over continuïteit is open norm wetgeving. Een open norm bevat een globaal geformuleerde doelstelling of globaal geformuleerde gedragsvoorschriften die de normadressaten ruimte laten om zelf te bepalen op welke wijze het doel wordt gerealiseerd of aan de gedragsvoorschriften wordt voldaan. Normontwikkeling is daarbij essentieel. In het overlegorgaan NCOT[2] hebben de vier aangewezen telecomaanbieders (Tele2, T-Mobile, KPN en VodafoneZiggo) in samenwerking met DGETM[3] op 31 augustus 2017 hiervoor de basis gelegd.

[1] Internet en dataverkeer; internettoegang en datadiensten; spraakdiensten en sms; plaats- en tijdsbepaling middels GPS
[2] NCOT: Nationaal Continuïteitsoverleg Telecom
[3] DGETM: Directoraat Generaal Energie, Telecom en Mededinging

1 Doelstelling en scope

1.1 Doelstelling

Het doel van de inspectie is om inzicht te krijgen in de invulling van de zorgplicht continuïteit en bereikbaarheid 112 door KPN. Uitgangspunt is de set van continuity objectives (afspraken set) die in het NCOT van 31 augustus 2017 is vastgesteld door de vier telecomaanbieders en DGETM. Deze bestaan uit vijf beheersdoelstellingen en 22 normen/criteria. Deze set vormt de eerste invulling van de passende en noodzakelijke maatregelen van de zorgplicht continuïteit. De vereiste maatregelen worden per aanbieder ingevuld. De continuity objectives zijn primair gebaseerd op de Europese ENISA[4] guidelines.

De doelstelling van deze inspectie is voor het agentschap tweeledig:

1. Het verkrijgen van inzicht in de invulling van de zorgplicht. Uitgangspunt is de afsprakenset zoals vastgelegd binnen het NCOT. Daarnaast inzicht verkrijgen in de noodzakelijke voorzieningen die zijn getroffen om de ononderbroken toegang tot 112 te waarborgen.
2. Het op basis van het verkregen inzicht stimuleren van de sector om het bereikte niveau te behouden dan wel te verbeteren ten aanzien van de zorgplicht continuïteit.

1.2 Scope

Aanbieders hebben een zorgplicht met betrekking tot de continuïteit van hun aangeboden dienst(en) en/of netwerk(en). Dit is geregeld in artikel 11a.1 van de Telecommunicatiewet (Tw) en het Besluit continuïteit openbare elektronische communicatienetwerken en -diensten (hierna Besluit continuïteit).
Naast Hoofdstuk 11a Tw heeft Agentschap Telecom als wettelijke taak toezicht te houden op artikel 7.7, derde lid, van de Tw.
Buiten de scope van deze inspectie vallen netwerken en/of diensten die uitsluitend bedoeld zijn voor het verspreiden van programma's, zoals radio- of Tv-programma's.

[4] ENISA: European Union Agency for Network and Information Security

2 Werkwijze

Insteek van de inspectie is primair de opzet. Er zal, voor zover mogelijk, ook gekeken worden naar het bestaan en de werking aangezien de PDCA cyclus als één van de criteria wordt gehanteerd. De aantoonbaarheid krijgt vorm door middel van documenten en inzage in de systemen zoals door die KPN worden gehanteerd.

De inspectie bestaat uit de volgende drie fasen:
Informeren
Het telefonisch informeren van KPN, het plannen en het houden van een voorbereidingsgesprek (27 november 2017).

Voorbereiding inspectie
In fase twee worden voorbereidingen getroffen van de inspectie, het verzenden van de aankondigingsmail (15 januari 2018) inclusief het opvragen van documenten, de bestudering hiervan na ontvangst (2 februari 2018) en het inregelen van de inspectie.

Locatiebezoek, opstellen en aanbieden rapportage
Deze fase start met de uitvoering van de inspectie op locatie (19 en 20 februari 2018). Dit bestaat uit interviews en het inzien van nieuwe documenten. Vervolgens wordt de concept rapportage opgesteld. Deze wordt ter verificatie voorgelegd aan KPN (11 april 2018) en de definitieve rapportage aangeboden aan de directie van KPN. Agentschap Telecom verwacht van KPN een formele reactie op de inspectieresultaten.

3 Waarnemingen

In dit hoofdstuk zijn de beheersdoelstellingen, normeringen/criteria en maatregelen nader uitgewerkt. De beheersdoelstellingen zijn onderverdeeld in vijf hoofdonderwerpen (B). Deze zijn vervolgens nader uitgewerkt in 22 normen/criteria (C). KPN geeft voor iedere C aan een maatregel te hebben genomen.

3.1 Beheersdoelstelling B1: Beleid, Governance en risicomanagement

De organisatie heeft continuïteitsbeleid, een adequate governance van de continuïteit en hanteert een risicomanagement-framework.

Continuïteitsbeleid

C1.1
Normen/criteria
Er is continuïteitsbeleid vastgesteld waarin de continuïteit van de dienstverlening is geadresseerd.

Maatregel KPN
KPN Security Policy (KSP) op KPN's intranet.

Bevindingen
KPN beschikt over vastgesteld continuïteitsbeleid. Hierin is de dienstverlening geadresseerd. Dit beleid is opgenomen in de KPN Security Policy (KSP) en bestaat uit een Top level Policy, rationales en requirements. Deze drie elementen zijn verplicht voor alle bedrijfsonderdelen van KPN. Daarnaast zijn er guidelines die dienen als richtlijnen. De focus ligt op de vitale en kritieke diensten/halffabrikaten, en vervolgens op de maatwerk- en overige diensten. Nieuwe diensten moeten van begin af aan voldoen.
Er kunnen zich situaties voordoen dat een bestaande situatie niet voldoet aan de KSP. Dan moet de KSP alsnog worden geïmplementeerd. Als de KSP niet toegepast kan worden, is sprake van een exceptie die tijdelijk wordt toegestaan. Dit wordt in het exceptieregister opgeslagen waarbij aanvullende maatregelen vereist zijn om het risico te mitigeren.

Er wordt op verschillende wijzen gerapporteerd naar de
en hoger. Ten eerste gebeurt dit via Weekly RiskIntel reports. Dit zijn
reitelijke rapportages. Deze worden gerapporteerd aan de Raad van Bestuur leden.
Daarnaast zijn er maandelijkse rapportages (Management Letter) waar
gerapporteerd wordt door aan de Chief Operational Officer (COO) over de
stand van zaken. Hierbij wordt o.a. gerapporteerd over prevents (policy's), detects
(bevindingen van het responds (bevindingen van het
n verify (bevindingen van de
. Hierbij zijn prioriteiten benoemd, cyber gerelateerd en
voor continuïteit geeft een totaal beeld van de
samenhang tussen halfrabrikaten en diensten, en wordt verder aangevuld met
applicaties en gebouwen. Het is een database waarin de resultaten van het Business
Continuity Management (BCM) proces voor alle diensten zijn vastgelegd maar ook
de continuïteitsplannen. Deze tool biedt KPN het inzichtelijk maken van onderlinge
afhankelijkheden en hierop actie te gaan ondernemen. Deze tool is gestart met het

ondersteunen van de Business Impact Analysis (BIA) en wordt stapsgewijs steeds verder uitgebreid.
Tot slot wordt er gerapporteerd in de kwartaalrapportages van de Document of Representation (DoR) naar de Raad van Bestuur waarin elementen uit de management letters zijn meegenomen.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- KPN continuïteitsplan t.b.v. de Telecomwet, december 2017
- [redacted]

C1.2
Normen/criteria
Sleutelfunctionarissen (key personnel) zijn bekend met en zich bewust van het continuïteitsbeleid.

