De calamiteitenplannen worden regelmatig betrokken in bewustwordings-, trainings- en testactiviteiten.

Implementatierichtlijnen (Code 14.1.1.i, 14.1.3, 14.1.4) (BS 9.2, 9.3)
1. De calamiteitenplannen worden volgens een testschema getest en personeel wordt op basis daarvan getraind. In het testschema is beschreven hoe en wanneer deze activiteiten plaatsvinden. In het testprogramma worden de technische, logistieke, administratieve, procedurele en andere operationele en ondersteunende systemen van het plan betrokken. Tot het testschema behoort ook het periodiek houden van ontruimingsoefeningen.
2. Er wordt - op operationeel niveau - toegezien op het uitvoeren van het testen van calamiteitenplannen. Er kunnen verschillende technieken worden gebruikt om er zeker van te zijn dat de plannen daadwerkelijk functioneren. Dit omvat bijvoorbeeld: (Code 14.1.5)
a. gezamenlijk doorlopen van diverse scenario's (bespreking van de bedrijfsherstelprocedures aan de hand van voorbeelden van onderbrekingen);
b. simulaties (in het bijzonder om mensen te trainen in hun rol na een incident en bij crisisbeheer);
c. testen van technische herstelprocedures (om te waarborgen dat bedrijfsactiviteiten en informatiesystemen doeltreffend kunnen worden hersteld);
d. testen van herstel op een andere locatie (waarbij bedrijfsprocessen parallel aan hersteloperaties worden uitgevoerd, op een andere plaats dan de hoofdlocatie);
e. testen van voorzieningen en diensten van leveranciers (om te waarborgen dat externe diensten en producten in overeenstemming zijn met contractuele verplichtingen);
f. realistische oefeningen (waarbij wordt getoetst dat organisatie, personeel, apparatuur, voorzieningen en processen bestand zijn tegen onderbrekingen);
g. beschikbaarheidstesten van de leden van een crisisteam.
3. Het ontwerp van de uitwijktest borgt dat er geen oneigenlijke mutaties in productiegegevens aangebracht kunnen worden.
4. Testdata worden na afloop van het testen van de gebruikte computersystemen verwijderd.
5. Bij het testen van mutatiefuncties wordt altijd uitgegaan van kopieën van productiedata.
6. Van het trainen en testen wordt een onafhankelijk verslag gemaakt, dat gebruikt wordt voor evaluatie en het verbeteren van de plannen.
7. Er wordt regelmatig een bewustwordingsprogramma uitgevoerd. (BS 10.2)
8. Bedrijfscontinuïteitsspecialisten worden regelmatig getraind op de verschillende onderdelen van hun vakgebied. (BS 10.3)
9. Op basis van de evaluatie, maar ook op basis van wijzigingen in organisatie, personeel en middelen worden de plannen onderhouden. (BS 9.4)
10. Het management evalueert periodiek de plannen als self-assessment of door middel van een audit. (BS 9.5.1, 9.5.2, 9.5.3, 9.5.4)

C.9.2.7. Onderhouden beveiligingskaders

Beheersmaatregel
De beveiligingskaders worden bijgesteld op basis van controles, testen en evaluaties.

Implementatierichtlijnen
1. Beveiligingskaders worden onderhouden op basis van
a. de uitkomsten van 9.2.5 Evalueren beveiliging; (Code 14.1.5)
b. wijzigingen in organisatie, techniek en processen;
c. periodieke beoordeling van het beveiligingsbeleid;
d. het actuele dreigingsprofiel

C.9.3. Centraal beheer elektronische identiteiten

Beheersmaatregel
Elektronische identiteiten worden centraal in de organisatie beheerd.

Implementatierichtlijnen
1. Gebruikers en IT-voorzieningen krijgen op organisatieniveau een unieke elektronische identiteit toegekend, zodat zij verantwoordelijk kunnen worden gesteld voor hun handelingen in geautomatiseerde systemen. (Code 11.2.1.a)
2. Aanvragen voor externe elektronische identiteiten namens de organisatie zijn goedgekeurd door het daarvoor bevoegde management.

3. Er is een formele registratie van alle elektronische identiteiten die geregistreerd zijn als gebruiker of IT-voorziening binnen de organisatie en extern namens de organisatie. (Code 11.2.1.g)
4. Er zijn waarborgen dat overtollige gebruiker-id's niet aan andere gebruikers worden uitgegeven (Code 11.2.1.j)
5. De elektronische identiteiten van medewerkers worden afgestemd met de personeelsregistratie.
6. Elektronische identiteiten, die niet vast zijn toegewezen aan personen en bedoeld zijn voor tijdelijk gebruik, kennen een apart beheerregiem waarin geregeld is dat
a. de tijdelijke toewijzing aan een persoon met identificerende gegevens wordt geregistreerd;
b. periodieke onafhankelijke controle plaatsvindt op het gebruik van deze identiteiten.
7. De identificerende gegevens van vertrouwde derden worden periodiek gecontroleerd door bevoegde vertegenwoordigers van de desbetreffende organisaties.
8. De identificerende gegevens van IT-voorzieningen worden periodiek gecontroleerd door functioneel bedrijfsmiddelenbeheerders.
9. De identificerende gegevens van externe elektronische identiteiten namens de organisatie worden periodiek gecontroleerd door het hogere lijnmanagement.

C.9.4. Verstrekken authenticatiemiddelen

Beheersmaatregel
Authenticatiemiddelen worden aan gebruikers verstrekt onder gecontroleerde condities.

Toelichting
Onder authenticatiemiddelen worden wachtwoorden, tokens, smart cards (bijv. voor fysieke toegang), digitale sleutels en certificaten verstaan. Een aparte categorie authenticatiemiddelen vormen de legitimatiebewijzen, die aan personeel wordt uitgegeven om zich extern voor hun functie te kunnen verantwoorden.

Implementatierichtlijnen
1. Fysieke authenticatiemiddelen worden verstrekt na controle van de identiteit d.m.v. deugdelijke identificatiemiddelen en tegen kwijting.
2. Bij het verstrekken van wachtwoorden wegens een eerste opvoer, het opheffen van geblokkeerde identiteiten of het vergeten zijn van het wachtwoord bestaat voldoende zekerheid omtrent de identiteit. (Code 11.2.3.c)
3. Tijdelijke wachtwoorden behoren uniek te zijn voor een persoon en mogen niet te raden zijn. (Code 11.2.3.e)
4. Tijdelijke wachtwoorden worden op een veilige manier uitgegeven aan gebruikers; gebruik via derden of gebruik van onbeschermde e-mailberichten (ongecodeerde tekst) wordt vermeden. (Code 11.2.3.d)
5. De authenticatiemiddelen van onpersoonlijke identiteiten (bijv. systeemaccounts) met speciale bevoegdheden worden via een procedure waarin de exclusiviteit geborgd is ter beschikking gesteld. Hierbij gelden de volgende uitgangspunten:
a. na initieel inloggen wordt het wachtwoord of pincode op een onafhankelijke manier gewijzigd en opnieuw vastgelegd zodat daar geen kennis van bestaat, of van kan worden genomen, zonder het opnieuw doorlopen van de procedure voor beschikbaarstelling (bijvoorbeeld middels een verzegelde enveloppe);
b. het authenticatiemiddel wordt beschermd bewaard zodat de exclusiviteit geborgd is (bijvoorbeeld in een kluis). De procedure voor uitgifte en de vindplaats zijn bekend bij medewerkers van de processen, die incidenten moeten afhandelen;
c. het ophalen en gebruiken van het authenticatiemiddel is herleidbaar naar de noodzaak daartoe (een incident, een change, etc.), en wordt na gebruik weer exclusief gemaakt (zie a) en bewaard (zie b). Er vind gericht toezicht en controle plaats op het gebruik van speciale bevoegdheden;
d. Periodiek wordt gecontroleerd of de exclusiviteit tijdens het bewaren doorlopend geborgd wordt (bijvoorbeeld of de enveloppe nog verzegeld is.

C.9.5. Aanvragen autorisaties

Beheersmaatregel
Autorisatie-aanvragen worden bij voorkeur centraal in een organisatie ontvangen en al dan niet geautomatiseerd ter afhandeling door gegeven aan de (technische beheerders van de) doelsystemen.

Implementatierichtlijnen
1. Aanvragen voor autorisaties worden alleen gedaan door bevoegde lijnmanagers.

2. Periodiek wordt vastgesteld of door lijnmanagers aangevraagde autorisaties overeenstemmen met de in de doelsystemen daadwerkelijk voor de gebruikers vastgelegde toegangsrechten (Soll-Ist vergelijking).

C.9.6. Beheren groepering autorisaties

Beheersmaatregel
Autorisaties worden zo centraal mogelijk in een organisatie(deel) gegroepeerd op basis van het beleid voor toegangsbeveiliging en de eisen van functiescheiding.

Implementatierichtlijnen
1. Toegangsrechten worden uitsluitend verleend via autorisatiegroepen.
2. Autorisatiegroepen worden samengesteld op basis van 2.3 Beleid voor functiescheiding en 2.5 Toegangsbeleid. (Code 11.2.1.c)
3. De onverenigbaarheid van autorisatiegroepen worden zoveel mogelijk ingebracht in het tool voor autorisatiebeheer, teneinde ze automatisch te laten signaleren.
4. Autorisatiegroepen worden op functioneel niveau gedocumenteerd.
5. Autorisatiegroepen en rules zijn goedgekeurd door het Informatie- of lijnmanagement, afhankelijk van het type. (Code 11.2.1.b)

C.9.7. Beheren decentrale autorisaties gebruikers

Beheersmaatregel
Autorisaties worden aan gebruikers toegekend op basis van het beleid voor toegangsbeveiliging en de eisen van functiescheiding.

Implementatierichtlijnen
1. Toegangsrechten worden voor gebruikers aangevraagd op basis van:
a. 2.3 Beleid voor functiescheiding;
b. 2.5 Toegangsbeleid; (Code 11.2.2.b)
c. de functiescheidingen per proces en organisatie;
d. de goedgekeurde autorisatiegroepen en rules volgens norm 9.6.5.
2. Toegekende autorisaties die als onverenigbaar zijn gesignaleerd, worden op basis van advies door tactisch beveiligingsbeheer door het management goedgekeurd.
3. Voor gebruikers, die binnen dezelfde organisatie van het ene naar het andere dienstverband gaan worden de toegangsrechten opnieuw aangevraagd. (Code 11.2.4.b)
4. Er is vastgesteld wanneer sprake is van speciale accounts en speciale bevoegdheden alsmede van autorisaties die alleen per gebeurtenis worden toegekend.
5. De speciale bevoegdheden behorend bij elke IT-voorziening en de (soort) gebruikers aan wie deze bevoegdheden kunnen worden toegewezen, wordt op basis van advies door tactisch beveiligingsbeheer door het management goedgekeurd. (Code 11.2.2.a)
6. Wijzigingen van speciale accounts worden geregistreerd en periodiek onafhankelijk beoordeeld. (Code 11.2.4.e)
7. Bij aanvragen van onverenigbare of niet primair bij de functie behorende autorisatiegroepen worden aanvullende maatregelen getroffen om misbruik te voorkomen, zoals logging, vier-ogenprincipe of aanvullende interne controle. Van aanvullende maatregelen wordt een overzicht bijgehouden.
8. Rechten voor het gebruik van systeemhulpmiddelen worden:
a. zo beperkt mogelijk toegekend; (Code 11.5.4.c)
b. of slechts op ad hoc-basis toegekend; (Code 11.5.4.d)
c. of slechts voor de duur van een geautoriseerde wijziging (Code 11.5.4.e)
d. en worden niet beschikbaar gesteld aan gebruikers, die toegang hebben tot toepassingen op systemen waar scheiding van taken is vereist. (Code 11.5.4.i)
9. Periodiek wordt door lijnmanagers op basis van een overzicht uit de toegangsrechtenadministratie gecontroleerd en bevestigd dat de toegangsrechten van gebruikers juist zijn en zo niet welke overtollige identiteiten en toegangsrechten moeten worden gewijzigd. (Code 6.2.1.f, 11.2.1.i, 11.2.4.a)
10. Autorisaties voor speciale toegangsrechten worden met een hoge regelmaat beoordeeld; bijvoorbeeld elke 3 maanden (Code 11.2.4.c, 11.2.4.d, 11.2.4.e).
11. Periodiek wordt vastgesteld of de aan gebruikers toegekende autorisaties overeenstemmen met de in de doelsystemen daadwerkelijk voor de gebruikers vastgelegde toegangsrechten (Soll-Ist vergelijking). Voor zover de autorisatieverlening via een centraal beheertool verloopt, zal dit als geautomatiseerd proces kunnen plaatsvinden.

C.9.8. Controleren van systeemgebruik

Beheersmaatregel
Er zijn procedures vastgesteld om het gebruik van IT-voorzieningen te controleren. Het resultaat van de controleactiviteiten wordt regelmatig beoordeeld.

Implementatierichtlijnen (Code 10.10.2)
1. Het vereiste controleniveau voor afzonderlijke voorzieningen wordt bepaald aan de hand van een risicobeoordeling. Aspecten waar rekening mee wordt gehouden omvatten:
a. geautoriseerde toegang, waaronder details als:
  1. de gebruikers-id;
  2. de datum en tijd van belangrijke gebeurtenissen;
  3. het type gebeurtenis;
  4. de bestanden waartoe toegang is verkregen;
  5. de gebruikte (hulp)programma's;
b. alle handelingen met speciale bevoegdheden, zoals:
  1. gebruik van accounts met speciale bevoegdheden, bijvoorbeeld supervisor, root operator, beheerder;
  2. opstarten en afsluiten van het systeem;
  3. aan-/afsluiten van apparatuur voor in- en uitvoer van gegevens;
c. pogingen tot ongeautoriseerde toegang, zoals:
  1. mislukte of geweigerde gebruikersacties;
  2. mislukte of geweigerde handelingen met betrekking tot gegevens of andere hulpmiddelen;
  3. overtredingen van 2.5 Toegangsbeleid en meldingen aan netwerkgateways en firewalls;
  4. alarmeringen van eigen systemen voor het opsporen van inbraak;
d. systeemwaarschuwingen of -fouten, zoals:
  1. consolewaarschuwingen of -berichten;
  2. uitzonderingen in het logbestand;
  3. waarschuwingen van het netwerkbeheer;
  4. alarmeringen door het toegangsbewakingssysteem;
e. veranderingen van of pogingen tot verandering van de systeembeveiligingsinstellingen en -beheersmaatregelen.
2. Hoe vaak de resultaten van de controleactiviteiten worden beoordeeld hangt af van de volgende risicofactoren:
a) hoe kritisch de toepassingsprocessen zijn;
b) waarde, gevoeligheid of onmisbaarheid van de desbetreffende informatie;
c) ervaringen uit het verleden met systeeminfiltratie en -misbruik en hoe vaak de kwetsbare plekken zijn aangevallen;
d) mate waarin het systeem is gekoppeld met andere systemen (in het bijzonder openbare netwerken);
e) deactiveren van de logfaciliteiten.

C.9.9. Technisch beveiligingsbeheer

Doelstelling
De toegang tot voorzieningen wordt beheerd in overeenstemming met de autorisatieaanvragen en de overige beveiligingsinstellingen worden gehandhaafd in overeenstemming met de technische beveiligingsdocumentatie.

Afbakening
Tot de hier bedoelde voorzieningen worden IT-voorzieningen en voorzieningen van fysieke aard, zoals gebouwen, ruimten, kluizen, kasten e.d. gerekend.

C.9.9.1. Beheer toegangsregels

Beheersmaatregel
Toegang tot IT-diensten en -middelen wordt om reden van doelmatig beheer geregeld door middel van groepsautorisaties.

Implementatierichtlijnen
1. Autorisatiegroepen worden vastgesteld in overeenstemming met het beveiligingsbeleid en de ontwerpdocumentatie van de desbetreffende voorziening.