Maatregelen KPN
in het CISO team die elk een deel van de organisatie als scope hebben, in de organisatie onderdelen.
houden contact met het management, en andere functionarissen.

Bevindingen
KPN heeft binnen het CISO team sleutelfunctionarissen benoemd, de zogenaamde Deze medewerkers hebben een deel van de organisatie als scope waar zij zorgen voor bekendheid van het continuïteits- en securitybeleid bij de managers en werknemers in de organisatie, en toezien op de uitvoering van de KSP binnen deze bedrijfsonderdelen samen met de Daarnaast dienen zij als vraagbaak. De naken onderdeel uit van de specifieke onderdelen van de organisatie. Zij hebben als taak het uitvoeren van KSP binnen hun organisatieonderdeel. De vormen de communicatielijn tussen CISO, de managers en de

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]

C1.3
Normen/criteria
Continuïteitsbeleid wordt herijkt naar aanleiding van incidenten en/of periodiek herijkt.

Maatregelen KPN
Input uit Be Alert evaluaties; Life Cycle Management KSP: elk kwartaal een update van KSP op basis van input voor beleid vanuit de organisatie.

Bevindingen
Het continuïteitsbeleid wordt per kwartaal geactualiseerd op basis van signalen vanuit de organisatie en CISO zelf. Jaarlijks zijn er één major en drie minor momenten om wijzigingen door te voeren. De laatste wijziging betreft een forse

aanpassing van de KSP. Er is een nieuwe tool [redacted] door KPN ontwikkeld waarin alle organisatieonderdelen hun analysebevindingen en plannen moeten vastleggen. De planning is dat eind 2019 de tool is gevuld voor alle diensten/halffabrikaten.

Het [redacted] dashboard is een real time dashboard wat inzicht geeft in de kwetsbaarheden van IT systemen op basis van een [redacted] Gerapporteerd wordt o.a. op basis van de PHOSI (Potential Harm Of Security Incident) bedrag in euro's. Aan de hand van een demonstratie heeft KPN een nadere toelichting op de werking hiervan gegeven.
Alle (nieuwe) diensten moeten voldoen aan de CISO/KSP eisen. Exceptie gelden voor maximaal één jaar en worden door het CISO bewaakt.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]

Governance en risicomanagement

C1.4
Normen/criteria
Er is een lijst van de belangrijkste continuïteitsrisico's opgesteld (per dienst), rekening houdend met de belangrijkste dreigingen ten aanzien van de continuïteit van een dienst.

Maatregelen KPN
RisicoTool per dienst/halffabrikaat met risicobeoordeling aan de hand van een dreigingenlijst.

Bevindingen
KPN beschikt over een lijst van continuïteitrisico's, genoemd een dreigingenlijst. Deze zijn onderverdeeld in vier soorten dreigingen. Deze lijst maakt onderdeel uit van het risk assessment binnen het BCM proces. Jaarlijks moeten alle vitale en kritieke diensten/halffabrikaten het BCM proces opnieuw doorlopen waaronder een risk assessment. De resultaten van het BCM proces inclusief het risk assessment moeten vanaf 1 januari 2018 vastgelegd worden in de tool.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]

C1.5
Normen/criteria
Er is een risicomanagement methodologie (en/of instrumentarium) opgezet (gebaseerd op industrie-standaarden).

Maatregelen KPN
RisicoTool per dienst/halffabrikaat met risico assessment op basis van dreigingenlijst en een risktreatment plan.

Bevindingen
De risicomanagement methodologie bestaat uit twee onderdelen, de scoring op de dreigingenlijst en vervolgens het opstellen van een risktreatmentplan. Hierin moeten alle benoemde risico's voorzien worden van een maatregel, accepteren of mitigeren. De risk treatment staat standaard op mitigeren. De producteigenaar van de dienst is eindverantwoordelijk. Dit alles wordt vastgelegd in de RisicoTool.
CISO beoordeelt voor iedere dienst de risk assessment, ook of de beoogde risicoacceptaties en maatregelen op het juiste niveau zijn gemandateerd. Naast de dreigingenlijst kunnen bij een risk assessment ook andere risico's betrokken worden. Hierbij wordt gedoeld op "van welke risico's lig je wakker?".

Jaarlijks wordt door CISO het strategisch riskassesment voorbereid op basis van de actuele ontwikkelingen intern en extern. Voor het monitoren van kwetsbaarheden is een realtime dashboard ontwikkeld (zie C1.3).

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:
- [redacted]

C1.6
Normen/criteria
Risico assessments worden herijkt naar aanleiding van belangrijke wijzigingen of incidenten en/of periodiek herijkt.

Maatregelen KPN
Jaarlijkse update met als input incidenten en ontwikkelingen van de dienst/halffabrikaat. Update RisicoTool bij een grote wijziging van de dienst.

Bevindingen
De evaluaties van de Be Alert incidenten (post mortems) vormen input voor het eventueel actualiseren van de dreigingenlijst. Dit geldt ook voor de uitkomsten van de jaarlijkse BCM updates van de vitale en kritieke diensten/halffabrikaten.
Single Point of Failure (SPoF) lijsten bestaan niet meer. Deze worden ingevuld door middel van opgedane inzichten binnen de tool (onderlinge afhankelijkheden) en SPoFs uit de Risico Assessments. Door op verschillende schaalniveaus te kijken kunnen SPoF's op een lokaal niveau een probleem zijn (bijvoorbeeld geen redundantie) maar op een hoger niveau niet (wel redundantie). RvB bepaalt de Risk Appetite – Het vertaalt dit naar de organisatie.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:
- [redacted]

Rollen en verantwoordelijkheden

C1.7
Normen/criteria
Rollen en verantwoordelijkheden ten aanzien van continuïteit zijn toebedeeld aan personeel.

Maatregelen KPN
KSP BCM proces definieert de verantwoordelijkheden, en BIA en RisicoTool wijzen de rollen aan personen toe die verantwoordelijk zijn, ook voor geaccepteerde risico's.

Bevindingen
Binnen het BCM proces zijn verantwoordelijkheden en rollen gedefinieerd. Deze zijn vormgegeven in schema's. Dit geldt ook voor de RiskTool. Hierin staat aangegeven welke functies gemandateerd zijn voor geaccepteerde risico's.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:
- [redacted]
- [redacted]
- [redacted]

C1.8
Normen/criteria
Rollen en verantwoordelijkheden ten aanzien van continuïteit worden herijkt op basis van wijzigingen of incidenten.

Maatregelen KPN
Organisatiewijzigingen worden verwerkt bij jaarlijkse update van de BIA en de RiskTool. Incidenten die verantwoordelijkheidsvacuüm aan het ligt brengen worden in het Be Alert evaluatieproces met een aan betrokken management toebedeelde actie opgevuld.

Bevindingen
In de jaarlijks verplichte actualisatie van alle diensten/halffabrikaten worden organisatiewijzigingen meegenomen. Daarnaast geven evaluaties van incidenten vanuit het Be Alert proces inzicht in de risico's t.a.v. (ontbrekende) verantwoordelijkheden. Hiervoor worden acties ingezet die vallen onder de verantwoordelijkheid van de betreffende manager van de betreffende kritieke dienst/halffabrikaat). Voor evaluaties van changelogs geldt eenzelfde aanpak.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:
- [redacted]
- [redacted]

3.2 Beheersdoelstelling B2: Asset management

De organisatie heeft invulling gegeven aan asset management ten aanzien van de continuïteit kritieke onderdelen en systemen.

Asset management

C2.1
Normen/criteria
Er is een overzicht van kritieke onderdelen en systemen voor de continuïteit (van een dienst) opgesteld.

Maatregelen KPN
Opdeling van een commerciële dienst in halffabrikaten in de BIA Excel, tab Halffabrikaten; halffabrikaten hebben een eigen scope beschrijving, impact Assesment (IA) en RT.

Bevindingen
KPN heeft ter verificatie van de maatregelen die genomen zijn om aan de beheerdoelstelling en normering/criteria te voldoen een aantal documenten aangeleverd die met name ingaan op de Business impact analyse en de BCM impact analyse.
Asset beheer is één van de sub area's van de KSP. Voor de classificatie van de asset wordt een BCM proces doorlopen. Daarbij zijn halffabricaten, diensten en gebouwen in scope. Voor het bepalen van de classificatie wordt een business impact analyse (BIA) per asset uitgevoerd. Hierin wordt bepaald of een asset kritieke, een high of een medium classificatie krijgt. Deze BIA wordt jaarlijks of bij innovatie door de product manager uitgevoerd. Binnen de BCM IA wordt meegenomen welke diensten (commercieel/vitaal) afhankelijk zijn van het betreffende asset, welke eisen door de diensten hieraan worden gesteld en wie verantwoordelijk en aansprakelijk is binnen KPN. De resultaten van de BIA en IA wordt opgeslagen in het nieuwe systeem Hierdoor wordt een overzicht gecreëerd waarbij de afhankelijkheden tussen diensten en assets inzichtelijk wordt gemaakt. Inzage is gegeven in de applicatie aan de hand van een aantal voorbeelden.

De RvB stelt jaarlijks op basis van het strategisch Risk Assessment een lijst samen waarin onder andere de kritieke diensten en kritieke gebouwen zijn opgenomen. Momenteel zijn geïdentificeerd en is aan de hoogste risicoklasse toegekend. Deze lijst is ter inzage beschikbaar gesteld.

Voor het beheer van assets is een rationale (KSP-RA-108) opgesteld binnen de KSP met als doel dat assets gedurende hun lifecycle zodanig worden beheerd dat ze operationeel blijven (fit for purpose). Er is binnen KPN altijd een verantwoordelijke (contract) manager aangewezen. Tijdens de inspectie is aangegeven dat voor de technische apparatuur het beheer bij de Managed Service Providers (MSP) is belegd.

112/Noodcommunicatievoorziening (NCV)
De diensten 112 en NCV zijn door de RvB aangewezen als kritieke diensten. In eerder onderzoek naar deze diensten door Agentschap Telecom is vastgesteld dat

bij navraag tijdens de inspectie bleek dat dit niet bekend was bij de aanwezigen en ook niet de reden van het plaatsen van deze apparatuur in
Achteraf is de navolgende toelichting gegeven: "De plaatsing is destijds vooral ingegeven door waar beschikbare ruimte was. De

platformen staan nog steeds

In de aangeleverde documenten betreffende de beveiliging van (wordt het volgende aangegeven:

Bij medegebruik door derden moeten de gezamenlijke verkeersruimten met de derden worden gezien als 'buitenschil'. (KSP-RE-197)

Er moet rekening worden gehouden dat KPN ruimte moet bieden aan Derden/ TELCO's:

1. Deze derden moeten buiten de processen van KPN worden gehouden.
2. Een separate ingang rechtstreeks in/naar hun ruimte is hierbij vereist. Is dit niet mogelijk, dan moet de routing tot de verhuurde ruimten buiten het primaire proces van KPN worden gehouden.
3. De TELCO ruimte wordt gezien als een zelfstandig compartiment.
4. De scheiding tussen het KPN en het TELCO gedeelte moet gelijkwaardig zijn aan die van een buitenschil. (KSP-RE-156)".

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

C2.2

Normen/criteria

In contracten met derde partijen (third parties) worden continuïteitseisen gesteld om te borgen dat afhankelijkheden van derden geen negatief effect hebben op de continuïteit.

Maatregelen KPN

KSP eist het in contracten met derden het opstellen van een Security Annex, de via tooling van de juiste requirements wordt voorzien.

Bevindingen

Er is vastgesteld beleid met betrekking tot de continuïteitseisen bij derden. Middels een procedure wordt vastgesteld welke requirements, vanuit het KSP vereist zijn voor het product dat wordt geleverd door de desbetreffende derde (KSP-GL-47). Na het vaststellen van de requirements worden deze opgenomen in een Security Annex. Een sjabloon (KSP-GL-49) een dergelijke Security Annex is beschikbaar. Doel is om de continuïteitseisen (KSP) bij de derde van toepassing te verklaren. Ter illustratie hiervan heeft KPN aan de hand van een contract van een derde laten zien hoe deze annex hierin is vormgegeven. KPN is gerechtigd om audits, penetration en andere vulnerability test uit te voeren bij de derde. Daarnaast moeten derden ook self assessments uitvoeren.

Security incidenten bij MSP's worden rechtstreeks bij [redacted] van KPN gemeld. Overige incidenten moeten tijdig hersteld worden en worden gerapporteerd bij de betreffende[redacted]

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]
- [redacted]
- [redacted]

C2.3

Normen/criteria

De beschrijving van de dienstverlening of het netwerk is dusdanig dat eindgebruikers zich bewust kunnen zijn van mogelijke onderbrekingen in de continuïteit en duur en omvang daarvan. Het is aan gebruikers zelf om passende maatregelen te treffen.

Maatregelen KPN

In dienst- en productomschrijving en levervoorwaarden of in proposals voor individuele klanten worden de beschikbaarheidseigenschappen omschreven. Bij offertetrajecten zijn de continuïteitseisen en wensen van de klant integraal onderdeel van het bid proces.

Bevindingen

Het maatschappelijke belang wordt per dienst bepaald. Tijdens het interview geeft KPN aan dat grootverbruikers/zakelijke klanten zelf goed in staat zijn om op basis van hun eigen continuïteit het juiste product met de daarbij behorende specificaties te definiëren. Op basis van deze eisen zal een passende dienstverlening of netwerk worden aangeboden.
Voor het MKB zijn de sales managers bij KPN of partners dusdanig geïnstrueerd dat de continuïteit een verplicht onderwerp van gesprek is. Er wordt gewezen op de continuïteit van de dienstverlening en de impact van een onderbreking. Daarbij worden alternatieven aangedragen. Bij klachten over onderbrekingen wordt onderzocht in hoeverre de betreffende sales manager het onderwerp continuïteit naar behoren heeft besproken en de klager tijdens het gesprek voorafgaande aan de overeenkomst is gewezen op de impact van een mogelijke onderbreking en uitleg heeft gekregen over de betekenis van de cijfers. De performance wordt opgenomen in de overeenkomst.
Voor de consument is in de algemene voorwaarden de dienstverlening opgenomen. KPN heeft aan de hand van haar website laten zien welke specifieke diensten worden aangeboden. Naast de aangeboden kwaliteit wordt ook de minimum aangeboden performance opgenomen.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- Algemene voorwaarden dienstverlening, 20 februari 2018
- Website KPN, 20 februari 2018

3.3 Beheersdoelstelling B3: Operationele procedures

De organisatie heeft operationele procedures voor het werken met voor continuïteit kritieke onderdelen en systemen.