2. Er wordt een actuele documentatie bijgehouden, waarin per autorisatiegroep een omschrijving is gegeven van de aard van de erin opgenomen autorisaties.
3. Autorisatiegroepen voldoen aan een naamgevingsconventie, die recht doet aan de uniciteit van groepen op organisatieniveau.
4. Van gebruikte coderingen zijn verklarende beschrijvingen beschikbaar.
5. Indien (voorziene) wijzigingen in groepsautorisaties niet binnen de bestaande groepsstructuur kunnen plaatsvinden, wordt dit tijdig gerapporteerd aan de functioneel beheerder van de desbetreffende voorziening.
6. Er worden geen rechtstreekse autorisaties verleend buiten de formele aanvraagprocedures om. (Code 11.2.1.f)
7. De toegangsrechten worden periodiek ter beschikking gesteld voor controle van de juistheid van de autorisatieverlening. (Code 9.1.2.e)

C.9.9.2. Beheer van cryptografische sleutels en certificaten

Beheersmaatregel
Voor het beheren van cryptografische sleutels en certificaten geldt een apart beheerregiem om ongeautoriseerde toegang of verlies van bedrijfskritische gegevens te voorkomen.

Implementatierichtlijnen (Code 12.3.1.d, 12.3.1.e, 12.3.2)
1. Voor het beheer van sleutels/certificaten voor de organisatie of IT-voorzieningen gelden aparte procedures met extra waarborgen voor de vertrouwelijkheid en integriteit.
2. Een centrale vertrouwde instantie of functie is verantwoordelijk voor de uitvoering en controle van de sleutelbeheerprocedures gedurende levensfasen van sleutels en certificaten; bij Multy Party Control is er een aparte bedrijfsvertegenwoordiger (auditor) voor controle en verslag daarover.
3. De Centrale Sleutelbeheerder heeft een uitvoerende rol in de sleutelprocedure; bij Multy Party Control is er een tweede Centraal Sleutelbeheerder.
4. De Decentrale Sleutelbeheerder voert de technisch handelingen uit op de (cryptografische) systemen; bij Multy Party Control is er een tweede Decentraal Sleutelbeheerder.
5. De Kluisbeheerder heeft toegang tot het algemene deel van de kluis; bij Multy Party Control is er een tweede Kluisbeheerder voor het tweede compartiment, die tevens tweede Centraal Sleutelbeheerder is.
6. Er is functiescheiding tussen Centrale Sleutelbeheerder en Decentrale Sleutelmeester en tussen Kluisbeheerder en Decentrale sleutelmeester; bij Multy Party Control tussen eerste en tweede overeenkomstige functies.
7. Gebruikers krijgen bij uitreiking van sleutels altijd een instructie hoe de sleutels moeten worden geactiveerd, hoe ze toegang tot de sleutels krijgen, wanneer en hoe het wijzigen van sleutels verloopt en hoe te handelen bij het compromitteren van sleutels: intrekken of deactiveren.
8. De beschikbaarheid van sleutelparen/sleutels is gewaarborgd door het maken van back-ups/reservekopieën. Dit geldt voor zowel actieve als verlopen sleutelparen.
9. De logische en fysieke toegangsbeveiliging van de opgeslagen sleutels in de cryptohardware is strikt gewaarborgd.
10. De exploitatieorganisatie heeft te allen tijde technisch de mogelijkheid om verloren of gecompromitteerde encryptiesleutels te vervangen. Hiervoor gelden schriftelijke aanvraagprocedures via de centrale vertrouwde instantie of functie.
11. De levensduur van sleutelparen wordt met een vaste periodiciteit (bijv. 1 jaar) verlengd.
12. Alle handelingen met betrekking tot het sleutelbeheer worden vastgelegd.

C.9.9.3. Controleren beveiligingsinstellingen

Beheersmaatregel
De beveiligingsinstellingen van de voorzieningen worden regelmatig gecontroleerd op overeenstemming met de technische documentatie.

Afbakening
Bedoelde controles worden in ieder geval verricht voor die IT-voorzieningen die onderdeel uitmaken van de logische toegangspaden tot gegevens en voor de voorzieningen van fysieke aard, die bepalend zijn voor de fysieke toegangscontrole.

Implementatierichtlijnen
1. Toegangsverkeer buiten de algemene openstellingstijden tot fysieke voorzieningen met automatische

detectie wordt als beveiligingsincident beschouwd.
2. De beveiligingsinstellingen van IT-voorzieningen worden getoetst volgens de daarvoor geldende technische documentatie, onafhankelijk van de technische beveiligingsbeheerders. (Code 15.2.2)
3. Voorzieningen die een vitale functie vervullen in het kader van de gegevensbescherming of die extra risico's lopen op beveiligingslekken, worden periodiek gecontroleerd door onafhankelijke specialisten door middel van penetratieproeven en kwetsbaarheidsbeoordelingen. Zulke testen worden gepland en gedocumenteerd en zijn herhaalbaar. (Code 15.2.2)
4. De mate waarin risico's worden gelopen, is bepalend voor de frequentie van de controle op beveiligingsinstellingen van de voorzieningen.
5. Afwijkingen van de voorgeschreven frequentie van de controle op beveiligingsinstellingen worden aan de functioneel beheerder van de voorziening en aan tactisch beveiligingsbeheer gerapporteerd.

C.9.9.4. Beheersmaatregelen voor audits op de technische infrastructuur

Beheersmaatregel
Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op technische voorzieningen in productie, worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

Toelichting
Onder technische voorzieningen worden in dit verband verstaan die IT-voorzieningen die onderdeel uitmaken van de logische toegangspaden tot gegevens en de voorzieningen van fysieke aard, die bepalend zijn voor de fysieke toegangscontrole.

Implementatierichtlijnen (Code 15.3.1, 15.3.2)
1. De auditeisen worden met de juiste managers overeengekomen.
2. De reikwijdte van de controles wordt overeengekomen en beheerst;
3. De controles worden beperkt tot alleen-lezen-toegang ('read-only') tot programmatuur en gegevens.
4. Andere toegang dan 'alleen lezen' wordt uitsluitend toegelaten voor geïsoleerde kopieën van systeembestanden, die na beëindiging van de audit weer worden gewist of op een juiste wijze worden beschermd indien de auditdocumentatie dit vereist.
5. Hulpmiddelen voor de uitvoering van de controles worden expliciet vastgesteld en beschikbaar gesteld.
6. De hulpmiddelen voor systeemaudits, bijvoorbeeld programmatuur of gegevensbestanden, worden gescheiden van ontwikkelingssystemen en productiesystemen en worden niet opgeslagen in bibliotheken of gebruikersruimte, tenzij hiervoor aanvullende beschermingsmaatregelen van een geschikt niveau zijn getroffen.
7. Eisen voor bijzondere of aanvullende verwerking worden vastgesteld en overeengekomen.
8. De uitvoerenden van de audit hebben geen belangen bij de uitkomst van de audit.

C.9.10. Fysiek sleutelbeheer

Beheersmaatregel
Het fysiek sleutelbeheer beheert fysieke sleutels op zodanige wijze dat onbevoegden er geen gebruik van kunnen maken.

Implementatierichtlijnen
1. Er is vastgesteld van welke soort sleutels een voorraadregistratie wordt bijgehouden.
2. Er is een sleutelplan, waarin is vastgelegd aan welke functionarissen te registreren sleutels worden uitgereikt onder welke voorwaarden van gebruik, inclusief de inrichting van het beheer.
3. Het gebruik van reserve- en noodprocedures leutels voor gebouwen, kritische ruimten, kluizen en kasten kent een apart beheerregiem met aandacht voor registratie van het gebruik met opgave van reden en extra onafhankelijke controle bij het toepassen van de noodprocedure.
4. De niet-uitgereikte of niet-in-gebruik-zijnde sleutels van een locatie worden in een afgesloten inbraakwerend(e) kast(je) of kluis bewaard.
5. Periodiek wordt gecontroleerd of alle sleutels volgens het sleutelplan zich in de kast of kluis bevinden dan wel bij de juiste functionaris aanwezig zijn.

C.10. Loketfunctie

C.10.1. Inleiding

Doelstelling
Het bieden van het enige loket /aanspreekpunt voor het melden van incidenten, het geven van werkopdrachten, het stellen van vragen en het ondersteunen van de klantorganisatie.

Toelichting
Het behandelen van vragen en werkopdrachten, het ontvangen van meldingen vervult een rol voor de processen:

Informatiebeheer
3.5 Centraal uitvoerend informatiebeheer;

Beheer en exploitatie IT (ITIL-proces Request fulfillment):
9.5 Aanvragen autorisaties;
12.8 Release & Deployment Management voor het installeren van hard- en software;
12.9 Incident Management voor calls van het type “incident”;
12.12 Operations management voor incidentele productie-opdrachten;

Leveren Huisvesting
13. Leveren huisvesting voor alle aanvragen en meldingen.

Organisatorisch kunnen er om praktische redenen, bijvoorbeeld voor specifieke product- of klantgroepen, afzonderlijke processen worden ingericht, zolang ze maar onder een centrale regie vallen.

Motivering
Door het centraliseren van de ontvangst van vragen en werkopdrachten worden goede voorwaarden geschapen voor het ordelijke afdoen ervan. Bevoegdheidscontrole is essentieel voor het handhaven van functiescheidingen in een organisatie (vooral bij het in behandeling nemen van autorisatieaanvragen) en kan het onbevoegd ontsluiten of vernietigen van gegevens voorkomen. Door eenduidige en bekende kanalen voor vraagafhandeling kunnen oneigenlijke handelingen bij eindgebruikers voor een deel worden voorkomen.

Afbakening
Het behandelen vragen en werkopdrachten wordt alleen voor de klantcontacten op operationeel niveau uitgewerkt.

Beheersmaatregel
Werkopdrachten en meldingen worden geregistreerd, gecontroleerd op bevoegdheid en bewaakt op afhandeling.

Implementatierichtlijnen
1. Er wordt voorlichting gegeven over het centraal kunnen afhandelen van vragen en werkopdrachten.
2. Alle werkopdrachten en meldingen worden geregistreerd. Dit geldt ook voor opdrachten die meteen kunnen worden afgehandeld.
3. Elke opdracht krijgt een unieke identificatie die wordt teruggemeld aan de opdrachtgever.
4. Er is vastgesteld welke typen opdrachten rechtstreeks afgehandeld worden. Hiervoor gelden standaard afhandelingsinstructies.
5. Van ingediende werkopdrachten wordt vastgesteld dat zij door bevoegden zijn geautoriseerd, voordat zij in behandeling worden genomen.
6. Voor het afhandelen en bewaken van opdrachten, die afwijken van de standaard dienstverlening worden procedures gehanteerd die zijn afgestemd met de processen, waarin de werkzaamheden moeten worden uitgevoerd.
7. Werkopdrachten en meldingen worden bewaakt op afhandeling.
8. De opdrachtgevers krijgen een terugmelding wanneer de opdracht c.q. melding afgehandeld is.

C.11. Leveren applicaties

C.11.1. Inleiding

Doelstelling
Leveren applicaties is het technisch ontwerpen, realiseren en testen van toepassingsprogrammatuur volgens het functioneel detailontwerp.

Motivering
Dit proces draagt ervoor zorg dat de uiteindelijk op te leveren applicatie voldoet aan de eisen van Informatiemanagement inclusief de geprogrammeerde controles, zoals die worden gedocumenteerd in de beveiligingsparagraaf van het detailontwerp.

Implementatierichtlijnen
1. De kwaliteitsbeheersing is in overeenstemming met 3.4 Kwaliteitsbeheer.
2. Het ontwikkelen en gebruiken van systeemroutines dan wel programmatuur voorkomt het verlenen van speciale bevoegdheden aan systeembeheerders. (Code 11.2.2.d, 11.2.2.e)
3. In het ontwerp is beschreven welke directe en indirecte licenties van ingekochte software worden gebruikt in de (IT-)dienstverlening en hoe het verbruik hiervan wordt geregistreerd.
4. Bij uitbesteding van applicatieontwikkeling wordt de opgeleverde programmatuur voorafgaand aan installatie getest om eventuele virussen en Trojaanse paarden te ontdekken. (12.5.5.f)
5. Wijzigingen in softwarepakketten worden vermeden. Indien dit toch noodzakelijk wordt geacht, wordt rekening gehouden met de volgende punten:
a. het risico dat ingebouwde beveiligingsmaatregelen en integriteitprocessen gecompromitteerd kunnen worden;
b. eventuele noodzakelijke toestemming van de leverancier;
c. de mogelijkheid om de gewenste wijzigingen te verkrijgen van de leverancier;
d. de impact op het toekomstig onderhoud van de software.
6. Voor IT-dienstverlening die van invloed is op de geldstroom dient in het ontwerp en de testspecificaties zichtbaar rekening te worden gehouden met het beperken van het risico dat oneigenlijke programmatuurregels (i.v.m. afrondingen) worden toegevoegd.
7. De acceptatietestomgeving is representatief voor de toekomstige exploitatieomgeving.
8. Het gebruik van operationele databases met persoonlijke informatie of enige andere gevoelige informatie voor testdoeleinden wordt vermeden, tenzij dit leidt tot onevenredige inspanningen en kosten, zulks ter beoordeling door de gegevensbeheerder. Ingeval er met kopieën van productiegegevens (b.v. in de acceptatie- of testomgeving) wordt gewerkt, worden de volgende maatregelen getroffen:
a. de privacybepalende of anderszins gevoelige informatie in de kopieën van de productiedata worden verwijderd of aangepast, zodat het onherkenbaar is; (Code 12.4.2) algemeen)
b. de toegangsprocedures die voor besturingssystemen worden gebruikt, worden ook gebruikt voor testsystemen; (Code 12.4.2.a)
c. telkens wanneer besturingsinformatie (o.a. instellingsparameters) naar een testsysteem wordt gekopieerd, wordt per keer autorisatie verkregen; (Code 12.4.2.b)
d. besturingsgegevens worden onmiddellijk na beëindiging van de proef van het testsysteem gewist; (Code 12.4.2.c)
e. kopiëren en gebruik van besturingsgegevens wordt geregistreerd om in een ‘audit trail’ te voorzien; (Code 12.4.2.d) of
f. als niet aan punt a kan worden voldaan, wordt bij tactisch beveiligingsbeheer advies ingewonnen over aanvullende maatregelen en worden deze met de gegevensbeheerder afgestemd.
9. In de systeemdocumentatie zijn aanwijzingen opgenomen voor het geval dat bestands- en/of gegevensmanipulaties door een optredend incident noodzakelijk zijn.

C.11.2. Secure Programming

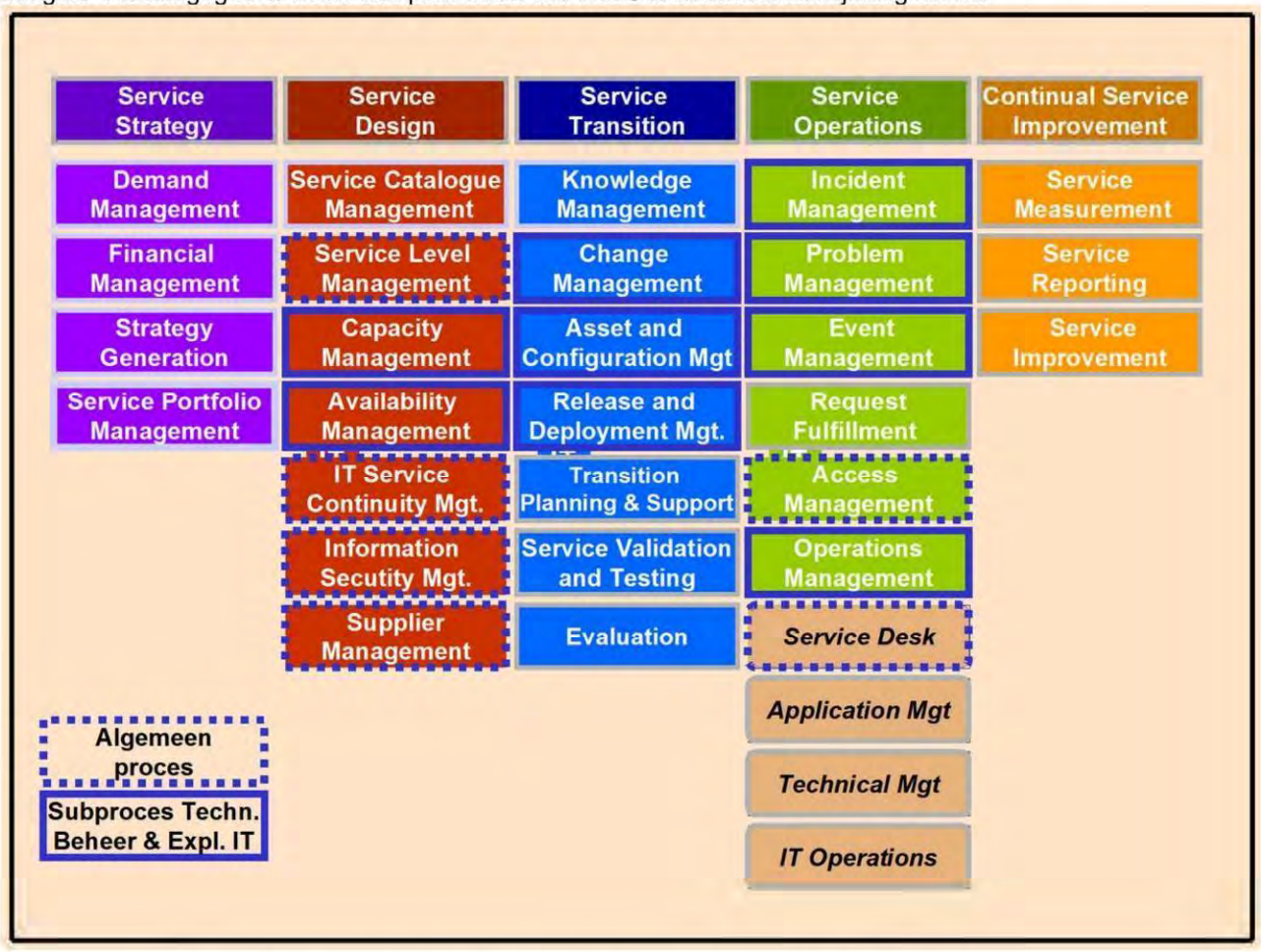
Dit onderdeel moet nog worden uitgewerkt, mede op basis van het Raamwerk Beveiliging Webapplicaties van Govcert, Publieke uitgave: 30.07.2009. Tot deze beheersmaatregelen/implementatierichtlijnen behoort:
11.2.1 Waarborgen dat de opslag van de transactiedetails wordt gedaan buiten enige openbaar toegankelijke omgeving, bijvoorbeeld een opslagplatform op het intranet van de organisatie, en niet ondergebracht en toegankelijk op een opslagmedium dat direct via het internet toegankelijk is. (Code 10.9.2.e)

C.12. Leveren technisch beheer en exploitatie

C.12.1. Inleiding

Technisch beheer en exploitatie IT stelt op basis van klantafspraken gegevens en IT-voorzieningen in de ruimste zin van dit begrip beschikbaar, houdt deze in stand en voert productie-opdrachten uit.
De verscheidenheid aan werkzaamheden die onder deze noemer vallen is bijzonder groot, zodat verder verwezen wordt naar de meer gedetailleerde doelstellingen in de paragrafen in dit hoofdstuk.

Toelichting
Onder het hoofd Technisch beheer en exploitatie worden een 12-tal sub-processen onderscheiden.
In figuur 4 is aangegeven welke sub-processen van ITIL-3 in dit hoofdstuk zijn uitgewerkt.



Figuur 4 In dit normenkader uitgewerkte (sub)processen (zie blauwe kaders)

In dit ITIL-framework is niet een eenduidig ontwikkelproces voor de technische infrastructuur aan te wijzen; meerdere processen en activiteiten spelen hierbij een rol. Voor dit normenkader wordt hiervoor het vervangende proces Ontwikkelen en onderhouden Technische infrastructuur gebruikt.
De volgende processen zijn – vanwege hun algemene karakter – buiten dit hoofdstuk uitgewerkt, maar zijn onlosmakelijk met de wel in dit hoofdstuk uitgewerkte processen verbonden:

- Service Level Management, zie 8. Afnemersbeheer;
- IT Service Continuity Management, zie 9.2.3 Pannen bedrijfscontinuïteitsbeheer en 9.2.6 Testen, bewustwording, evaluatie en onderhoud plannen bedrijfscontinuïteit;
- Information Security Management, zie 9.2 Tactisch beveiligingsbeheer;
- Supplier Management, zie 7. Leveranciersbeheer;
- Access Management, zie 9.9.1 Beheer toegangsregels;

- Service Desk, zie 10. Loketfunctie.

De beveiligingsrelevante kleinere onderdelen van de andere ITIL-3-processen zijn ondergebracht in de verschillende paragrafen van 9. Beveiligingsbeheer om versnippering van normen te voorkomen.

Motivering
Nadat het ontwikkelingstraject ervoor heeft moeten zorgen dat er in opzet beveiligde IT-voorzieningen zijn opgeleverd, zal Technisch beheer en exploitatie het bestaan en de voortdurende werking van de beveiligingsmaatregelen in de IT-voorzieningen moeten borgen, vooral ook in de onderhoudsfase, opdat er sprake kan zijn van een voortdurende, technisch betrouwbare, geautomatiseerde gegevensverwerking.

C.12.2. Algemeen exploitatie

Beheersmaatregel
Bij technisch beheer en exploitatie van IT worden functiescheidingen in acht genomen.

Implementatierichtlijnen
1. Er is scheiding aangebracht tussen de volgende essentiële activiteiten binnen Technisch beheer en exploitatie: (Code 10.1.3) vult dat minder concreet in)
a. beschikkende functies en daarbinnen tussen:
 - 8. Afnemersbeheer,
 - de tactische dienstverleningsprocessen: 9.2 Tactisch beveiligingsbeheer, 12.4 Capacity Management, 12.5 Availability Management,
 - 7. Leveranciersbeheer;
b. bewarende/operationeel beherende functies en daarbinnen tussen:
- het gegevensbeheer van identificerende en classificerende gegevens van alle beheerregistraties,
- het beheer van computerruimten en hardware-voorzieningen bij 12.12 Operations management,
- het beheer van 'known errors' bij 12.10 Problem Management,
- het beheer van encryptiesleutels bij creatie, uitgifte en herstel of vervanging van sleutels bij 9.9.2 Beheer van cryptografische sleutels en certificaten;
c. registrerende functies, zoals het registreren van:
- CI's door 12.7 Asset and configuration Management,
- opdrachten door 10. Loketfunctie,
- incidenten door 12.9 Incident Management,
- wijzigingen door 12.6 Change Management,
- programma's/releases door 12.8 Release and Deployment Management;
d. uitvoerende functies en daarbinnen tussen
- netwerkbeheer en productiebeheer, (Code 10.6.1.a)
- degenen die de beveiligingsinstellingen van het normbestand kunnen muteren en degenen die de gesignaleerde afwijkingen afhandelen bij automatische controles op beveiligingsinstellingen;
e. controlerende functies.
2. Bij vervangingsregelingen mogen de functiescheidingen niet worden doorbroken.
3. Bij nood- of escalatieregelingen mogen de functiescheidingen alleen worden doorbroken door de hogere managementlaag, waarbij dit onverwijld schriftelijk wordt vastgelegd. Na afloop van de calamiteit wordt onafhankelijk nagegaan of er geen compromittering heeft plaatsgevonden en of de functiescheiding (bijv. wijzigen alle wachtwoorden) ten volle hersteld is.
4. Medewerkers van de exploitatieorganisatie hebben geen toegang tot gebruikersfuncties en productiegegevens van klanten, tenzij zij expliciet door de gegevensbeheerder zijn geautoriseerd.
5. Er zijn waarborgen dat wijzigingen in de organisatie door 9.2 Tactisch beveiligingsbeheer wordt getoetst aan het overeengekomen beveiligingsniveau.

C.12.3. Ontwikkelen en onderhouden Technische infrastructuur

Doelstelling
Bij het ontwikkelen en onderhouden van de technische infrastructuur wordt voldaan aan de beveiligingseisen.

Toelichting
Het proces Ontwikkelen en onderhouden technische infrastructuur is verantwoordelijk voor de inrichting van de beveiliging van de technische infrastructuur en is daarmee van groot belang voor het geheel van de

beveiligingsmaatregelen. De maatregelen in veel andere processen moeten aansluiten op de technische beveiligingsmaatregelen.

Motivering
Het proces Ontwikkelen en onderhouden Technische infrastructuur is verantwoordelijk voor de inrichting van de beveiliging van de technische infrastructuur en daarmee van groot belang voor het geheel van de beveiligingsmaatregelen. De maatregelen in veel andere processen moeten aansluiten op de technische beveiligingsmaatregelen.

C.12.3.1. Beheersen ontwerp en onderhoud

Beheersmaatregel
De besturing van het ontwerp en onderhoud van de technische infrastructuur vindt op ordelijke wijze plaats.

Implementatierichtlijnen
1. De sturing van nieuwbouw en onderhoud van de technische infrastructuur is in overeenstemming met paragraaf 3.2.
2. De fasering van nieuwbouw en onderhoud van de technische infrastructuur is in overeenstemming met paragraaf 3.3
3. De kwaliteitsbeheersing in overeenstemming met paragraaf 3.4.

C.12.3.2. Pro-actief onderhoud

Beheersmaatregel
De voorzieningen van de technische infrastructuur worden pro-actief onderhouden teneinde leemten in de beveiliging te voorkomen.

Implementatierichtlijnen
1. Rollen en verantwoordelijkheden zijn gedefinieerd en vastgelegd met betrekking tot het beheer van technische kwetsbaarheid, waaronder controle van de risico's, risicobeoordeling van de kwetsbaarheid, installeren van herstelprogrammatuur, nalopen van bedrijfsmiddelen en alle vereiste coördinatieverantwoordelijkheden. (Code 12.6.1.a)
2. Voor programmatuur en andere technologie worden informatiebronnen vastgesteld om de relevante technische kwetsbaarheden te bepalen en het veiligheidsbewustzijn levend te houden; deze informatiebronnen worden geüpdate op basis van veranderingen in de Configuratie-Items of wanneer er nieuwe en nuttige hulpbronnen worden gevonden. (Code 12.6.1.b)
3. Door het systematisch raadplegen van leveranciersinformatie en informatie van gekwalificeerde bronnen en specialistische platforms, wordt vastgesteld in hoeverre de eigen technische infrastructuur zwakheden of beveiligingslekken vertoont. (Code 6.1.7.c, 10.4.1.g, 10.4.1.h)
4. Risico's die gepaard gaan met het installeren van het herstelprogramma worden beoordeeld t.o.v. de risico's die worden gelopen door de kwetsbaarheid. (Code 12.6.1.f)
5. Nieuwe releases en patches worden getest en beoordeeld voordat ze worden geïnstalleerd om te waarborgen dat ze doeltreffend zijn en geen ontoelaatbare neveneffecten met zich meebrengen. (Code 12.6.1.g)
6. Nieuwe releases en patches o.a. wegens zwakheden en beveiligingslekken worden tijdig geïnstalleerd dan wel er andere beheersmaatregelen genomen. (Code 12.6.1.c, 12.6.1.d)
7. Het installeren van nieuwe releases en patches doorloopt de procedures van Change Management. (Code 12.6.1.e)
8. Er wordt zorggedragen voor regelmatige updates van de bestanden met viruskenmerken.
9. Bij patches en anti-virusupdates, die vanaf Internet worden gedownload, wordt gecontroleerd dat met de juiste Internetsite contact is gelegd en/of wordt het gebruik van digitale handtekeningen geverifieerd. (Code 10.4.1.h)
10. Er zijn beheerprocedures en verantwoordelijkheden vastgesteld voor de bescherming tegen virussen op systemen, training in het gebruik ervan, rapportage en herstel van aanvallen met virussen (Code 10.4.1.e)
11. De resultaten van interne controles op beveiligingsinstellingen worden geëvalueerd op grond waarvan voorstellen tot aanpassing van beveiligingsdocumentatie worden uitgewerkt dan wel de instellingen zelf worden aangepast.

C.12.4. Capacity Management

Doelstelling
Capacity Management draagt zorg voor het aanwezig zijn van voldoende capaciteit van de IT-diensten en IT-voorzieningen in overeenstemming met het afgesproken niveau van dienstverlening en met de doelstellingen van het management.

Toelichting
Onder capaciteit wordt verstaan: ruimte voor gegevensopslag, voldoende processorvermogen voor de afgesproken verwerkingen, bij on-line verwerking resulterend in het kunnen realiseren van afgesproken responsetijden voor gedefinieerde tijdvakken, rekening houdend met piekverwerking.

Motivering
Het proces Capacity Management draagt in belangrijke mate bij aan de beschikbaarheid van de geautomatiseerde gegevensverwerking.
Indien de geautomatiseerde gegevensverwerking stagneert door onvoldoende resources, kan dat aanleiding geven tot slechte responsetijden, doorbreking van verwerkingscycli en te late aanlevering van gegevens aan opeenvolgende processen. Onvolledige verwerking kan de integriteit van de gegevensverwerking schaden. Onacceptabele responsetijden kunnen irritaties bij gebruikers oproepen, die daardoor eerder fouten gaan maken of oneigenlijke oplossingen gaan verzinnen.

Afbakening
Het proces Capacity Management heeft geen betrekking op de inzet van personeel. Er wordt vanuit gegaan dat de personele capaciteit een afgeleide is van de prestatieafspraken in de dienstverleningsovereenkomsten.
De belangrijkste maatregelen voor voldoende capaciteit worden getroffen in de inrichting van de technische infrastructuur onder verantwoordelijkheid van het proces 12.3 Ontwikkelen en onderhouden Technische infrastructuur in combinatie met het proces 12.11 Event Management dat signalen afhandelt om capaciteitsoverschrijdingen tijdens de verwerking te voorkomen. Capacity Management als tactisch proces ziet toe op het voldoende aanwezig zijn van capaciteit in de IT-voorzieningen.

C.12.4.1. Plannen capaciteit

Beheersmaatregel
Voor alle relevante IT-voorzieningen wordt het capaciteitsbeslag dusdanig gepland dat continu wordt voldaan aan de eisen gesteld in de Dienstverleningsovereenkomsten.

Implementatierichtlijnen
1. De werklast van de verschillende IT-diensten is geïnventariseerd in een capaciteitsplan voor de IT-voorzieningen, waarbij rekening is gehouden met mogelijke piekbelastingen. (Code 10.3.1)
2. Er zijn voorzieningen getroffen om de werklast evenwichtig over servers en netwerken te kunnen verdelen, bij voorkeur wordt daarbij gebruik gemaakt van modellen waarmee de capaciteitsbelasting van nieuwe diensten en/of gewijzigde diensten kan worden gesimuleerd.
3. Nieuwe en gewijzigde met klanten overeengekomen capaciteitsafspraken voor IT-diensten worden vertaald naar het capaciteitsplan, dat capaciteitswijzigingsvoorstellen, investeringsvoorstellen, voorstellen voor aanpassing van het afgesproken niveau van dienstverlening en andere acties bevat die nodig zijn om op de langere termijn in een optimale performance en capaciteitsbenutting te kunnen blijven voorzien. (Code 10.3.1)
4. Er wordt bijzondere aandacht besteed aan IT-voorzieningen met lange levertijden of hoge kosten. (Code 10.3.1)

C.12.4.2. Evalueren en bijstellen capaciteit

Beheersmaatregel
Het capaciteitsplan wordt voortdurend geëvalueerd en bijgesteld op basis van opgetreden capaciteitsoverschrijdingen en wijzigingen in de IT-voorzieningen.

Implementatierichtlijnen
1. Voorstellen voor nieuwe en/of te wijzigen IT-voorzieningen worden getoetst op consequenties voor de capaciteitsplanning.

2. Op grond van de gerapporteerde afwijkingen van instelwaarden voor capaciteit en eventuele wijzigingen in de besteltermijnen voor IT-voorzieningen wordt het capaciteitsplan bijgesteld, worden adviezen gegeven voor aanpassing van applicaties (application sizing) en worden wijzigingsvoorstellen ingediend voor aanpassing van de technische infrastructuur of een andere verdeling van de werklast.

C.12.5. Availability Management

Doelstelling
Availability Management draagt ervoor zorg voor dat alle voorwaarden aanwezig zijn om de IT-diensten onder normale bedrijfsomstandigheden beschikbaar te houden op de normale productielocatie, in overeenstemming met het afgesproken niveau van dienstverlening.

Motivering
Availability Management vervult een belangrijke rol voor het aspect beschikbaarheid van beveiliging.