Operationele procedures

C3.1
Normen/criteria
Ten behoeve van het werken met kritieke onderdelen en systemen voor de continuïteit zijn operationele procedures opgesteld en die worden door het personeel gevolgd.

Maatregelen KPN
Interne en externe beheer- en installatiepartijen werken met vastgestelde procedures en normtijden voor herstel bij uitval. Bij evaluaties van incidenten die de normtijden hebben overschreden worden correctieve maatregelen genomen en de procedures overeenkomstig bijgesteld.

Bevindingen
Operationeel
Binnen KPN worden alle procedures vastgelegd in de KSP. Verschillende artikelen zoals fysieke beveiliging, KPN Company Card en het beheren van assets worden omschreven en toegelicht in de KSP. Naast deze verschillende artikelen worden diverse eisen zoals beveiligde ruimtes, bescherming tegen externe gevaren en registratie toegang omschreven met bijbehorende gerelateerde zaken en één of meerdere van de bovengenoemde artikelen.

Het proces van de toegang tot verschillende ruimten wordt door de[ ]monitord. Daarnaast zorgt CISO ervoor dat alle vastgelegde procedures door[ ]worden uitgevoerd. Mochten er incidenten plaatsvinden, dan worden deze aan CISO gerapporteerd.
Ruimten waarin apparatuur staat opgesteld voor de diensten/netwerken in de operationele gebouwen zijn ingedeeld in categorieën met hun eigen fysieke beveiliging. Zo wordt er bijvoorbeeld een onderscheid gemaakt tussen het beheren van de mobiele masten en de gebouwen (zogenaamde "telefooncentrales").

In geval van netwerk en/of dienst uitval, werken zowel interne als externe beheer- en installatiepartijen met vastgestelde procedures en normtijden voor herstel. Bij evaluaties van incidenten die de normtijden hebben overschreden worden correctieve maatregelen genomen en de procedures overeenkomstig bijgesteld. Daarnaast is er een[ ]beschikbaar die inzetbaar is bij uitval van de[ ]

Problem management
Problem management houdt zicht op, en analyseert de incidenten die niet onder de Be Alert procedure (klantimpact) vallen. Vervolgens worden deze incidenten binnen de reguliere operatie afgehandeld.

Het monitoren van elementen
KPN is in bezit van een[ ]le als een datawarehouse fungeert voor de Information Technology (IT) aspecten. Daarnaast

is er vanuit de Technische Infrastructuur (TI) omgeving gebleken dat alle apparatuur inclusief softwareversies(wordt.
De netwerk elementen worden in de Network Operation Centers (NOC) in bewaakt (de zogenoemde "elementen bewaking") en alle alarmeringen worden via geclusterd en gemonitord. Dit vormt de basis van de dienstbewaking door Service Quality Center. Vanuit de IT omgeving geeft het een realtime inzicht van de kwetsbaarheden van de netwerk elementen (zie C1.3).

Bij KPN is lifecycle beheer van toepassing en is geheel belegd bij de MSP. Daarnaast worden de eigenschappen van het netwerk vanuit de operatie beheerd, bijvoorbeeld load-balancing 50% - 50%. Dit gebeurt vanuit de desbetreffende verantwoordelijke afdeling.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten

- [redacted]

Change management

C3.2
Normen/criteria
Bij veranderingen in onderdelen van het netwerk of de dienst die kritiek zijn voor de continuïteit worden vooraf vastgestelde procedures gevolgd.

Maatregelen KPN
Het changemanagement proces werkt met de Change Advisory Board (CAB) waar de risico's van changes worden beoordeeld op het honoreren van de klantafspraken en het minimaliseren van de continuïteitsrisico's voor kritieke en vitale diensten.

Bevindingen
Change management wordt door KPN als volgt gedefinieerd: het toevoegen, wijzigen of verwijderen van alles dat van invloed zou kunnen zijn op IT/TI diensten. Binnen changemanagement kunnen meerdere soorten changes worden onderscheiden, met name: Standard change, Normal change, Emergency change en Urgent change. Deze changes volgen dezelfde processtroom, hoewel, de RACI van de verschillende soorten changes kan echter verschillen. Bijvoorbeeld, een Standaard change is een change die pre-geautoriseerd is via het Change management proces, terwijl bij een Emergency change het Change management proces alleen gebruikt wordt voor de administratie en om het traceerbaar te maken.

Proces en rollen
Het primaire doel van het Change Managementproces binnen(is aanwezig om ervoor te zorgen dat wijzigingen op een gecontroleerde manier worden vastgelegd, gecategoriseerd en geëvalueerd, geautoriseerd, geprioriteerd, gepland, getest, geïmplementeerd, gedocumenteerd en beoordeeld.
De Change Managementproces bestaat uit vijf relevante rollen. Deze rollen worden als volgt gedefinieerd:

- werkt op de afdeling Change Control. Change Control is verantwoordelijk voor het valideren van ingediende changes om de kwaliteit van het proces te waarborgen;
- houdt in dat een change door verschillende personen kan worden aangevraagd. Hiernaast bepaalt de zelf welke change een prioriteit is, moet het runbook (impact, process, rollback, classification) geheel doorlopen en is zelf verantwoordelijk voor de aanvraag;

- etekent dat een change alleen door een geautoriseerde voor goedkeuring bij de relevante autoriteiten kan worden aangevraagd. De applicatie/elementhouder is verantwoordelijk voor het benoemen van de
- verantwoordelijk voor het autoriseren van changes. De functie van de kan worden vervuld door één persoon of een groep personen;
- Wanneer een change wordt uitgevoerd, wordt dit gecoördineerd door een centrale afdeling. De persoon die verantwoordelijk is voor deze coördinatie op de centrale afdeling, wordt een

Vervolgens werkt het Change Managementproces met de Change Advisory Board (CAB).

Vanuit de geleverde documentatie blijkt het volgende:

-
-

De combinatie van deze vier elementen zal resulteren in één van de volgende classificaties en autorisatieniveaus die nodig zijn:

- Low, mag uitgevoerd worden door de
- Medium, onder beheer van de
- High, onder beheer van de

Het monitoren van changes

Het zo genoemde "first time right" (FTR) percentage van uitgevoerde changes is Het merendeel van de overige her-planning. KPN geeft aan dat deze overige eer impact heeft dan vooraf bepaald door de
Bovendien, de meest belangrijkste KPI's zijn FTR en het aantal changes met bijbehorende downtime.

KPN geeft aan dat er gemiddel hanges zijn per week. Capaciteit en software updates zijn de meest voorkomende changes. Er wordt vervolgens een maandelijkse rapportage per afdeling opgesteld over de verwerkte changes met hun impact.
Bij opvallende afwijkingen in de zogenoemde change categorie "not first time right" wordt ingegrepen en afhankelijk van de risico van de change kan het hoog geëscaleerd worden. Eén van de mogelijkheden in een dergelijk geval is een No/Go beslissing van de CAB voor changes.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

3.4 Beheersdoelstelling B4: Voorbereiding contingencies en herstel

De organisatie is voorbereid op contingencies en het snel herstellen van de diensteverlening na uitval.

Contingency planning

C4.1
Normen/criteria
Er is een contingency plan opgesteld met reactieve maatregelen indien risico's zich voordoen.