Afbakening
Het bepalen van de beschikbaarheidseisen voor de dienstverlening is de verantwoordelijkheid van de klantorganisatie en van het management van de serviceorganisatie.
De belangrijkste preventieve maatregelen voor beschikbaarheid worden getroffen in de inrichting van de technische infrastructuur onder verantwoordelijkheid van het proces 12.3 Ontwikkelen en onderhouden Technische infrastructuur dat in combinatie met het proces 12.11 Event Management signalen afhandelt om onbeschikbaarheid in de verwerking zelf te voorkomen. Availability Management als tactisch proces ziet toe op het op elkaar afgestemd zijn van alle maatregelen voor beschikbaarheid, m.u.v. de maatregelen voor calamiteitenbeheersing, waarvoor het proces 9.2.3 Plannen bedrijfscontinuïteitsbeheer verantwoordelijk is.

C.12.5.1. Plannen beschikbaarheid

Beheersmaatregel
Er is een beschikbaarheidsplan waarin de klanteisen voor beschikbaarheid van IT-diensten is vertaald naar alle daarvoor in te zetten middelen bij Technisch beheer en exploitatie IT.

Implementatierichtlijnen
1. Er is een actueel, gedocumenteerd en door het management geaccordeerd beschikbaarheidsplan waarin de klanteisen voor beschikbaarheid van IT-diensten is vertaald naar alle daarvoor in te zetten middelen bij Technisch beheer en exploitatie IT. Bij middelen gaat het onder meer om:
a. IT-voorzieningen en de wijze waarop deze redundant zijn geconfigureerd;
b. locaties van computerruimten;
c. personele aanwezigheid (bijv. stand-by regeling);
d. onderhouds- en vervangingsplan;
e. instelwaarden voor Event management.

C.12.5.2. Evalueren en bijstellen beschikbaarheidsplan

Beheersmaatregel
Het beschikbaarheidsplan wordt voortdurend geëvalueerd en bijgesteld op basis van opgetreden onbeschikbaarheid en wijzigingen in de voor beschikbaarheid ingezette middelen.

Implementatierichtlijnen
1. Wijzigingsvoorstellen voor de middelen die bepalend zijn voor het voldoen aan de eisen voor beschikbaarheid worden getoetst en zonodig doorvertaald naar het beschikbaarheidsplan en wijzigingsvoorstellen en andere acties om de beschikbaarheid op de langere termijn op niveau te houden of verder te verbeteren.
2. De gerapporteerde onbeschikbaarheid wordt geëvalueerd, waarbij wordt nagegaan in hoeverre dit moet leiden tot wijzigingen in het beschikbaarheidsplan.
3. Er wordt toegezien op het naleven van het beschikbaarheidsplan inclusief het realiseren van voorstellen voor wijziging van de ingezette middelen.

C.12.6. Change Management

Doelstelling
Het Change Managementproces zorgt er voor dat wijzigingen in de IT-voorzieningen en -diensten met zo min mogelijk verstoring van de kwaliteit van de dienstverlening worden uitgevoerd.

Toelichting
Het proces ondersteunt de acceptatie, registratie, planning en bewaking van de wijzigingen. Het is in eerste instantie een coördinerend en bewakend proces, dat zelf geen uitvoerende taken bij het bouwen, testen en implementeren vervult.

Motivering
De ervaring leert dat het doorvoeren van wijzigingen vaak leidt tot verstoringen in de IT-dienstverlening. Het gecontroleerd doorvoeren van wijzigingen moet de kans daarop verminderen en bevorderen dat eventuele toch opgetreden storingen korter duren (door in wijzigingsproces ingebouwde voorzieningen voor terugdraaien van wijzigingen).
Het Change Management-proces biedt het proces tactische beveiliging de mogelijkheid om wijzigingen eerst op beveiligingsconsequenties te toetsten voordat ze worden uitgevoerd. Dit vermindert de kans op het ontstaan van beveiligingsincidenten en bevordert pro-actief het continue blijven voldoen aan de normen voor het bedrijfsmiddel infrastructuur.

Afbakening
Het Change Management-proces omvat niet het wijzigen van beleid, organisatie en procedures, die ook voor beveiliging zeer relevant kunnen zijn.

C.12.6.1. Accepteren wijzigingen

Beheersmaatregel
Voorgestelde wijzigingen worden geautoriseerd, geregistreerd en geclassificeerd met inachtneming van de impactanalyse.

Implementatierichtlijnen
1. Er is vastgelegd welke functionarissen welke typen wijzigingen mogen aanvragen. Er worden alleen geautoriseerde voorgestelde wijzigingen in behandeling genomen. (Code 12.5.1.a)
2. Alle wijzigingen worden geregistreerd in een Change Management-systeem. Dit Change Management-systeem voldoet aan de volgende eisen:
a. unieke identificatie van wijzigingen; (Code 10.1.2.a)
b. mogelijkheden om de verschillende stappen in het changeproces vast te leggen;
c. mogelijkheden om te registreren welke configuration items bij de wijziging zijn betrokken (bevat relatie met de Configuration Management Database); (Code 12.5.1.d)
d. mogelijkheid om te registreren voor welke problemen en known errors de wijziging een oplossing biedt (bevat relatie met de problemregistratie);
e. voorzieningen voor de rapportage over de status van wijzigingen en het verloop van het Change Management-proces (aantallen wijzigingen wachtend op goedkeuring, aantal teruggedraaide wijzigingen etc.).
f. er is van 'audit trail' van alle wijzigingsaanvragen (Code 12.5.1.i)
3. Voorgestelde wijzigingen worden geautoriseerd met inachtneming van de impactanalyse. (Code 10.1.2.c, 12.5.1.e)
4. Ingeval de adviezen vanuit de tactische beheerprocessen niet volledig of tijdig (kunnen) worden geïmplementeerd, wordt - bijvoorbeeld door het instellen van een projectgroep - gezorgd voor algemeen gedragen besluitvorming. (Code 10.1.2.c)
5. Voorgestelde wijzigingen worden toegewezen aan wijzigingscategorieën. Hierbij gelden de volgende aanvullende normen:
a. er zijn objectieve criteria vastgelegd op grond waarvan bepaald kan worden in welke categorie een wijziging thuishoort. De Change Manager ziet er op toe dat deze criteria juist worden toegepast;
b. er zijn in elk geval categorieën voor spoedeisende (emergency), standaard en omvangrijke (major) wijzigingen;
c. aan elke categorie zijn specifieke afhandelingsprocedures gekoppeld, waarin o.m. is geregeld:
  1. op welke wijze impactanalyse plaatsvindt op beschikbaarheid, capaciteit, beveiliging, continuïteit en exploiteerbaarheid/gebruik; (Code 10.1.2.c)

2. dat voor routinematige wijzigingen standaardprocedures en –checklists worden gehanteerd;
3. dat er voor spoedeisende wijzigingen een aparte procedure is waarbij eventueel achteraf het changeproces alsnog wordt doorlopen;

d. in de afhandelingsprocedure is begrepen dat alle wijzigingen worden geautoriseerd door de budgethouder, functioneel en technisch beheerder.

C.12.6.2. Plannen wijzigingen

Beheersmaatregel
Voorgestelde wijzigingen worden geprioriteerd en gepland in overleg met alle belanghebbenden.

Implementatierichtlijnen
1. Er is een beslissingsforum van alle belanghebbenden (de Change Advisory Board, CAB), die de prioriteit van wijzigingen bepaalt en die toestemming verleent voor realisatie en implementatie.
a. de CAB is zodanig samengesteld dat er een evenwicht bestaat tussen de belangen van de beheer- en exploitatieorganisatie (continuïteit en stabiliteit) en de klantenorganisatie (nieuwe functionaliteit); (Code 12.5.1.f, 6.1.4.a)
b. In de CAB zijn de vertegenwoordigers van de tactische beheerprocessen (Capacity Management, Tactisch beveiligingsbeheer (Code 12.5.1.c, 6.1.4.a), Availability Management vertegenwoordigd dan wel kunnen via de Change Manager hun standpunten over wijzigingen in de CAB inbrengen. (Code 10.1.2.d)
2. Voorgestelde wijzigingen worden geprioriteerd en gepland in overleg met alle belanghebbenden. Voor het indelen in prioriteitsklassen zijn regels vastgesteld. (Code 10.1.2.b, 10.1.2.e)
3. Planningsgegevens worden gepubliceerd in een algemeen bekend gemaakte wijzigingenkalender. Afwijkingen van de planning worden gesignaleerd en geregistreerd.
4. Op urgente wijzigingen, die niet volledig volgens de reguliere procedure kunnen worden afgehandeld, is een bijzondere procedure van toepassing die vereist dat overgeslagen controlestappen achteraf worden doorlopen.
5. Bij wijzigingen in besturingsprogrammatuur worden de eigenaren van toepassingssystemen tijdig ervan op de hoogte gesteld dat de werking van kritische toepassingssystemen opnieuw beoordeeld moeten worden om zeker te stellen dat er geen nadelige gevolgen zijn voor de controle- en integriteitprocedures. (Code 12.5.2)

C.12.6.3. Uitvoeren wijzigingen

Beheersmaatregel
Wijzigingen worden onder gecontroleerde condities ingevoerd.

Implementatierichtlijnen
1. Voor elke wijzigingscategorie zijn regels opgesteld voor de omvang en diepgang van de testen.
2. Voor elke wijziging is een terugval scenario opgesteld waarin is vastgelegd waaruit de terugval bestaat, onder welke condities tot een terugval wordt overgegaan en wie daartoe kan besluiten. (Code 10.1.2.f, 12.4.1.e)
3. De formele acceptatie van een wijziging is gebaseerd op de volgende acceptatiecriteria: (Code 10.3.2.a, 10.3.2.b, 10.3.2.c, 10.3.2.d, 10.3.2.e, 10.3.2.f, 10.3.2.g, 10.3.2.h, 10.3.2.i, 10.3.2.j, 12.4.1.c)
a. eisen aan prestaties en capaciteit van het computersysteem;
b. procedures voor foutherstel en herstart;
c. voorbereiding en testen van routinematige bedieningsprocedures volgens welomschreven normen;
d. de normen voor infrastructurele beveiligingsmaatregelen zijn geïmplementeerd;
e. zekerheid dat installatie van het nieuwe systeem geen nadelige invloed heeft op bestaande systemen, ook bij piekverwerkingen; (Code 12.5.1.k)
f. waarborgen dat de bedrijfsdocumentatie en gebruikersprocedures worden aangepast; (Code 12.5.1.j)
g. opleiding in bediening of gebruik van nieuwe systemen.
h. gebruiksgemak, omdat hiermee gebruikersprestaties worden beïnvloed en menselijk fouten wordt vermeden.
4. Het beschikbaar stellen voor gebruik van nieuwe IT-voorzieningen worden goedgekeurd door de desbetreffende functioneel bedrijfsmiddelbeheerder. (Code 6.1.4.a)
5. De relatie tussen bekende fouten van te implementeren wijzigingen worden geregistreerd.

C.12.6.4. Bewaken wijzigingen

Beheersmaatregel
Wijzigingen worden bewaakt op afhandeling.

Implementatierichtlijnen
1. Er wordt voortgangsbewaking uitgeoefend op de afhandeling van (voorgestelde) wijzigingen.
2. Het prioriteren en de voortgangsbewaking van wijzigingen zijn functioneel gescheiden van de uitvoering van wijzigingen.
3. Een wijziging wordt pas afgesloten na controle op afronding van alle activiteiten en registraties voor de wijziging.
4. Er is van 'audit trail' van alle wijzigingsaanvragen

C.12.7. Asset and Configuration Management

Doelstelling
Asset and Configuration Management draagt zorg voor de vastlegging van gegevens over de IT-voorzieningen en IT-diensten en voor het beschikbaar stellen van deze gegevens aan de andere IT-beheerprocessen.

Toelichting
De gegevens over IT-voorzieningen en IT-diensten worden aangeduid als Configuratie-Items (CI's). Tot de CI's horen ook documentatie over de middelen en diensten. Daarnaast worden de relaties tussen deze voorzieningen vastgelegd. Alle vastleggingen worden opgenomen in de Configuratie Management Database (CMDB), die periodiek wordt vergeleken en in overeenstemming gebracht met de werkelijkheid.

Motivering
Asset and Configuration Management is voorwaardenscheppend voor bijna alle andere processen. Voor zover die andere processen een beveiligingsbelang hebben, werkt dat door naar het belang van dit proces. Het proces zelf heeft een beveiligingsbelang in het kader van de integriteitshandhaving, doordat het kan borgen dat updates van CI's overal worden aangebracht waar ze worden gebruikt. Door juiste en volledige informatieverstrekking aan 12.7 Asset and Configuration Management en 12.6 Change Management wordt voorkomen dat er verschillende (en dus verouderde) versies van dezelfde CI in exploitatie komen of zijn. Door het beschikbaar stellen van tekeningen of schematische voorstellingen van systeemvoorzieningen en hun onderlinge (netwerk)verbindingen is mogelijk om fysieke en logische toegangsbeveiligingsaspecten te beoordelen, ook in relatie tot wijzigingen. Het vaststellen of er geen sprake is van single-points-of-failure wordt hierdoor mede mogelijk gemaakt.

C.12.7.1. Plannen registratie configuration items

Beheersmaatregel
Een gestructureerde vastlegging is ontworpen voor configuration items, hun kenmerken en onderlinge relaties (inclusief historische data) en gerelateerde documentatie.

Implementatierichtlijnen (Code 7.1.1.a, 7.1.1.b, 7.1.1.c, 7.1.1.d, 12.4.1.d)
1. De vast te leggen gegevens van de Configuratie-Items sluiten aan op de informatiebehoefte van andere processen. Enkele belangrijke gegevenselementen zijn:
a. technische aspecten (bijvoorbeeld uniek identificatie, type/serienummer, aanschafdatum, relatie met dienst en andere CI's, belang voorziening, consequenties uitval);
b. registratieaspecten (bijvoorbeeld wanneer, door wie en op basis waarvan een verandering in registratie heeft plaatsgevonden);
c. onderhoudsaspecten (bijvoorbeeld onderhoudscontracten, verricht onderhoud, leverancier, dienstverlener);
d. organisatorische aspecten (bijvoorbeeld locatie, beheerder, functioneel houder, technisch houder, budgethouder).
e. aspecten van het beschermen van intellectueel eigendom en bewaring en onderhoud van bijbehorend bewijsmateriaal (Code 15.1.2.d, 15.1.2.e)
f. documentatieaspecten (naamgevingsconventies, identificatie en verwijzing naar vindplaats van documentatie, configuratietekeningen of -schema's van alle locaties).
2. Alle soorten CI's worden in de registratie opgenomen.

3. Er zijn waarborgen dat de systeemdocumentatie van de CI's na elke wijziging wordt geüpdate en dat oude documentatie wordt gearchiveerd of verwijderd. (Code 12.5.1.g)
4. De historische gegevens met betrekking tot een automatiseringshulpmiddel en de daaraan gerelateerde gegevens (auditlogbestand) blijven beschikbaar gedurende een afgesproken periode (5 jaar). (Code 12.4.1.f)
5. Bij het muteren in de CMDB van kenmerken is geborgd dat de relaties consistent blijven.

C.12.7.2. Uitvoeren registratie configuration items

Beheersmaatregel
Procedures zijn ingericht om nieuwe, gewijzigde en verwijderde configuration items te identificeren en te registreren.

Implementatierichtlijnen
1. Alle fysieke CI's worden voorzien van het identificatiekenmerk, dat op deugdelijke wijze op de CI wordt aangebracht.
2. De procedures waarborgen dat alle mutaties in de configuraties juist, volledig en tijdig worden vastgelegd in de registratie.
3. De verantwoordelijkheid voor het opvoeren en muteren van de CI's en daarmee voor de inhoudelijke juistheid van de CMDB is eenduidig in de organisatie belegd.
4. Configuratiebeheer stelt actuele en historische informatie over de geregistreerde Configuratie-Items en de daaraan gerelateerde gegevens ter beschikking.

C.12.7.3. Bewaken registratie configuration items

Beheersmaatregel
Geborgd wordt dat de administratieve gegevens in de configuratiedatabase in overeenstemming zijn met de werkelijkheid.

Implementatierichtlijnen
1. Periodiek (evt. door middel van partieel roulerende inventarisatie) wordt vastgesteld dat de geregistreerde gegevens van CI's in de CMDB overeenkomen met de werkelijkheid. Eventuele verschillen worden verklaard en gecorrigeerd.
2. De periodieke controle borgt dat er alleen toegestane IT-voorzieningen met licentie zijn geïnstalleerd.
3. Ten behoeve van de interne controle binnen de gebruikersorganisatie worden overzichten beschikbaar gesteld, waaruit in gebruik zijnde en nieuw geïnstalleerde informatiesystemen blijken.