Maatregelen KPN
Er worden afhankelijk van de scope diverse soorten continuïteitsplannen vastgelegd. Een BCM tool waarin als deze plannen worden opgeslagen en onderhouden is in ontwikkeling.

Bevindingen
KPN beschikt over recovery plans. Met name Technical Recovery Plan (TRP), Chain Recovery Plan (CRP), Service Repair Plan (SRP). De recovery plannen zijn een onderdeel van het Services Continuity Management (SCM) welke onder het beleid van de KSP valt. Het is verplicht een TRP, CRP of een SRP op te stellen en moet beschikbaar zijn op het moment van het in productie nemen van het element, de keten of de dienst.
De plannen worden opgeslagen in een SCM tool waardoor ze bij een uitval direct beschikbaar zijn en in de juiste informatie voorzien om de uitval zo snel mogelijk te kunnen herstellen. In het SCM worden de uitvoerende en eindverantwoordelijke voor het proces aangewezen. In de process Manual van SCM is een procesflow opgenomen waarin de (PDCA) cyclus en RACI is weergegeven. Onderhoud aan de recovery plannen is belegd bij de Regelmatig worden oefeningen gepland (BCM kalender). Voor de test wordt een scenario opgesteld. Hierbij wordt gebruik gemaakt van het Runbook (recovery procedure). Indien nodig wordt op basis van de evaluatie van de test het Runbook aangepast.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:
- [redacted]
- [redacted]

C4.2
Normen/criteria
Er zijn procedures en beleid vastgesteld voor de beheersing van incidenten/calamiteiten.

Maatregelen KPN
Het Be Alert proces beschrijft het escalatie proces voor incidenten en calamiteiten. Dit proces beschrijft de specifieke besturing en communicatie voor de incidenten die in verband met de impact niet in het normale storingsproces behandeld kunnen worden. Bij elk incident wordt de werking van Be Alert geëvalueerd.

Bevindingen
Business/Service Continuity Management is een onderdeel van de KSP. Hierin is het beleid vastgelegd. Een belangrijk onderdeel van de continuïteit is het beheersen van incidenten/calamiteiten. Hiervoor is het Be Alert proces ingesteld. Het Be Alert proces beschrijft het escalatieproces voor incidenten en calamiteiten en de werkwijze om zo snel als mogelijk is te komen tot dienst herstel. Bij een incident met een verwachte grote impact start het Be Alert proces. Het Be Alert proces kent de fases aanloop, opstart, beheersen, afronden en nazorg. Het Be Alert proces van classificatie, opschaling en procesbewaking wordt aangestuurd door een vast team van ervaren SQC medewerkers vanuit een calamiteitenteam met duidelijke verantwoordelijkheden en rolverdelingen. Communicatie over de Be Alert status en voortgang intern KPN vindt plaats via
Sinds de introductie van s de informatie veel meer toegankelijk. In kunnen medewerkers van KPN keuzes/selecties maken voor het ontvangen van een alert. Het Be Alert proces treedt in werking vanaf gradatie Geel. De incidenten zijn opgedeeld in classificaties (aantal getroffen gebruikers) aangegeven middels een kleur groen blauw geel oranje h rood . Bij iedere kleur past een escalatiemodel. De incidenten groen en blauw worden opgelost in het reguller proces. Be Alert incidenten vanaf code geel worden geëvalueerd met als doel te leren van incidenten, het vaststellen van acties en problems en het voorkomen van vergelijkbare incidenten.

KPN heeft tijdens de inspectie een live overzicht van Be Alert incidenten uit een omgeving gepresenteerd, maar ook een overzicht van de code oranje incidenten uit 2017 inclusief een voorbeeld van een code oranje incident met gegevens en de evaluatie, inclusief namen van actiehouders en de tijdlijn voor verbeteringen. De in de Be Alert evaluatie benoemde acties en ook het Problem management worden afgehandeld en bewaakt door

Een aantal vaste medewerkers is opgeleid tot binnen het SQC Voorheen werd dit gedaan door in roosterdienst. De laatste wijziging is het benoemen van communicatiemedewerkers in het SQC, gezien het toenemende belang van communicatie in- en extern KPN.

Gemiddeld zijn er per maan blauwe ele en oranje Be Alert incidenten. Over jn e cidenten als oranje Be Alert incidenten geregistreerd. KPN geeft aan dat alleen de oranje (en rode) incidenten die impact hebben op de klanten gemeld worden aan Agentschap Telecom, de interne oranje incidenten niet. Dit houdt in dat het aantal gemelde incidenten beduidend lager liggen dan het totaal aantal oranje incidenten.
Het SQC fungeert als een brandweerorganisatie, daarom is Problem management onderdeel van de ketenbesturing. De gele, oranje en rode incidenten worden geëvalueerd. Acties worden vastgelegd in centraal systeem. Uitvoering en bewaking vinden plaats in de verantwoordelijke keten.

Het SQC stuurt op de snelst mogelijke oplossing van het incident en stuurt niet op SLA afspraken. Dit omdat KPN van mening is dat alle oplossingen zo snel mogelijk afgehandeld moeten worden.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]

C4.3
Normen/criteria
Er zijn preventieve en bedrijfseconomische verantwoorde maatregelen genomen om de impact van regelmatig terugkerende externe calamiteiten te voorkomen
Dit geldt niet voor eventuele overmachtssituaties.

Maatregelen KPN
Een breed scala van normen en maatregelen om externe effecten op de werking van dienstverlening in Technische Objecten te garanderen,

Daarnaast zijn de maatregelen verder uitgewerkt in uitvoeringsrichtlijnen voor aannemers.

Bevindingen
KPN heeft diverse maatregelen in scope om de impact van externe calamiteiten te adresseren. Er moeten fysieke beschermingsmaatregelen worden ontworpen en toegepast tegen schade als gevolg van brand, overstromingen, aardbevingen, explosies, onlusten en andere natuurrampen of door mensen veroorzaakte calamiteiten (KSP-RE210).

Apparatuur moet worden beschermd tegen stroomonderbrekingen en andere storingen veroorzaakt door uitval van nutsvoorzieningen (KSP-RE214).

Elektriciteits- en telecommunicatiekabels die worden gebruikt voor datatransmissie of ondersteunende informatiediensten, moeten worden beschermd tegen aftappen en beschadiging (KSP-RE215).

Daarnaast is er een breed scala van normen en maatregelen om externe effecten op de werking van dienstverlening in Technische Objecten te garanderen zoals fysieke beveiliging, toegangscontrole, monitoring.

Stroomvoorziening/ batterijen
Tijdens de inspectie is alleen het vaste netwerk besproken gezien het werkveld van de aangeschoven vertegenwoordiger vanuit KPN.
Regelmatig worden de voorzieningen getest.

Mobiele NSA voorzieningen en zijn beschikbaar.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]
- [redacted]

Herstelvermogen

C4.4

Normen/criteria

Er zijn procedures opgesteld om na uitval te zorgen voor snel herstel van de dienstverlening.

Maatregelen KPN

Het Be Alert proces beschrijft de werkwijze om zo snel als mogelijk is te komen tot dienst herstel. Daarbij wordt gebruik gemaakt van de ontworpen redundancy maatregelen de continuïteitsplannen (SCP's/BCP's/CRP's/TRP's).

Bevindingen

Incidentafhandeling is een van de taken van het SQC. Hiervoor wordt het Be Alert proces gebruikt. Het proces is gericht op snelle detectie en snelle communicatie. Triggers voor het Be Alert proces zijn signalen vanuit klanten/social media, netwerk- en dienstmonitoring.
Uitgangspunt is dat de dienst weer zo snel mogelijk beschikbaar is. Daarbij maakt de soort dienst geen onderdeel van de afweging. In uitzonderlijke gevallen wordt er een prioritering opgesteld.
Dan gaat eerst voor daarna kritieke diensten etc. Bijvoorbeeld het verkeer over een De oorsprong van het verkeer dat daadwerkelijk over een wordt verwerkt is niet bekend. Bij een verstoring wordt dit beeld opgebouwd uit de klachten van gebruikers en vanuit de techniek.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]

C4.5

Normen/criteria

Er staat een crisisorganisatie paraat.

Maatregelen KPN

Het Be Alert proces team in het SQC is elke week voor alle rollen ingeroosterd, evenals het CCMT welke maand.

Bevindingen

Bij een crisis treedt Be Alert code Rood in werking. Dit is een uitzonderlijke situatie zoals een ernstige sociale, economische of maatschappelijke verstoring.
heeft de leiding
KPN beschikt over met een vaste bezetting die vormen en die op elkaar zijn ingewerkt) in een maandelijks rooster oproepbaar zijn.
Ook zijn er nu sinds drie jaar aste teams met samengesteld voor Be Alert code rood die kunnen handelen namens de RvB van KPN. Deze teams zijn opgeleid en voeren jaarlijks een table top oefeningen uit en een enkele keer in actie geweest. Daarnaast hebben zij als schaduw gedraaid bij enkele oranje storingen. Voor hel s een beschikbaar in iet uitwi

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]

C4.6
Normen/criteria
Er zijn procedures opgesteld voor de crisiscommunicatie, bijvoorbeeld als het gaat om contact met verantwoordelijke overheden en crisispartners.

Maatregelen KPN
In Be Alert proces en lijn de procedures en verantwoordelijkheden beschreven voor het melden van incidenten aan Agentschap Telecom en doormelding aan EZ DCC, en het informeren en zo nodig afvaardigen van liaisons naar de Veiligheidsregio's. Ook de ingangen bij KPN voor de verantwoordelijke overheidspartijen zijn bij hen bekend gemaakt.

Bevindingen
In Be Alert proces en lijn de procedures en verantwoordelijkheden beschreven voor het melden van incidenten aan Agentschap Telecom en doormelding aan EZ DCC, en het informeren en zo nodig afvaardigen van Liaisons naar de Veiligheidsregio's. Ook de ingangen bij KPN voor de verantwoordelijke overheidspartijen zijn bij hen bekend gemaakt.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]

3.5 Beheersdoelstelling B5: Oefening en monitoren

De organisatie oefent en monitort de continuïteit van de dienstverlening.

Continuïteit monitoren

C5.1
Normen/criteria
Er is een systeem om de continuïteit te monitoren.

Maatregelen KPN
Het SQC van KPN beschikt over dienstbewakingstooling om degradatie en uitval te signaleren en te analyseren. Triggers vanuit onder meer contactcenters, webcare, social media, aantallen storingstickets, aansturing monteurs en klantescalaties kunnen ook aanleiding zijn tot onderzoek.
MSP's beschikken over tooling om vanuit technisch perspectief [redacted] te monitoren en kunnen aldus ook storingen signaleren en analyseren. In alle gevallen kan dit bij grote impact leiden tot het opstarten van het Be Alert proces.

Bevindingen
Monitoring continuïteit dienstverlening
KPN beschikt over vastgesteld continuïteitsbeleid, de KSP zoals beschreven in B1, waarin de continuïteit van de dienstverlening is beschreven en vastgesteld. Volgens de KSP moeten storingen of performance degradatie in systemen, netwerken en diensten vroegtijdig, near realtime, worden gedetecteerd.

De continuïteit van de dienstverlening wordt centraal vanuit het SQC in [redacted] gemonitord met behulp van dienstbewakingstools. Ook informatie en incidenten vanuit onder meer contactcenters, social media, webcare en van monteurs kunnen aanleiding zijn tot het starten van een onderzoek. Binnen het SQC zijn naast de dienstbewaking ook de kernfuncties Be Alert, change control en het [redacted] geplaatst.

Als voorbeeld heeft KPN het dashboard van 112 getoond, waarbij wordt aangegeven dat er 24/7 een [redacted] in het vaste net actief is om de verbindingen naar de meldkamers te testen.

KPN geeft tijdens de inspectie aan dat in het SQC meer dan [redacted] van alle diensten worden bewaakt. Het restant betreft de zakelijke diensten van voorheen [redacted] welke elders worden bewaakt. MSP's beschikken over tooling om de fysieke componenten in de netwerken zoals netwerkelementen en bekabeling te monitoren, incidenten te signaleren, te analyseren en af te handelen. Deze bewakingscentra bevinden zich [redacted]

Naast de feitelijke wekelijkse en maandelijkse managementrapportage wordt er elk kwartaal de BCM status over de continue levering van de geaccordeerde kritieke diensten en kritieke halffabricaten gerapporteerd worden door de diensteigenaar/productmanager aan het CISO. Alle rapportage eenheden moeten hetzelfde Business Continuity Framework hanteren, zoals beschreven in B1.

Als voorbeeld voor diensten is het 112 dashboard besproken. [redacted] elt 112 met een mobiel toestel. KPN gebruikt voor bewaking van vaste 112 verbindingen een [redacted] daarnaast worden deze lijnen 24/7 getest. Voor landelijke meldkamer in

Driebergen zijn e[illegible]ijnen beschikbaar verdeeld over[illegible] voor elke meldkamer zijn er[illegible] ij langdurige incidenten ligt de hoogste prioriteit bij 112. De prioriteiten zijn[illegible] De 112 gesprekken zijn onderdeel van de voice dienst.
In de eerste helft van[illegible] al een nieuwe 112 omgeving in opdracht van de Nationale Politie in gebruik genomen (planning[illegible]. Deze 112 dienst is als een IP dienst redundant ondergebracht in twee datacenters op de hoge netwerk[illegible] bcaties. Beide zijn continue actief en kunnen de dienst volledig overnemen. Als last resort kan ook de ontwikkel en test omgeving in[illegible] geschikt gemaakt worden om de 112 dienst over te nemen. De nieuwe dienst heeft een gescheiden (logisch) netwerk met eigen core routers. In de nieuwe dienst worden alle gesprekken, ook EPOTS gesprekken, als VoIP aangeboden aan de landelijke 112 meldkamer bij het MDC. Het bijbehorende nieuwe dashboard is in ontwikkeling.
Het NCV wordt apart gemonitord in het SQC.

Dashboards worden getoond op de grote schermen in het SQC, als ook op de werkplekken van de medewerkers. De getoonde dashboards zijn in principe identiek. Medewerkers waren in het verleden gespecialiseerd en per dienst georganiseerd. Nu is iedereen generiek inzetbaar (met nog een milde vorm van specialisatie). Het proces van signaleren en analyseren kan leiden tot opstarten van het Be Alert proces zoals beschreven in B4. Dit proces bestaat uit de fases aanloop, opstart, beheersen, afronden en nazorg.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Contingency plan

C5.2
Normen/criteria
Er wordt periodiek geoefend met contingencies / contingency plan en daar wordt van geleerd.

Maatregelen KPN
KSP schrijft voor dat continuïteitsplannen jaarlijks worden geoefend en geüpdatet.