C.12.8. Release & Deployment Management

Doelstelling
Release & Deployment Management voert het beheer en de distributie uit van programmatuur- en apparatuurversies, die in gebruik zijn en die door de exploitatieorganisatie worden ondersteund, teneinde te voldoen aan het vereiste niveau van dienstverlening.

Toelichting
Release & Deployment Management is een uitvoerend proces, dat het koppelvlak vormt tussen het ontwikkel-/ onderhoudsproces van programmatuur, het bestelproces van apparatuur en het Operationsproces. Daarbij wordt Release & Deployment Management aangestuurd door 12.6 Change Management (als controlerend proces) en is het deels sturend voor 12. 7 Asset and Configuration Management en Operations.

Motivering
Het Release Management-proces is in medebepalend voor de integriteit van de gegevensverwerking. Het proces moet borgen dat alleen de door de beheerder of opdrachtgever geaccordeerde versies van de programmatuur ter beschikking worden gesteld voor productiedoeleinden. Voorts is dit proces verantwoordelijk voor het veilig bewaren van moederkopieën van alle programmatuur.

Afbakening
De activiteiten samenhangend met het testen en accepteren en alle maatregelen die de inhoudelijke kwaliteit van programmatuur bepalen, worden niet tot het beheer, maar tot het voortbrengingsproces

gerekend.
Het feitelijk implementeren (productierijp maken) van de programmatuur kan afhankelijk van de omgeving (het platform) tot dit proces worden gerekend, maar kan ook thuishoren onder Operations.

C.12.8.1. Beheersysteem Release & Deployment

Beheersmaatregel
Er is een beheersysteem dat het ordelijk beheer van programmatuur en hun versies ondersteunt.

Implementatierichtlijnen
1. Er is een beheersysteem, dat o.m. de volgende registraties verzorgt:
a. de status (ontwikkeling, test, acceptatietest, productie) van de release en release-attributen; (Code 12.5.1.h)
b. de versieaanduiding van de release en release-attributen;
c. de release-aanduiding van de doelservers waarop de toepassingsprogrammatuur van een release draait;
d. de samenstelling van een release naar release-attributen;
e. de releases, waarin een attribuut voorkomt;
f. logging van wijzigingen in releases incl. elke toegang tot broncodebibliotheken; (Code 12.4.3.f)
g. een audit-logboek waarin alle toegang tot bibliotheken met bronprogramma's wordt vastgelegd.
2. Het beheersysteem voorziet in een gescheiden ontwikkel-, acceptatietest- en productieomgeving, waarbij de overdracht van programmatuur tussen deze omgevingen wordt beheerst.
3. Broncodebibliotheken worden niet in de productieomgeving opgeslagen. (Code 12.4.3.a)
4. Het beheersysteem beperkt de bevoegdheden om operationele programmabibliotheken bij te werken tot bevoegde functionarissen. (Code 12.4.3.c)
5. Het beheersysteem draagt ervoor zorg dat de met de beheerder overeengekomen bewaartermijn van de programmaversies wordt gehandhaafd. (Code 12.4.1.g)
6. Oude versies van programmatuur worden gearchiveerd, samen met alle vereiste informatie en parameters, procedures, configuratiedetails en ondersteunende programmatuur zolang er gegevens in het archief worden bewaard. (Code 12.4.1.h)
7. Het onderhouden, kopiëren en afgeven van broncodebibliotheken is onderworpen aan strikte procedures voor wijzigingsbeheer. (Code 12.4.3.b, 12.4.3.d, 12.4.3.g)
8. Periodiek wordt de programmatuur volgens de bestandscatalogi uit de productiesystemen gecontroleerd met de registratie van programmatuur in het beheerssysteem.

C.12.8.2. Overdracht programmatuur

Beheersmaatregel
De overdracht van programmatuur van Ontwikkel-, Test-, en Acceptatieomgevingen naar de Productie omgeving wordt beheerst.

Implementatierichtlijnen (Code 10.1.4.a)
1. Overdrachten naar de acceptatietest- en productieomgeving vinden plaats op basis van geautoriseerde opdrachten. (Code 12.4.1.a)
2. Overdrachten van programmatuurversies tussen de verschillende omgevingen worden geregistreerd.
3. Het bijwerken van bibliotheken met bronprogramma's en het afgeven van bronprogramma's aan programmeurs wordt uitgevoerd door de aangewezen beheerfunctionaris na goedkeuring van de IT onderhoudsmanager voor de betreffende toepassing.
4. Bij overdracht van programmatuur wordt vastgesteld dat geen ontwikkeltools, compilers of broncode wordt aangeboden voor implementatie in de productie- acceptatie- en testomgeving, zodat in deze omgevingen geen aanpassingen van de programmatuur kunnen plaats vinden.
5. Naar de acceptatietestomgeving en productieomgeving overgedragen programmatuur kan niet meer gewijzigd worden. Het is uitsluitend mogelijk deze programmatuur door nieuwe versies te vervangen, die in de ontwikkelomgeving zijn vervaardigd.

C.12.8.3. Distribueren en implementeren programmatuur

Beheersmaatregel
Een distributiesysteem garandeert de juiste implementatie van productversies van programmatuur.

Implementatierichtlijnen

1. Indien mogelijk bevatten operationele servers alleen uitvoerbare code.
2. De implementatie van een release wordt tijdig ingepland in de overall release- of wijzigingenkalender.
3. De wijze waarop de distributie/implementatie van een release moet plaatsvinden, wordt vastgelegd in een implementatieplan en met betrokkenen en opdrachtgever afgestemd.
4. Release & Deployment Management levert de installatiehandleiding t.b.v. de fysieke implementatie inclusief de schoning van vervallen programmatuurversies.
5. De opdrachtprocedure voorziet in identificatie van de over te brengen release en specificatie van het moment waarop deze programmatuur bij de gegevensverwerking gebruikt moet worden.
6. Tijdens de overgang (voor, tijdens en na de invoering) van de release worden maatregelen getroffen om de continuïteit van de operationele werkzaamheden van de eenheden te waarborgen (terugval scenario).
7. Uitsluitend programmatuurvoorzieningen, die deel uitmaken van een tevoren overeengekomen, samenhangend geheel (een release) en voorzien zijn van een vrijgaveadvies van de opdrachtnemer en vrijgaveakkoord van de opdrachtgever, worden gedistribueerd.
8. Er worden alleen releases gedistribueerd die zijn geadministreerd zowel in het beheersysteem als de CMDB.
9. Er worden alleen releases geïmplementeerd op doelservers als de status van de release in overeenstemming is met de omgevingsvereisten (juiste versies van besturings- en toepassingsprogrammatuur en patches).
10. Er wordt vastgesteld dat de implementatie op alle doelservers volledig heeft plaatsgevonden.
11. Een emergency release raakt altijd het versienummer, wordt ook in het beheersysteem en de CMDB geregistreerd en zo spoedig als mogelijk opgevolgd door een complete release waarin met name de documentatie is bijgewerkt.
12. Op basis van licentieovereenkomsten, die het gebruik van de IT-voorzieningen tot bepaalde servers en mogelijk ook het kopiëren van de programmatuur beperken, worden maatregelen getroffen om te waarborgen dat het maximale aantal toegestane gebruikers niet wordt overschreden. (Code 15.1.2.g)

C.12.9. Incident Management

Doelstelling
Incident Management draagt zorg voor het afhandelen van klachten en verstoringen in de IT-dienstverlening en voor het tijdig herstellen van het afgesproken niveau van dienstverlening.

Toelichting
Onder incident wordt verstaan elke gebeurtenis, die niet tot de standaardoperatie van een IT-dienstverlening behoort en die een interruptie of een vermindering van de kwaliteit van die dienstverlening kan veroorzaken.
Bij het herstel is de inzet van tijdelijke reparaties (work-arounds) geoorloofd. Ook kan een wijzigingsverzoek worden ingediend via het proces 12.6 Change Management.

Motivering
Het proces zorgt voor een onafhankelijke registratie van klachten over en storingen in de IT-dienstverlening, zodat er een volledig inzicht kan ontstaan. Het proces zorgt voor het (doen) afhandelen van urgente beveiligingsproblemen samenhangend met beveiligingslekken, virussen e. dergelijk naar een zogenaamd Computer Emergency Response Team (CERT), die als een aparte oplosgroep is te zien. Door een gestructureerde en snelle afhandeling van dit type incidenten kan escalatie van dergelijke storingen worden voorkomen.

Afbakening
Het afhandelen van gebruikersverzoeken om ondersteuning, levering van informatie, advies of documentatie bij het gebruik van informatiesystemen (ook wel aangeduid als “Service Request”) valt niet onder het proces Incident Management. Afhandeling van deze categorie valt onder 10. Loketfunctie.
Het Incident-proces is niet in eerste instantie bedoeld voor het melden van beveiligingsincidenten, zie hiertoe paragraaf 6.8 Afhandelen beveiligingsmeldingen.

C.12.9.1. Registreren en classificeren van incidenten

Beheersmaatregel
Incidenten worden systematisch geregistreerd, geclassificeerd op impact en urgentie, en geprioriteerd in overeenstemming met de afspraken over het dienstenniveau.

Implementatierichtlijnen
1. Voor alle typen incidenten is een formeel en bereikbaar loket ingesteld.
2. Alle incidenten worden centraal geregistreerd en van een unieke identificatie voorzien.
3. Er zijn criteria bepaald voor het classificeren (bepalen soort, impact, urgentie en prioriteit) en registreren (standaard coderingen, verplichte attributen) van incidenten. Deze criteria sluiten aan bij de criteria en opdrachttypen (bijv. incidentele bestandsingrepen) die in Dienstverleningsovereenkomsten zijn vastgelegd. Hierbij is aandacht besteed aan:
a. incidenten die voortvloeien uit meldingen van gebruikers;
b. incidenten die het gevolg zijn van automatisch door monitoringsystemen gegenereerde gebeurtenissen (events);
c. reguliere en niet-reguliere beveiligingsincidenten
4. Verstoringen met overeenkomstige oorzaken (known errors) kunnen als zodanig herkend worden ter ondersteuning van een efficiënte afhandeling.
5. De prioriteit die aan incidenten wordt toegekend, is afhankelijk van de consequenties voor de overeengekomen dienstverlening, waaronder:
a. gevaar voor de beschikbaarheid van de informatiesystemen;
b. gevaar voor betrouwbaarheid of exclusiviteit van gegevenstransmissie;
c. gevaar voor continuïteit van de gegevensverwerking;
d. het aantal gedupeerde gebruikers;
e. het karakter van de taak van de gedupeerde gebruikers;
f. het afgesproken niveau van dienstverlening.
6. De gegevens van configuratiebeheer kunnen worden geraadpleegd om onderhoudsverplichtingen van leveranciers of dienstverleners voor betreffende faciliteiten vast te stellen en op grond hiervan desgewenst het verhelpen van de verstoring aan deze derden toe te wijzen.
7. Elk incident, dat niet onmiddellijk bij aanmelding kan worden opgelost, wordt aan een oplosgroep toegewezen.

C.12.9.2. Oplossen en herstel incidenten

Beheersmaatregel
Geregistreerde incidenten worden afgehandeld door oplosgroepen.

Implementatierichtlijnen
1. Van elke oplosgroep zijn de verantwoordelijkheden (aandachtsgebied) en bevoegdheden (o.a. mogelijkheden voor inschakelen leveranciersondersteuning) bepaald.
2. Voor het afhandelen van urgente en niet-standaard beveiligingsincidenten (bijv. bij computervirusinfecties en aanvallen via internet) fungeert een aparte oplosgroep, een CERT (= Computer Emergency Response Team) met vertegenwoordiging uit Security Management.
3. De beschikbaarheid en bereikbaarheid van oplosgroepen zijn geborgd. Hierbij wordt speciale aandacht geschonken aan de beschikbaarheid en bereikbaarheid buiten kantooruren (stand-by diensten).
4. Oplosgroepen beschikken over informatie over known errors en beschikbare work-arounds.
5. Er worden gekwalificeerde bronnen gebruikt om onderscheid te maken tussen vals virusalarm en werkelijke virussen, wormen, Trojaanse paarden en andere malware.
6. Bij het overnemen van clients door beheerders om te kunnen meekijken op het werkstation wordt altijd eerst toestemming aan de gebruiker gevraagd.
7. Buiten het reguliere problem- en changeproces om aangebrachte noodwijzigingen als gevolg van incidenten met een bijzonder (urgent) karakter doorlopen achteraf alsnog de gebruikelijke procedures. In het proces zijn hiervoor de waarborgen geschapen.
8. Oplosgroepen registreren de voor de afhandeling van incidenten uitgevoerde werkzaamheden (wie heeft wat wanneer gedaan).

C.12.9.3. Bewaken en afsluiten incidenten

Beheersmaatregel
De voortgang van het oplossen van incidenten wordt bewaakt.

Implementatierichtlijnen
1. De doorlooptijd van incidenten wordt bewaakt. De verantwoordelijkheid daarvoor is eenduidig in de organisatie belegd.
2. De incidentregistratie biedt voldoende mogelijkheden om overschrijding van de afgesproken

doorlooptijden te signaleren.
3. Er zijn escalatieprocedures vastgelegd voor incidenten die niet binnen de geldende normtijden kunnen worden opgelost. Hierbij is expliciet aandacht besteed aan criteria voor het onderkennen van (potentiële) calamiteiten die aan het proces 2.6 Tactisch Beveiligingsbeheer worden doorgespeeld.
4. Incidenten worden pas afgesloten nadat is vastgesteld dat alle vereiste gegevens zijn ingevuld en is geverifieerd dat het daadwerkelijk het gewenste resultaat is bereikt. Het afsluiten van een incident wordt onafhankelijk van de probleemoplossing geregistreerd.

C.12.10. Problem Management

Doelstelling
Problem Management draagt zorg voor het wegnemen of voorkomen van structurele fouten in de IT-dienstverlening.

Toelichting
Door de structurele fouten in de IT-dienstverlening te minimaliseren draagt Problem Management ertoe bij het aantal en de impact van potentiële incidenten te verminderen. Het proces van Problem Management tracht dit doel te bereiken door het pro-actief en reactief identificeren van oorzaken van (potentiële) incidenten en problemen en door het beheersen van bekende fouten tot ze zijn opgelost. Voor het oplossen van gevonden oorzaken en bekende fouten zal Problem Management een wijzigingsverzoek indienen via het proces 12.6 Change Management.

Motivering
Het proces zorgt ervoor dat de structurele oorzaak van incidenten wordt opgespoord en weggenomen en is daarmee van belang om (toekomstige) storingen te voorkomen. Hiermee wordt de beschikbaarheid en integriteit van IT-dienstverlening bevorderd.

Afbakening
Het proces beperkt zich uitsluitend tot regelmatig terugkerende incidenten die om een structurele oplossing vragen. Deze incidenten worden geselecteerd uit de registratie van incidenten binnen het proces 12.9 Incident Management.

C.12.10.1. Signaleren problemen

Beheersmaatregel
Problemen worden zowel reactief als pro-actief opgespoord en geregistreerd.

Implementatierichtlijnen
1. Incidenten worden systematisch geanalyseerd ter signalering van problemen (reactief).
2. Externe bronnen (leveranciers, gebruikersgroepen, conferenties) worden systematisch geraadpleegd ter signalering van problemen (pro-actief).
3. Gesignaleerde problemen worden tijdig geregistreerd.
4. Vanuit het changemanagementproces wordt informatie ontvangen en geregistreerd over known errors van te implementeren wijzigingen (met name al bekende fouten van nieuwe diensten).

C.12.10.2. Plannen probleemoplossing

Beheersmaatregel
Problemen worden geprioriteerd en toegewezen aan oplosgroepen, die over voldoende capaciteit beschikken.

Implementatierichtlijnen
1. Er zijn criteria vastgelegd voor classificeren van problemen (bepalen impact, urgentie en escalatietijd).
2. Er is voldoende informatie voor de identificatie van de juiste personen voor toewijzing aan de uitvoerende instanties ter onderzoek en diagnose inclusief de identificatie van de onderhoudsverplichtingen van leveranciers.
3. Er is voldoende tijd en capaciteit beschikbaar voor het opsporen en wegnemen van de structurele oorzaken van incidenten.
4. De bevoegdheden en procedures voor het claimen van capaciteit (tweede en derdelijns) voor probleemanalyse en probleemoplossing zijn vastgelegd.