Bevindingen
Continuïteitsplannen
De KPN Security Policy (KSP) schrijft voor dat alle systemen en applicaties zowel bij de initiële levering ('robuustheidstesten') als daarna bij de continue levering jaarlijks tegen de continuïteitseisen worden getest om te zorgen dat ze de vereiste capaciteit en performance kunnen invullen. Voor gebouw gebonden voorzieningen moet de

redundantie, de stand-by techniek en processen, bij aanvang en daarna jaarlijks getest worden.

Alle continuïteitsplannen (SCP's/BCP's/CRP's/TRP's) en alle technische maatregelen die zijn genomen om continuïteitsrisco's te beperken moeten minimaal jaarlijks, maar ook bij aanzienlijke wijzigingen van de dienst, halffabricaat of het gebouw worden geoefend.

Oefeningen en rapportages
Oefeningen moeten worden geëvalueerd en worden vastgelegd in een rapport. Aanbevelingen en verbeteringen moeten worden doorgevoerd binnen de overeengekomen tijdslijnen.

Iedere rapportage eenheid stelt jaarlijks een BCM-planning op over de invulling van het BCM-proces. Jaarlijks wordt de classificatie voor KPN Telecom gebouwen en datacenters herijkt aan de hand van de BCM Impact Analyse. Als de classificatie kritiek of hoog is zal er aansluitend een risico assessment uitgevoerd worden met de BCM RiskTool. De resultaten hiervan worden aar[redacted]erapporteerd. [redacted] onderhoudt het overzicht van afgestemde kritieke gebouwen en biedt het jaarlijks ter goedkeuring aan het topmanagement aan. Voor ieder kritiek gebouw moet een continuïteitsplan beschikbaar zijn dat jaarlijks wordt getest/geoefend.

Ook MSP's zijn contractueel (KSP's) verplicht om jaarlijks te oefenen. Evaluaties en verbeterplannen worden uitgevoerd door de MSP en bewaakt / afgestemd met de verantwoordelijke demand manager.

KPN geeft tijdens de inspectie aan dat NSA's maandelijks worden getest, zowel voor de antenne-opstelpunten in het mobiele netwerk als in de technische gebouwen in het vaste netwerk. Voor de Hoge Netwerk[redacted]caties zijn per locatie plannen opgesteld. Dit geldt deels ook voor de[redacted]t andere deel heeft een generiek plan, wat tevens geldt voor de[redacted]caties evenals voor de[redacted]ocaties.

KPN platformbeheer werkt met een online [redacted]waarin zoals KPN tijdens de inspectie heeft laten zien, op basis van RACI de rollen en verantwoordelijk zijn vastgelegd. In dit[redacted]staan verder onder meer het Technical Recovery Plan (TRP), het type test (live, table top of een runbook), de BCM kalender, het ticket nummer en de evaluatie. KPN geeft aan dat ook een ongepland Be Alert incident gebruikt wordt om aan te tonen dat de redundantie en de procedures correct werken. Een goed resultaat tijdens een klein of groot Be Alert incident toont de echte waarde van de robuustheid van het platformontwerp en heeft dus meerwaarde ten opzichte van een procedurele live test.

Bij changes en projecten (initiële levering) moet aantoonbaar worden gemaakt dat alle redundantie, procedures en runbooks werken door te testen en te oefenen.

[redacted]eeft tijdens de inspectie aan dat kwetsbaarheden in de software worden bewaakt met een [redacted]

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

- [redacted]

Rapportage en overleg

C5.3
Criteria/normen
Periodiek wordt in overleg getreden (of gerapporteerd) met (richting) de toezichthouder over de continuïteit van de dienstverlening.

Maatregelen KPN
Naast de jaarlijkse rapportage aan AT, het 'Toezichtsgesprek' en het meldloket overleg worden ook op aanvraag details storingsgegevens verstrekt bij bijvoorbeeld stroomstoring of een incident tijdens een evenement.

Bevindingen
KPN rapporteert jaarlijks de ingevulde H.14 vragenlijst aan het Agentschap Telecom. Tevens vindt er jaarlijks een 'Toezichtsgesprek" plaats en worden grote incidenten (Be Alert vanaf code oranje) gemeld aan het meldloket. Verder worden op aanvraag details storingsgegevens verstrekt bij een groot of bijzonder incident zoals bijvoorbeeld een stroomstoring of een incident tijdens een evenement.

Beschrijving aangeleverde of ter inzage beschikbaar gestelde specifieke documenten:

- [redacted]

4 Conclusies en aanbevelingen

4.1 Conclusies

Op basis van de bevindingen uit hoofdstuk 3 zijn voor de vijf beheersdoelstellingen de volgende conclusies getrokken.

B1: Beleid, Governance en risicomanagement
KPN beschikt over continuïteitsbeleid, een adequate governance van de continuïteit en hanteert een risicomanagement-framework.

Het continuïteitsbeleid is opgenomen in het KSP waarin aandacht is besteed aan de doelstelling, kritische netwerken en diensten en ondersteunende kritieke onderdelen en systemen. De focus ligt primair op de vitale en kritieke diensten/halffabrikaten en nieuwe diensten. Er wordt gerapporteerd door middel van maandelijkse management letters en kwartaalrapportages. KPN heeft een tool, ontwikkeld dat inzicht moet gaan bieden in de onderlinge afhankelijkheden van alle diensten en continuïteitsplannen.
KPN heeft sleutelfunctionarissen benoemd vaarbij taken, verantwoordelijkheden en bevoegdheden conform het RACI model zijn ingevuld voor de uitvoering van het continuïteitsbeleid. Daarnaast is de organisatie zodanig ingericht nnen de afzonderlijke bedrijfsonderdelen), dat het continuïteitsbeleid voortdurend onder de aandacht wordt gebracht bij de medewerkers.
KPN herijkt op basis van een PDCA cyclus, evaluaties van (grotere) incidenten en incidenten als gevolg van changes in principe vier keer (één grote en drie kleinere) paar jaar het vastgestelde continuïteitsbeleid.

Als invulling voor risicomanagement beschikt KPN over een risicomanagement methodologie bestaande uit een scoring op de dreigingenlijst en het opstellen van een risktreatmentplan. Onderdeel van een risicoassessment vormt een lijst van de belangrijkste continuïteitsrisico's in de vorm van een algemene dreigingenlijst. De RisicoTool vormt hierbij de administratieve borging. Ook voor risicomanagement herijkt KPN op basis van een PDCA cyclus, evaluaties van (grotere) incidenten en incidenten als gevolg van changes risico assessments.

Voor de borging van rollen en verantwoordelijkheden heeft KPN voor haar medewerkers deze toebedeeld met behulp van RACI schema's. KPN herijkt de rollen en verantwoordelijkheden op basis van evaluaties en changelogs als gevolg van wijzigingen en/of incidenten.

B2: Asset management
KPN heeft invulling gegeven aan asset management ten aanzien van voor de continuïteit kritieke onderdelen en systemen. Grootzakelijke klanten en MKB worden over het algemeen goed geïnformeerd over beschikbaarheid van de afgenomen dienst, consumenten daarentegen niet.