C.12.10.3. Oplossen problemen

Beheersmaatregel
Onderkende problemen worden gestructureerd opgelost.

Implementatierichtlijnen
1. Er is vastgelegd wie en in welke situaties (bij welke klasse van problemen) bevoegd is om vanuit het Problem Management-proces een spoedeisende wijziging te initiëren.
2. Alle incidenten die het gevolg zijn van een bepaald probleem worden als zodanig herkend en gezamenlijk onderzocht en opgelost.
3. Indien de oorzaak van een probleem is bepaald, wordt deze als “known error” geregistreerd, waarbij oorzaken en oplossingen, inclusief een motivatie voor de oplossing wordt vastgelegd.
4. Bij het wegnemen van structurele oorzaken van problemen (known errors) wordt een relatie gelegd met incidenten, de betrokken Configuratie Items en het wijzigingsverzoek waarmee de oorzaak wordt weggenomen.
5. Als een work-around bestaat uit het tijdelijk opheffen of versoepelen van beveiligingsmaatregelen, wordt deze op basis van advies door tactisch beveiligingsbeheer door het management goedgekeurd.

C.12.10.4. Bewaken en afsluiten

Beheersmaatregel
Er wordt voortgangsbewaking uitgeoefend op de diagnose en oplossing van problemen.

Implementatierichtlijnen
1. Prioriteren en voortgangsbewaking van problemen zijn functioneel gescheiden van de oplosgroepen.
2. Voor afsluiten van een probleem wordt, onafhankelijk van de uitvoering, vastgesteld of het probleem is verholpen.
3. Afgesloten incidenten, die niet gekoppeld konden worden aan ‘known errors’, worden periodiek beoordeeld.

C.12.11. Event Management

Doelstelling
Event Management draagt zorg voor het analyseren, beoordelen en zonodig ondernemen van acties als gevolg van automatisch gemelde gebeurtenissen in de IT-verwerking.

Toelichting
Onder een event wordt verstaan elke gebeurtenis, die een vooraf ingestelde drempelwaarde overschrijdt. Events worden gecategoriseerd op belangrijkheid en zijn als volgt te onderscheiden:
- een informatief event: Dit is een event die geen actie vereist en geen uitzondering vertegenwoordigt (bijvoorbeeld het inloggen van een gebruiker). Informatieve events worden meestal voor een bepaalde tijd opgeslagen in een logbestand.
- een alert event: Dit is een event een aangewezen persoon, proces of tool gewaarschuwd wordt, zodat de juiste actie kan worden ondernomen.
- een exception event: een event waaruit blijkt dat een IT-dienst of IT-voorziening zich abnormaal gedraagt, of dat de SLA niet wordt gehaald en het bedrijfsproces in gevaar komt.

Motivering
Het proces zorgt ervoor dat te voorziene verstoringen in de werking van IT-diensten en IT-voorzieningen kunnen worden voorkomen door het tijdig attenderen van degene (persoon of proces) die een standaard oplossingshandeling moet verrichten. Security violations worden eveneens tot events gerekend. Daarmee heeft dit proces betekenis voor alle aspecten van beveiliging.

Afbakening
Het proces handelt een voorgedefinieerde categorie van verstoringsmogelijkheden af en geeft deze aan 12.9 Incident Management af als ze niet direct kunnen worden opgelost. Het proces gaat ervan uit dat bij het ontwerpen en ontwikkelen van IT-diensten en –voorzieningen, de soorten events en hun afhandeling tevoren uitgewerkt worden.

C.12.11.1. Opsporen events

Beheersmaatregel
Uit de logging van de productieverwerking wordt op basis van drempelwaarden bepaald of er sprake is van events die informatief zijn of om verdere actie vragen.

Implementatierichtlijnen
1. Voor elke logging producerende IT-voorziening worden drempelwaarden (o.a. voor capaciteit of onbeschikbaarheid) vastgesteld en onderhouden, die in de desbetreffende IT-voorzieningen events afgeven als de drempelwaarden wordt overschreden. (Code 10.3.1)
2. Op basis van een filtermechanisme wordt bepaald of een event aan een centraal management tool wordt doorgegeven. Zo niet vindt logging plaats.

C.12.11.2. Analyseren en afhandelen events

Beheersmaatregel
Af te handelen events worden geanalyseerd en afgehandeld.

Implementatierichtlijnen
1. Op basis van categorisatie en correlatie wordt de betekenis van de events bepaald en vastgesteld welk soort actie moet worden ondernomen of een incident wordt aangemaakt.
2. De events worden gecontroleerd op afhandeling.
3. Op basis van analyse worden vervolgacties uitgezet, bijvoorbeeld een verzoek tot wijziging of een probleemsuggestie.
4. De doorlooptijd van afhandeling van events wordt bewaakt. De verantwoordelijkheid daarvoor is eenduidig in de organisatie belegd.
5. Bij overschrijding van afhandelingstermijnen wordt een incident aangemaakt.
6. Events worden pas afgesloten nadat is vastgesteld dat de oorzaak is verholpen.

C.12.12. Operations management

Doelstelling
Operations Management draagt zorg voor het operationeel houden en bewaken van de IT-voorzieningen, waaronder opslagmedia voor data, en voor het planmatig uitvoeren van incidentele en periodieke productieopdrachten.

Toelichting
De doelen van Operations Management zijn:
productieopdrachten uitvoeren ten behoeve van belanghebbenden;
het bewaken en controleren van de werking van IT-voorzieningen en de productieverwerking;
het registreren en beheren van verwijderbare opslagmedia.
Productieopdrachten kunnen worden onderverdeeld in incidentele en periodieke / structurele productieopdrachten. Bij de uitvoering van incidentele productieopdrachten dienen opdrachten te worden geautoriseerd en geaccepteerd. De verwerking van periodieke productieopdrachten heeft, na de initiële acceptatie van de opdracht, het karakter van een bewakingsproces.
Bij de bewaking van de IT-voorzieningen en productieverwerking worden, zo mogelijk via Event Management signalen uit de IT-voorzieningen afgehandeld en worden de IT-voorzieningen bediend, zodat ze voortdurend beschikbaar blijven.

Motivering
Het aantal en de verscheidenheid van activiteiten die tot het Operationsproces worden gerekend zijn groot. De integriteit van de technische verwerking en beschikbaarstelling van gegevens, de veilige opslag van gegevens, de zorg dat gegevens alleen toegankelijk zijn voor personen en processen, die in het systeem van logische toegangsbeveiliging zijn opgenomen en het testen van continuïteitsvoorzieningen zijn voorbeelden van het belang van dit proces voor beveiliging.

C.12.12.1. Voorbereiden productie

Beheersmaatregel
Productie-opdrachten worden gecontroleerd en gepland.

Implementatierichtlijnen
1. Productieopdrachten met een herhalingskarakter worden per periode gepland t.o.v. de beschikbare resources, rekening houdend met incidentele opdrachten en onderhoudswerkzaamheden.
2. Incidentele opdrachten worden bij ontvangst beoordeeld t.o.v. de beschikbaarheid van resources en in de planning opgenomen.
3. Bij de acceptatie van een productie-opdracht wordt gecontroleerd of:
a. er wordt voldaan aan de exploitatiecriteria;
b. er met goed gevolg acceptatietesten hebben plaatsgevonden;
c. de acceptatietestomgeving zoveel mogelijk overeenkomt met de productie-omgeving. (Code 10.1.4.d)
4. Het gebruik van algemene vraagtalen e.d. is zodanig aan voorwaarden gebonden dat deze IT-voorzieningen nimmer de verwerking door en het gebruik van reguliere informatiesystemen kunnen verstoren, dan wel inbreuk doen op de eisen van de logische toegangsbeveiliging.

C.12.12.2. Uitvoeren en bewaken productie algemeen

Beheersmaatregel
De uitvoering van de productie-opdrachten wordt bewaakt en gecontroleerd.

Implementatierichtlijnen
1. Van de exploitatieplanning wordt een registratie bijgehouden, aan de hand waarvan de voortgang van de planning wordt bewaakt.
2. De afhandeling van fouten en andere uitzonderlijke situaties die zich tijdens de uitvoering van de taak kunnen voordoen, waaronder beperkingen in het gebruik van systeemhulpmiddelen, geschiedt volgens instructie. (Code 10.1.1.d)
3. De resultaten van de uitgevoerde productieopdrachten worden teruggemeld aan de Loketfunctie resp. opdrachtgever.
4. Door systemen en klanten gerapporteerde storingen worden beoordeeld op afhandeling om te waarborgen dat de storingen genoegzaam zijn opgelost en om te beoordelen of de corrigerende maatregelen niet hebben geleid tot het compromitteren van de beheersmaatregelen en of de genomen acties volledig zijn geautoriseerd. (Code 10.10.5) N.B. Let op mogelijke samenhang met Event en Incident Management.
5. Operators handelen in overeenstemming met de volgende instructies: (Code 10.1.1.a)
a. bekendheid met de randvoorwaarden voor het gebruik van systeemhulpmiddelen;
b. bijhouden van het logboek van uitgevoerde werkzaamheden i.v.m. problemen met informatieverwerking- of communicatiesystemen met aanduiding wie de werkzaamheden heeft uitgevoerd; (Code 10.10.5)
c. maken van back-ups; (Code 10.1.1.b)
d. bekendheid met de namen van contactpersonen in geval van onverwachte bedieningsmoeilijkheden of technische storingen; (Code 10.1.1.e)
e. procedures voor het afsluiten, opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen; (Code 10.1.1.g)
f. veiligstellen van logging. (Code 10.1.1.h)

C.12.12.3. Integriteit verwerking

Beheersmaatregel
Er worden preventieve maatregelen getroffen om de integriteit van de productieverwerking in het algemeen te borgen.

Implementatierichtlijnen
1. Met de klanten worden tijdsblokken afgesproken voor het uitvoeren van onderhoud aan IT-voorzieningen (geplande downtime).
2. De beheersprocedures en verantwoordelijkheden bij het omgaan met virusbescherming op clients en servers zijn geregeld evenals training in het gebruik ervan, rapportage en herstel van virusaanvallen.
3. De werking van voorzieningen die apparatuur beveiligt tegen stroomstoringen en andere elektrische storingen worden regelmatig getest.
4. Voor het gebruik van diagnosepoorten op afstand gelden aparte procedures om ervoor te zorgen dat alleen toegang kan worden verkregen na overleg tussen de manager van Operations en het onderhoudspersoneel dat toegang tot de apparatuur of programmatuur wenst. (Code 11.4.4)
5. Er zijn speciale voorzieningen en instructies voor het uitvoeren van bedienings- en monitoringsactiviteiten

vanuit externe locaties (bijvoorbeeld als buiten kantooruren vanuit huis wordt gewerkt). Deze voorzieningen en instructies zijn afgestemd op de extra risico´s die hiermee gepaard kunnen gaan.
6. Periodiek wordt de integriteit van de onderlinge verwijzingen tussen indexen van bestanden, directory's, tabellen vastgesteld.
7. Periodiek vindt er enige vorm van integriteitscontrole (bijv. d.m.v. checksums) plaats op essentiële systeemprogrammatuur, toepassingsprogrammatuur en configuratiebestanden.

C.12.12.4. Behandelen output

Beheersmaatregel
Aan de beveiliging van de printoutput wordt speciale zorg besteed.

Implementatierichtlijnen
1. Operators beschikken over instructies voor de behandeling van speciale computeroutput, zoals het gebruik van speciaal papier of het beheer van vertrouwelijke uitvoergegevens, inclusief procedures voor een veilige afvoer van mislukte printopdrachten. (Code 10.1.1.f)
2. Bij het afdrukken en nabewerken van bescheiden worden steekproefsgewijze nagegaan dat de bescheiden voldoen aan kwaliteitseisen van leesbaarheid.
3. Papierafval (zoals uitval en onjuiste uitvoer) wordt tijdig afgevoerd naar een (brand)veilige plaats.

C.12.12.5. Maken back-ups

Beheersmaatregel
Er worden back-upkopieën van informatie en programmatuur gemaakt om in continuïteit over de productiegegevens te kunnen beschikken.

Implementatierichtlijnen (Code 10.5.1)
1. Het noodzakelijke niveau van back-upinformatie is gedefinieerd.
2. Er worden registers van back-upkopieën en gedocumenteerde herstelprocedures bijgehouden.
3. De omvang (bijvoorbeeld volledige back-up of alleen van de wijzigingen) en frequentie van back-ups is in overeenstemming met de afspraken over beschikbaarheid in de dienstverleningsovereenkomsten.
4. De back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als zich een calamiteit voordoet op de hoofdlocatie. (Code 9.1.4.b)
5. De beheersmaatregelen voor media op de hoofdlocatie gelden ook voor de back-uplocatie.
6. Back-ups worden regelmatig getest, om te waarborgen dat ze betrouwbaar zijn en in geval van nood kunnen worden gebruikt.
7. Herstelprocedures worden regelmatig gecontroleerd en getest, om te waarborgen dat ze doeltreffend zijn en dat ze kunnen worden uitgevoerd binnen de daarvoor volgens operationele herstelprocedures gestelde tijd.
8. In bijzondere gevallen waar vertrouwelijkheid van extra belang is, zoals bij systeemsoftwarebestanden, worden back-ups beschermd door middel van encryptie.
9. Back-ups worden niet voor andere doeleinden gebruikt, dan het restoren (of testen daarvan) voor reguliere productiedoeleinden.
10. Jaarlijks, of na belangrijke wijzigingen wordt vastgesteld of alle daarvoor in aanmerking komende systeemprogrammatuur, applicaties, gegevensbestanden en documentatie in de back-upprocedures zijn betrokken.

C.12.12.6. Incidentele bestandsingrepen

Beheersmaatregel
Opdrachten voor het uitvoeren van incidentele bestandsingrepen worden als apart werkproces gezien en voldoet aan extra eisen van betrouwbaarheid.

Implementatierichtlijnen
1. Alleen medewerkers die daarvoor door het bevoegde management zijn aangewezen, mogen incidentele bestandsingrepen uitvoeren.
2. Er wordt gebruik gemaakt van automatisch werkende voorzieningen om rapportages te genereren van de oude en nieuwe situatie bij het doen van bestandsingrepen. Kopieën van deze rapportages worden buiten de beïnvloedingssfeer van uitvoerende medewerkers naar aangewezen (controle)medewerkers van de klantorganisatie gestuurd, niet zijnde de opdrachtgever.

3. Het doen van incidentele bestandsingrepen wordt als incident aangemerkt en apart gerapporteerd in de dienstverleningsrapportages.
4. Jaarlijks wordt aan de klantorganisatie verzocht te bevestigen welke medewerkers als opdrachtgever en ontvanger van terugmeldingen namens de klantorganisatie optreden.

C.12.12.7. Leveren van gegevens buiten overeengekomen productiedoeleinden.

Beheersmaatregel
Productiegegevens met vertrouwelijke gegevens worden niet gebruikt buiten de door exploitatie beheerde omgevingen tenzij extra beveiligingsmaatregelen worden getroffen.

Implementatierichtlijnen
(Privacy-)gevoelige productiegegevens voor testen (Code 10.1.4.f)
1. Indien kopieën van productiegegevens voor testdoeleinden noodzakelijk worden geacht, wordt gecontroleerd of de functioneel beheerder van de data schriftelijke toestemming heeft gegeven.
2. De tot personen herleidbare gegevens worden geanonimiseerd (dus ook geen bestaande sleutelgegevens gebruiken);
3. Indien implementatierichtlijn 12.12.7.2 niet mogelijk is, wordt uitgegaan van een productieregiem, bestaande uit de volgende maatregelen:
a. de privacybepalende gegevens in de kopieën van de productiedata worden volgens een onvoorspelbaar patroon verschoven en als testgegevens herkenbaar gemaakt;
b. kopieën van productiedata worden uitsluitend in de acceptatietestomgeving ter beschikking gesteld;
c. de autorisaties voor het ontsluiten van de productiegegevens in de acceptatietestomgeving worden per test aan een zeer beperkte groep medewerkers toegekend. De toegangsrechten worden gedocumenteerd en gearchiveerd;
d. testoutput mag niet de productieruimten verlaten;
e. alle bestanden met (privacy-)gevoelige productiegegevens worden na gebruik gewist;
f. testoutput wordt door een aangewezen productiebeheerder gedurende een afgesproken periode in afgesloten kasten bewaard voor eventuele naslag, waarna de output wordt vernietigd.

Leveren productiegegevens aan derden
3. Voor het leveren van (kopieën van) productiedata aan andere bestemmingen dan die in de reguliere productie zijn gedocumenteerd, wordt gecontroleerd of de functioneel beheerder dan wel manager van de desbetreffende gebruikersafdeling toestemming heeft verleend. Dergelijke opdrachten worden gemeld aan tactisch beveiligingsbeheer.

Onderzoek van systeem(loggings)bestanden
4. Logging en events die privacygevoelige data bevatten, worden alleen via een speciale procedure ter beschikking gesteld voor onderzoek na goedkeuring van het hoogste klantmanagement en toezicht door de daartoe aangewezen beveiligingsfunctionaris.
5. Logging en events die privacygevoelige data bevatten worden alleen voor onderzoek ontsloten door medewerkers die daartoe door het management zijn aangewezen en geïnstrueerd.

C.12.12.8. Beheer computer- en nabewerkingsruimten

Beheersmaatregel
Computer- en nabewerkingsruimten worden ordelijk beheerd.

Implementatierichtlijnen
1. Computerruimten zijn ingericht volgens de normen van paragraaf 7.10 Computerruimten.
2. Apparatuur wordt onderhouden volgens de door de leverancier aanbevolen voorschriften en dienstverlening-tijdstippen. (Code 9.2.4.a)
3. Reparatie en onderhoud van apparatuur wordt alleen uitgevoerd door bevoegd onderhoudspersoneel. (Code 9.2.4.b, 9.1.2.d)
4. Onderhoud, reparaties en storingen worden geregistreerd. (Code 9.2.4.c)
5. Huisregels voorkomen eten, drinken en roken in de nabijheid van IT-apparatuur. (Code 9.2.1.e)
6. Voor het geven van rondleidingen wordt een terughoudend beleid gevoerd.
7. Ongeautoriseerd personeel wordt altijd begeleid door eigen medewerkers, die bevoegd zijn om in de computer- en nabewerkingsruimten te komen.
8. Begeleiders van bezoekers zien expliciet toe op het niet aanwezig zijn van fotografische, video-, audio- of

andere opnameapparatuur. (Code 9.1.5.d)
9. Leegstaande beveiligde ruimten worden fysiek afgesloten en periodiek gecontroleerd op leegstand.
10. Zonder toezicht werken in beveiligde ruimten wordt voorkomen, zowel om veiligheidsredenen als om de kans op kwaadwillige handelingen te voorkomen. Dit geldt temeer voor ondersteunende diensten.
11. Voor het buiten de beveiligde ruimte brengen van computersystemen is toestemming van de systeembeheerder nodig.
12. De werking van de fysieke beveiligingsmaatregelen (brandbeveiliging, beveiliging tegen blikseminslag en stroomstoringen) wordt regelmatig getest. In de testplannen zijn speciale maatregelen genomen om ongeplande onbeschikbaarheid als gevolg van testwerkzaamheden te voorkomen.
13. Uninterruptable Power Supplies en generatoren worden regelmatig gecontroleerd om te waarborgen dat ze voldoende capaciteit hebben en worden volgens de voorschriften van de fabrikant getest.

C.12.12.9. Bestandsbeheer

Beheersmaatregel
Bestanden worden ordelijk beheerd.

Implementatierichtlijnen
1. Bestanden worden per platform op basis van een naamgevingsconventie gegroepeerd per toepassingsgebied of organisatiedeel.
2. Voor elke groep bestanden (directory) is een functioneel beheerder aangewezen.
3. Bestanden worden bewaard volgens overeengekomen bewaartermijnen.
4. Logbestanden worden 2 jaar bewaard.

C.12.12.10. Beheer opslagmedia

Beheersmaatregel
Het beheer van opslagmedia voorkomt oneigenlijke ontsluiting van gegevens en garandeert de leesbaarheid van bestanden gedurende hun bewaartermijn.

Toelichting
Het registreren en beheren van de opslagmedia heeft grotendeels dezelfde kenmerken als het Asset and Configuration Management proces. Het doel is een betrouwbare registratie te onderhouden van de opslagmedia, zodat de bedrijfs- en IT-processen hier gebruik van kunnen maken voor dataopslag.
Tot de verwijderbare media worden gerekend: schijven, magneetbandhouders, flashgeheugenkaarten, losse harde schijven, CD's, DVD's en USB-sticks en dergelijke.

Implementatierichtlijnen
1. Alle media, die bedoeld zijn voor opslag van bestanden zijn uniek geïdentificeerd.
2. Alle media worden bewaard in een veilige en beveiligde omgeving, overeenkomstig de instructies van de fabrikant. (Code 10.7.1.c)
3. Alle fasen in de levenscyclus van opslagmedia worden met datumgegevens geregistreerd: ontvangst, locatie, in onderhoud, in transport, afgevoerd en door wie goedgekeurd. (Code 10.7.1.b) alleen afvoer, (Code 10.7.1.e) verwijderbare media)
4. Van alle opslagmedia is het einde van de technische levensduur bekend.
5. Er wordt bewaakt dat opslagmedia door geschikte apparatuur en programmatuur gelezen kunnen blijven worden gedurende de bewaartermijn van de opgeslagen bestanden. (Code 15.1.3.d)
6. Reparatie en onderhoud van apparatuur waarop zich gegevens bevinden, vindt op eigen locatie plaats, indien het niet mogelijk is gegevens vooraf te wissen dan wel de harde schijf te verwijderen. (Code 9.2.4.d)
7. Reparatie en onderhoud van apparatuur waarop zich gevoelige gegevens bevinden, vindt onder toezicht op eigen locatie plaats, indien het niet mogelijk is gegevens vooraf te wissen dan wel de harde schijf te verwijderen.
8. Bestanden worden veiliggesteld wanneer de levensduur van het betreffende opslagmedium ten einde is. (Code 10.7.1.d)
9. Bij afvoer van apparatuur worden alle onderdelen waarop gegevens kunnen worden opgeslagen, onherstelbaar gewist met speciale programmatuur dan wel gedemagnetiseerd met speciale apparatuur. (Code 9.2.6)
10. Van verwijderbare media die de organisatie verlaten of niet meer gebruikt worden, wordt de inhoud, als die niet meer nodig is, gewist (Code 10.7.1.a)
11. Opslagmedia en apparatuur, waarin zich opslagmedia bevinden, worden alleen afgevoerd na

goedkeuring en vernietigd door bedrijven, die hier hierin gespecialiseerd zijn en aantoonbare beveiligingsmaatregelen in acht nemen. (Code 9.2.6, 10.7.1.b)

C.12.12.11. Transporteren media

Beheersmaatregel
Het fysiek transport van bestanden voorkomt oneigenlijke ontsluiting of beïnvloeding van gegevens.

Implementatierichtlijnen
1. Het fysiek transporteren van bestanden naar derden is gebaseerd op ondertekende overeenkomsten inzake gegevensuitwisseling. (Code 10.7.1.b) goedkeuring)
2. De ontvangst en verzending van transportmedia wordt geregistreerd.
3. Geborgd is dat transportmedia voor interne doeleinden (bijv. ten behoeve van de uitwijk), daadwerkelijk tijdig en ongewijzigd in de andere opslaglocatie aankomen.
4. Bij het vervoer van transportmedia wordt gebruik gemaakt van aantoonbaar betrouwbare en door het management goedgekeurde transport- of koeriersdiensten. (Code 10.8.3.a, 10.8.3.b)
5. Bij het vervoer van transportmedia wordt ervoor zorggedragen dat:
a. de verpakking in overeenstemming is met de specificaties van de mediafabrikant en er afdoende bescherming is tegen fysieke schade tijdens het transport; (Code 10.8.3.d)
b. er extra maatregelen worden getroffen bij gevoelige informatie, zoals gebruik afgesloten containers; persoonlijk afleveren, verpakkingsmateriaal gebruiken waaraan manipulatie direct te zien is, opsplitsen verzending en onderdelen apart verzenden. (Code 10.8.3.e)
c. de identificatie van de koerier wordt gecontroleerd. (Code 10.8.3.c)
6. De te transporteren bestanden zijn te identificeren en gespecificeerd t.a.v. de inhoud en het overdrachtsmoment.
7. Overdacht van transportmedia geschiedt tegen kwijting.
8. Ontvangst van transportmedia op bestemming wordt bevestigd.

C.12.12.12. Remote support door externe partijen

Beheersmaatregel
Remote support kan de betrouwbare verwerking niet verstoren.

Implementatierichtlijnen
1. Ten behoeve van remote support worden alleen de verbindingen en toegangsroute gebruikt, die expliciet voor dit doel zijn aangewezen.
2. Indien het remote support betrekking heeft op het uitvoeren van beheerhandelingen (dus verder gaat dan remote diagnosis), wordt door eigen medewerkers - voor zover mogelijk - meegekeken.
3. Aan de hand van de logging worden de beheerhandelingen expliciet getoetst en in verband gebracht met een aanleiding of oorzaak voor het ingrijpen.

C.12.12.13. Remote beheer

Beheersmaatregel
Remote beheer kan de betrouwbare verwerking niet verstoren.

Implementatierichtlijnen (Code 10.6.1.b)
1) Er is functiescheiding tussen het gebruik en het beheer van de remote beheervoorziening.
2) Ten behoeve van remote beheer worden alleen de verbindingen en toegangsroute gebruikt, die expliciet voor dit doel zijn aangewezen.
3) Authenticatie van beheerders die op afstand beheer uitvoeren vindt plaats op basis van kennis en bezit.
4) De tijd op de remote beheervoorziening wordt gesynchroniseerd met de tijd van de technische infrastructuur waarop zich de op afstand te beheren IT-voorzieningen bevinden.
5) De handelingen die op de remote beheervoorziening plaatsvinden, wordt volledig gelogd.

C.13. Leveren huisvesting

C.13.1. Inleiding

Doelstelling
Leveren huisvesting stelt op basis van klantafspraken huisvestingsvoorzieningen beschikbaar en houdt deze in stand, waarmee voldaan wordt aan de eisen van fysieke beveiliging.

Toelichting
De levering van huisvesting wordt normaliter (anders dan bij het leveren van IT) in belangrijke mate bepaald door concernafspraken en standaards zodat overige afspraken met de klant slechts voor een gering deel bepaald worden door specifieke klantprocessen.

Motivering
Het leveren van huisvesting impliceert het treffen van maatregelen van fysieke beveiliging.

Afbakening
Het voldoen aan eisen van fysieke beveiliging wordt in dit normenkader alleen herkenbaar ingevuld bij het leveren van huisvesting. Bij de klantorganisatie komen deze eisen slechts impliciet aan de orde bij het proces personeelsbeheer t.b.v. het aanvragen van fysieke toegangsrechten. Voorts komt het voldoen aan de eisen van fysieke beveiliging voor zowel leverancier- en klantorganisatie aan de orde bij het sluiten van dienstovereenkomsten via de processen leveranciers- en afnemersbeheer.

C.13.2. Functiescheiding

Beheersmaatregel
Er is functiescheiding tussen facilitaire managers verantwoordelijk voor dienstverlenende processen, gebouwen- en installatiebeheerders en beveiligings- en controlefunctionarissen.

Geen implementatierichtlijn.

C.13.3. Ontwikkelen en verbouwen gebouwen en installaties

Doelstelling
Het proces voor het nieuw bouwen of verbouwen van gebouwen en installaties waarborgt de zorgvuldige besluitvorming over het voldoen aan eisen van fysieke beveiliging.

Motivering
Het achteraf aanbrengen of verbeteren van fysieke beveiligingsvoorzieningen is kostbaar. Indien er gelijk van de ontwerpfase van gebouwen en installaties rekening wordt gehouden met eisen van fysieke beveiliging kunnen deze als een integraal aspect worden meegenomen.

C.13.3.1. Besturen bouwproces

Beheersmaatregel
Er is een zorgvuldig bestuurlijk proces voor het geven van opdrachten voor het ontwerpen en realiseren van gebouwen en installaties.

Implementatierichtlijnen
1. Er zijn criteria vastgesteld op grond waarvan voor de besturing van grotere opdrachten een aparte projectorganisatie wordt ingesteld.
2. Ingeval een aparte projectorganisatie noodzakelijk wordt geacht, wordt een stuur of projectgroep ingesteld met vertegenwoordigers vanuit alle belanghebbende (in- en externe) partijen met voldoende mandaat om over de inhoud en voortgang te beslissen.
3. De werkzaamheden die worden uitbesteed aan derden met betrekking tot ontwerp, realisatie en plaatsing geschieden via de RGD of door partijen waarvan de bedrijfsvoering is erkend door een belanghebbende brancheverenigingen.

C.13.3.2. Vaststellen eisen fysieke beveiliging

Beheersmaatregel
De eisen van fysieke beveiliging worden vastgesteld en in de opdracht voor ontwerp en realisatie meegenomen.

Implementatierichtlijnen
1. De eisen voor fysieke beveiliging komen overeen met de normen van hoofdstuk 17 Gebouwen en installaties.
2. Voor het vaststellen van de eisen voor de specifieke situatie wordt een omgevingsanalyse uitgevoerd. Op basis hiervan en de analyses van opdrachtgever wordt in overleg bepaald in hoeverre de maatregelen van het basisniveau beveiliging voldoende zijn of dat de locatie door omstandigheden (op onderdelen) een hoger risicoprofiel kent. (Code 9.1.1.a)
3. Bij het betrekken van nieuwe gebouwen wordt een locatie gekozen in een omgeving waar de kans op natuurrampen en door mensen veroorzaakte rampen klein is
4. Er zijn criteria opgesteld op grond waarvan advies wordt ingewonnen van interne dan wel onafhankelijke externe fysieke beveiligingsadviseurs bij de ontwerpen.
5. In de projectietekeningen worden de technische beveiligingsmaatregelen vastgelegd, zoals deze mede naar aanleiding van het risicoprofiel zijn bepaald.

C.13.3.3. Controleren op uitvoering

Beheersmaatregel
De realisatie van de fysieke beveiliging vindt plaats conform de ontwerpeisen.

Implementatierichtlijnen
1. Het ontwerp, op grond waarvan bouw/installatie plaatsvindt, wordt goedgekeurd door hiervoor aangewezen in- en externe belanghebbenden.
2. De realisatie van de voorzieningen voor fysieke beveiliging wordt goedgekeurd door de beheerders van gebouwen en installaties dan wel door onafhankelijke technisch specialisten of de klant indien deze voldoende deskundig is (bijv. medewerkers van Exploitatie en technisch beheer IT).
3. De besluitvorming over voortgang en acceptatie van ontwerpen en opgeleverde gebouwen en installaties vindt – indien er geen projectorganisatie is ingesteld - op voldoende hoog managementniveau plaats.
4. Het (overdrachts)protocol wordt door alle belanghebbende partijen ondertekend.

C.13.4. Technisch beheer gebouwen en installaties

Beheersmaatregel
Alle zones, ruimten, leidingwegen, kabels, patch- en andere vaste kasten en installaties en apparatuur (hierna fysieke beveiligingsmiddelen genoemd) en hun documentatie worden juist en volledig geïdentificeerd, gedocumenteerd en met locatiegegevens vastgelegd.

Implementatierichtlijnen
1. Voor alle bedrijfsmiddelen zijn functionele beheerders aangewezen.
2. Alle fysieke beveiligingsmiddelen worden uniek geïdentificeerd, van een uniek herkenningsteken voorzien en centraal met een beschrijving en documentatie geregistreerd.
3. Van alle fysiek beveiligingsmiddelen is actuele documentatie aanwezig: technische en bedieningsdocumentatie, plattegronden en configuratieschema's.
4. Nieuwe, te wijzigen en te verwijderen fysieke beveiligingsmiddelen worden geïdentificeerd en geregistreerd.
5. Van alle daarvoor in aanmerking komende bedrijfsmiddelen wordt vastgesteld dat zij voldoen aan de Arbo-eisen (Code 9.1.3.a)
6. Bij een voorgenomen wijziging, eventuele afbraak en/of afstoting wordt eerst gecontroleerd of er geen nadelige effecten zijn op het niveau van beveiliging, d.w.z. tijdens het doorvoeren van de verandering en na afloop daarvan.
7. Periodiek wordt geverifieerd of de vastlegging van fysieke beveiligingsmiddelen overeenkomt met de werkelijkheid en worden verschillen geanalyseerd.
8. Bedienend personeel wordt actief op de hoogte gebracht waar bedienings- en beheerinstructies te vinden zijn.
9. Bedienings- en beheerinstructies worden periodiek geactualiseerd; in geval van afhankelijkheid van

derden zijn daarover afspraken gemaakt.
10. In geval van kritieke installaties worden beheer- en bedieningsinstructies opgeborgen in afgesloten kasten.
11. In geval van kritieke installaties worden beheer en bedieningsactiviteiten periodiek onafhankelijk van de uitvoering gecontroleerd.