Voor het beheer zijn de rollen en verantwoordelijkheden vastgelegd. Jaarlijks wordt een BIA en IA uitgevoerd en vastgelegd.
Er is beleid vastgesteld met betrekking tot continuïteitseisen bij derden. De relevante onderdelen van het KSP worden binnen de overeenkomst van toepassing verklaard. Hierop kan worden gecontroleerd door KPN of middels door derden geïnitieerde assessments.
Grootzakelijke klanten definiëren in de regel zelf de dienst waarbij continuïteit een onderdeel is en zijn bekend met de beschikbaarheid. Dit geldt ook voor het MKB

waarbij de sales managers zijn geïnstrueerd het onderwerp continuïteit als verplicht onderdeel te bespreken. Daarbij wordt gewezen op de beschikbaarheid en de eventuele impact. Voor consumenten is dit niet het geval.

Bereikbaarheid 112
Met betrekking tot de door KPN geleverde vitale diensten 112 en NCV wordt geconstateerd dat bij het jaarlijks uitvoeren van de BIA en IA herhaaldelijk niet naar voren is gekomen dat deze niet de hoogste [redacted] nieten dan wel dat dit risico is [redacted]. Er is [redacted] de mobiele en vaste 112 diensten.

B3: Operationele procedures
KPN heeft operationele procedures voor het werken met voor de continuïteit kritieke onderdelen en systemen.

KPN beschikt over lifecycle beheer. Procedures en normtijden zijn vastgesteld en hiermee werken zowel interne als externe beheer- en installatiepartijen mee in geval van incidenten. Zowel bij Problem management als Be Alert worden incidenten geregistreerd, geclassificeerd, geëscaleerd en geanalyseerd. Daarnaast is Problem management het proces dat zich bezighoudt met incidenten die uiteindelijk deel maken van de reguliere operatie. Binnen Be Alert en tijdens de reguliere (incidenten) operatie worden incidenten en wijzigingen geëvalueerd en afgehandeld.
Door middel van onder andere [redacted] kan KPN haar IT/TI diensten en netwerk elementen monitoren en evalueren.

KPN beschikt over change management. Er is beleid en een vertaling hiervan in een proces. Dit proces en de CAB borgen de beoordeling van changes volgens de klantafspraken en het minimaliseren van de continuïteitsrisico's voor kritieke en vitale diensten. Changes worden op een gecontroleerde manier vastgelegd, gecategoriseerd en geëvalueerd, geautoriseerd, geprioriteerd, gepland, getest, geïmplementeerd, gedocumenteerd en beoordeeld.

B4: Voorbereiding contingencies en herstel
KPN is voorbereid op contingencies en het snel herstellen van de dienstverlening na uitval.

KPN heeft de beschikking over diverse specifieke contingency plannen. Deze plannen moeten beschikbaar zijn bij het in productie nemen van een element, keten of dienst en zijn opgeslagen in een SCM tool. Hierin zijn de rollen en verantwoordelijkheden vastgelegd en het proces (PDCA). Regelmatig wordt geoefend.
Het beleid de doelen en het proces met betrekking tot het beheersen van incidenten/calamiteiten is binnen KPN vormgegeven. Be Alert is ingesteld om het proces te kunnen beheersen.
KPN heeft diverse preventieve maatregelen genomen om de impact van regelmatig terugkerende calamiteiten te mitigeren. Met betrekking tot de stroomvoorziening zijn extra voorzieningen getroffen in de vorm van accu's en NSA's.

KPN beschikt over een procedure om bij uitval te zorgen voor een snel herstel van de dienstverlening. Dit maakt onderdeel uit van Be Alert.

KPN heeft een crisisorganisatie. Deze treedt in werking bij een Be Alert code Rood. [redacted] Er zijn procedures voor crisiscommunicatie voor contacten met verantwoordelijke overheden en crisispartners.

B5: Oefening en monitoren
KPN oefent en monitort de continuïteit van de dienstverlening.

Er is een systeem om de continuïteit te monitoren. KPN beschikt over een systeem om de continuïteit te monitoren waar storingen of performance degradatie in systemen, netwerken en diensten vroegtijdig worden gedetecteerd. Daarnaast beschikt KPN over een "Be Alert" organisatie voor het beheersen van calamiteiten.

Er wordt periodiek geoefend met contingencies/ contingency plannen en daar wordt van geleerd. KPN test de systemen en applicaties zowel bij de initiële levering als bij de continue levering. Ook gebouw gebonden voorzieningen worden bij aanvang en vervolgens jaarlijks getest. KPN oefent periodiek, deze oefeningen worden geëvalueerd en vastgelegd. Aanbevelingen en verbeteringen worden doorgevoerd. Deze afspraken gelden ook voor derde partijen.

Periodiek wordt in overleg getreden (of gerapporteerd) met (richting) de toezichthouder over de continuïteit van de dienstverlening.
Er vindt jaarlijks een 'toezichtsgesprek" plaats met Agentschap Telecom en KPN rapporteert jaarlijks de H14 vragenlijst en grote incidenten (Be Alert vanaf code oranje). Verder verstrekt KPN op aanvraag details van storingsgegevens bij een groot of bijzonder incident of tijdens een evenement.

Algemene conclusie
Op basis van de interviews, de inzage in documenten (opzet) en dashboards (doorkijkje naar bestaan) wordt geconcludeerd dat KPN sinds het vorige inspectieonderzoek belangrijke stappen heeft gezet ten aanzien van de invulling van de zorgplicht continuïteit. Maatregelen zijn getroffen om het vastgestelde continuïteitsbeleid binnen n de afzonderlijke bedrijfsonderdelen binnen de organisatie verder te borgen en ten uitvoer te brengen. KPN blijft verdere stappen ondernemen om de continuïteit verder te verbeteren. Hierbinnen wordt ook invulling gegeven aan de PDCA-cyclus voor continuïteit.
Opgemerkt wordt dat security, vergeleken met het vorige inspectieonderzoek, een belangrijkere positie heeft verworven ten opzichte van continuïteit. KPN ziet continuïteit als onderdeel van security.

4.2 Aanbevelingen

Voor drie beheersdoelstellingen zijn de volgende aanbevelingen geformuleerd.

B1: Beleid, Governance en risicomanagement

- Betrek ook de diensten niet zijnde vitaal en kritiek in voldoende mate bij het continuïteitsbeleid.

B2: Asset management

- Verifieer het risicomanagement proces in hoeverre de jaarlijkse uitvoering het beoogde doel bereikt.
- Verifieer in hoeverre de locatie van de[redacted] voldoet aan de eisen uit het KSP.
- Informeer consumenten over de beschikbaarheid van de aangeboden diensten.

B4: Voorbereiding contingencies en herstel

- Draag er zorg voor dat KPN als vitale partner onderdeel gaat uitmaken van de huidige informatievoorziening tussen de huidige crisispartners (met name de netbeheerders in het bijzonder) gedurende calamiteiten en crisis.

5 Bijlage lijst geïnterviewden KPN

6 Bijlage afkortingen

BCM	Business Continuity Management
BIA	Business Impact Analysis
CAB	Change Advisory Board
COO	Chief Operational Officer
CRP	Chain Recovery Plan
DoR	Document of Representation
FTR	First time right
GCC	General Computer Control,
IA	Impact Assessment
IT	Information Technology
KPI	Kritische Prestatie Indicator
KSP	KPN Security Policy
MSP	Managed Service Providers
NCV	Noodcommunicatievoorziening
NOC	Network Operations Center
NSA	Noodstroomaggregaat
PHOSI	Potential Harm Of Security Incident
RACI	Responsible, Accountable, Consulted en Informed
SCM	Services of Continuity Management
SPOF	Single Point of Failure
SQC	Service Quality Center
SRP	Service Repair Plan
TI	Technische Infrastructuur
TRP	Technical Recovery Plan