C.13.5. Onderhoud gebouwen en installaties

Beheersmaatregel
De fysieke beveiligingsmiddelen worden zodanig onderhouden dat ze blijven voldoen aan de normen voor gebouwen en installaties.

Implementatierichtlijnen
1. De werkzaamheden die worden uitbesteed aan derden met betrekking tot onderhoud en salvage geschieden via de RGD of door partijen waarvan de bedrijfsvoering is erkend door een belanghebbende brancheverenigingen.
2. Voor alle gebouwen en gebouwgebonden installaties is een onderhouds- en servicecontract afgesloten, waarin is vastgelegd hoe gerapporteerd wordt over deze werkzaamheden.
3. De (onderhouds- en service)werkzaamheden aan gebouwen en/of installaties onderbreken, hinderen of verstoren zo min mogelijk het normale werkproces. De klant wordt zonodig tevoren geïnformeerd.
4. Reparatie en onderhoud van fysieke beveiligingsmiddelen worden alleen uitgevoerd door geautoriseerd onderhoudspersoneel.
5. Aan extern onderhoudspersoneel wordt beperkt toegang verleend tot kritische ruimten, waarop controle wordt uitgevoerd. (Code 9.1.2.d)
6. Onderhoud, reparaties en storingen worden geregistreerd.
7. Er wordt zorggedragen voor de blijvende geldigheid van een afgegeven gebruiksvergunning voor gebouwen.
8. De onderhouds- en wijzigingsprocedure voorziet in het tijdig actualiseren van de bouwkundige documentatie, inclusief de aangebrachte beveiligingsvoorzieningen en bewaring op locatie. Hiertoe worden periodiek contacten onderhouden met de klantorganisaties.
9. Het gebruik van alle aanwezige installaties is beschreven in daarvoor bedoelde handleidingen en is bekend bij de verantwoordelijke medewerkers.

C.13.6. Voorzorg gebouwen en installaties

Beheersmaatregel
Door middel van afspraken, toezicht en controle worden risico's op het doorbreken van de fysieke beveiliging zoveel mogelijk voorkomen.

Implementatierichtlijnen
1. Er zijn afspraken gemaakt met de plaatselijke brandweer (Code 6.1.6) over bluswatervoorzieningen en toegang tot het gebouw (aanvalsplan).
2. Gebouwen worden planmatig gecontroleerd op vormen van slijtage en schadevorming die van invloed zijn op het basis beveiligingsniveau.
3. De installaties wordt planmatig intern gecontroleerd op juiste werking. Afwijkingen worden aan de leiding gerapporteerd.
4. Afhankelijk van de zone waarin onderhouds- of schoonmaakwerkzaamheden plaatsvinden wordt toezicht uitgeoefend.

C.13.7. Toegangsdiensten

Beheersmaatregel
Er wordt toezicht uitgeoefend op de gecontroleerde toegang en vertrek van bezoekers en eigen personeel en zonodig bedrijfsmiddelen van de klantorganisatie en op gebouwen buiten de kantoortijden.

Implementatierichtlijnen
1. Alleen tevoren aangemelde bezoekers worden toegelaten tot beveiligde zones, waarbij erop wordt toegezien dat bezoekers door intern personeel worden opgehaald. (Code 9.1.1.c, 9.1.2.a)
2. Er wordt toezicht gehouden (eventueel via camerabewaking) op toegang door geautoriseerde medewerkers, opdat de toegangsbeveiliging niet omzeild wordt (bijv. meelopen).

3. Het op afstand bedienen van toegangen geschiedt onder duidelijke voorwaarden. (Code 9.1.6.a)
4. Bezorgingen buiten kantooruren zijn aan procedures gebonden.
5. Voor het verkrijgen van toegang tot een locatie met de sleutel en de kaart uit de beveiligde muurkluis, is een protocol opgesteld.
6. In overleg en/of opdracht van de klant kan controle worden uitgeoefend op de aanwezigheid van een verklaring, indien medewerkers ter beschikking gestelde bedrijfsmiddelen buiten het pand willen nemen.

C.13.8. Overige diensten fysieke beveiliging

Beheersmaatregel
Het verlenen van overige diensten op het gebied van fysieke beveiliging is gericht op algemene preventie.

Implementatierichtlijnen
1. Er is toezicht op het 's nachts gesloten zijn van nooddeuren en ramen. (Code 9.1.1.b)
2. Buiten de kantoortijd wordt alarmopvolging ingesteld ter voorkoming van schade en calamiteiten.
3. Voor het gebruik van camera's is een protocol opgesteld.
4. Camerabeelden van fysiek toezicht worden maximaal 72 uur bewaard en worden alleen afgegeven bij strafrechtelijk onderzoek en op verzoek van een opsporingsdienst (Politie, Justitie).
5. Leegstaande kritische ruimten worden periodiek gecontroleerd of zij gesloten zijn. (Code 9.1.5.c)
6. Gevaarlijke en brandbare materialen worden opgeslagen op veilige afstand van computerruimten. (Code 9.1.4.a)
7. Het verwijderen van papieren gegevensdragers geschiedt onder gecontroleerde omstandigheden:
 a. zorgvuldige selectie van verzamel- en verwijderdiensten, die aan te tonen beheersmaatregelen treffen om inzage van de afvoer te voorkomen en zorgdragen voor een zorgvuldige vernietigingsproces; (Code 10.7.2.c, 10.7.2.d)
b. gebruik van versnipperingsapparatuur voor gevoelige informatie (Code 10.7.2.a)
8. Periodiek wordt gecontroleerd of er overal vrij doorgang is t.b.v. ontruiming.
9. Voor het omgaan met verdachte brieven en pakketten is een protocol opgesteld.

C.13.9. Afhandelen incidentmeldingen fysieke beveiliging

Beheersmaatregel
Klachten en meldingen worden afgehandeld om (potentiële) verstoringen in de dienstverlening voor fysieke beveiliging te voorkomen of zo snel mogelijk op te lossen en om in voorkomende gevallen de veiligheid van aanwezige personen in het gebouw/de ruimte(n) te beschermen.

Implementatierichtlijnen
1. Alle soorten incidentmeldingen worden geregistreerd; beveiligingsincidenten (feitelijke inbreuk geconstateerd), beveiligingsvoorvallen (potentieel gevaar), agressie en geweld, bedreigingen, bedrijfsongevallen en meldingen van automatische alarmsystemen.
2. Voor het oplossen van incidenten zijn de verantwoordelijkheden (aandachtsgebieden) en bevoegdheden (o.a. voor inschakelen leveranciersondersteuning) bepaald.
3. Bij calamiteiten worden aanvullende maatregelen voor salvage genomen. Deze worden in samenwerking met specialisten (derden) bepaald.
4. Alle acties met betrekking tot de melding en afhandeling van incidenten wordt geregistreerd.
5. De doorlooptijd van incidentmeldingen wordt bewaakt.

C.13.10. Beschikbaarheid huisvesting

Beheersmaatregel
Er is in overleg met de klant een strategie ontwikkeld en geïmplementeerd om de gevolgen van het niet-beschikbaar zijn van huisvesting voor het uitoefenen van kritische bedrijfsactiviteiten van de afnemer te beperken.

Implementatierichtlijnen (BS 7.3)
1. De strategie om bij uitval van gebouwen of ruimten voor het uitvoeren van kritische bedrijfsactiviteiten over voldoende huisvesting te kunnen beschikken is gebaseerd op een analyse van de volgende uitgangspunten/overwegingen:
a. alternatieve huisvesting binnen de organisatie, inclusief het verplaatsen van andere activiteiten;
b. alternatieve huisvesting bij andere organisaties, eventueel wederzijds overeengekomen;

c. alternatieve huisvesting geleverd door hierin gespecialiseerde derden;
d. thuiswerken of op andere locaties;
e. gebruik van andere geschikte ruimten;
f. herverdelen van het werkaanbod naar andere vestigingen.

C.14. Diverse overeenkomsten

C.14.1. Inleiding

Doelstelling
Diverse overeenkomsten leggen de afspraken (contractueel) vast tussen leverancier en afnemer over:
informatie-uitwisseling met derden;
- verlenen aan derden van logische toegang tot bedrijfsinformatie;
- inhuur van derden;
- dienstverlening in het algemeen;
- ontwerp en/of bouw van applicaties;
- technisch beheer en exploitatie IT;
- aanschaf IT-voorzieningen.

Toelichting
De normen voor beveiliging in de soorten overeenkomsten van dit hoofdstuk zijn voor merendeel rechtstreeks ontleend aan de Code voor Informatiebeveiliging en niet geherformuleerd i.v.m. de herkenbaarheid voor derden.
In een overeenkomst kunnen meerdere van de hier onderscheiden soorten overeenkomsten van toepassing kunnen zijn.

C.14.2. Overeenkomsten informatie-uitwisseling

Beheersmaatregel
De overeenkomsten volgens het type: informatie-uitwisseling met derden voldoen aan zodanige eisen dat risico's op het gebied van beveiliging bij de tegenpartij/partner worden beheerst.

Implementatierichtlijnen

1. Eisen voor de geheimhouding inclusief een definitie van de informatie, die moet worden beschermd en de duur van de geheimhouding , ook na afloop van de overeenkomst volgens HBB, paragraaf 2.17 (Code 6.1.5.a, 6.1.5.b)
2. Voorwaarden en maatregelen om de teruggaaf of vernietiging van informatie en bedrijfsmiddelen aan het einde van, of op een overeengekomen punt tijdens de looptijd van het contract te waarborgen (Code 6.1.5.i)
3. Rapportage, kennisgeving en onderzoek naar gecompromitteerde bedrijfsmiddelen (bijvoorbeeld verlies of ongeoorloofde bekendmaking van gegevens) onjuistheden in informatie (bijvoorbeeld persoonsgegevens), verantwoordelijkheid en aansprakelijkheid in geval van informatiebeveiligingsincidenten en lekken in de beveiliging;(Code 6.1.5.h, 6.2.2.a, 6.2.2.e, 6.2.3.j, 10.8.2.g)
4. Een beschrijving van het product dat of de dienst die beschikbaar wordt gesteld, en een beschrijving van de informatie die moet worden verstrekt samen met de beveiligingsclassificatie (Code 6.2.2.b, 6.2.2.f, 6.2.3.k)
5. Voorwaarden voor heronderhandeling/beëindigen van overeenkomsten (Code 6.2.3.v)
6. Verantwoordelijkheden met betrekking tot beheersing en melding van doorgifte, verzending en ontvangst (Code 10.8.2.a)
7. Wijze van uitwisseling, kenmerken van het transportkanaal, technische specificaties van gegevens, de eisen die aan de uitwisseling (zowel elektronisch als fysiek: verpakking/verzending) worden gesteld; procedures voor kennisgeving aan de afzender van doorgifte, verzending en ontvangst (Code 10.8.2.b, 10.8.2.d)
8. Procedures voor het waarborgen van traceerbaarheid en onweerlegbaarheid (Code 10.8.2.c)
9. Identificatienormen voor de vervoerder (Code 10.8.2.f)
10. Identificatie van gerubriceerde gegevens, aanvullende beveiligingsmaatregelen, evt. beheersmaatregelen m.b.t. cryptografische sleutels.(Code 10.8.2.h, 10.8.2.k)
11. Retourneren of vernietigen van transportmedia
12. Ondertekening van overeenkomsten en onderliggende documenten door daartoe bevoegde vertegenwoordigers van de partijen

C.14.3. Overeenkomsten toegang derden

Beheersmaatregel

De overeenkomsten volgens het type: externen toegang verlenen tot informatie voldoen aan zodanige eisen dat risico's op het gebied van beveiliging bij de tegenpartij/partner worden beheerst.

Implementatierichtlijnen

1. Eisen voor de geheimhouding inclusief een definitie van de informatie, die moet worden beschermd en de duur van de geheimhouding , ook na afloop van de overeenkomst volgens HBB, paragraaf 2.17 (Code 6.1.5.a, 6.1.5.b)
2. Voorwaarden en maatregelen om de teruggaaf of vernietiging van informatie en bedrijfsmiddelen aan het einde van, of op een overeengekomen punt tijdens de looptijd van het contract te waarborgen (Code 6.1.5.i)
3. De IT-voorzieningen waartoe de externe partij toegang toe moet hebben (Code 6.2.1.a)
4. Het soort toegang dat de externe partij zal hebben tot de informatie en IT-voorzieningen, bijvoorbeeld: 1) fysieke toegang, zoals tot kantoren, computerruimten, archiefkasten; 2) logische toegang, zoals tot de databases of informatiesystemen van een organisatie; 3) netwerkverbindingen tussen de netwerken van de organisatie en de externe partij, zoals permanente verbinding, verbinding op afstand; 4) of de toegang op locatie of van buitenaf wordt verkregen (Code 6.2.1.b)
5. Het personeel van de externe partij dat is betrokken bij het verwerken van de informatie van de organisatie; (Code 6.2.1.e)
6. Hoe de organisatie of het personeel dat geautoriseerde toegang heeft kan worden vastgesteld, hoe de autorisatie kan worden geverifieerd en hoe vaak dit moet worden herbevestigd; (Code 6.2.1.f)
7. De verschillende middelen en beheersmaatregelen die door de externe partij worden gehanteerd bij het opslaan, verwerken, communiceren, delen en uitwisselen van informatie (Code 6.2.1.g)
8. De gevolgen van het ontbreken van toegang voor de externe partij wanneer dat is vereist en van het invoeren of ontvangen van onjuiste of misleidende informatie door de externe partij, inclusief het voorkomen van niet-geoorloofde bekendmaking van informatie. (Code 6.1.5.d, 6.2.1.h)
9. Werkvoorschriften en procedures om informatiebeveiligingsincidenten en potentiële schade af te handelen en de voorwaarden waaronder in geval van een informatiebeveiligingsincident de toegang voor de externe partij kan worden voortgezet (Code 6.2.1.i)
10. Rapportage, kennisgeving en onderzoek naar gecompromitteerde bedrijfsmiddelen (bijvoorbeeld verlies of ongeoorloofde bekendmaking van gegevens) onjuistheden in informatie (bijvoorbeeld persoonsgegevens), verantwoordelijkheid en aansprakelijkheid in geval van informatiebeveiligingsincidenten en lekken in de beveiliging; (Code 6.1.5.h, 6.2.2.a, 6.1.5.e, 6.2.3.j, 10.8.2.g)
11. Een beschrijving van het product dat of de dienst die beschikbaar wordt gesteld, en een beschrijving van de informatie die moet worden verstrekt samen met de beveiligingsclassificatie (Code 6.2.2.b, 6.2.2.f, 6.2.3.k)
12. Afspraken over toegangsbeleid, waaronder: (Code 6.2.2.d, 6.2.3.i.2, 6.2.3.i.3, 6.2.3.i.6) 1. goedgekeurde toegangsmethoden, evenals beheersing en gebruik van unieke identificatiemethoden en wachtwoorden; 2. een autorisatieproces voor toegang en speciale bevoegdheden van gebruikers; 3. Een verklaring dat elke toegang die niet expliciet is geautoriseerd, verboden is; 4. een proces voor het intrekken van toegangsrechten of voor het onderbreken van de verbinding tussen de systemen
13. Het recht om elke activiteit verband houdend met de bedrijfsmiddelen van de organisatie te controleren of in te trekken (Code 6.2.2.h, 6.2.3.n)
14. De respectievelijke aansprakelijkheden van de partijen die bij de overeenkomst betrokken zijn; (Code 6.2.2.i, 6.2.3.r)
15. Verantwoordelijkheden met betrekking tot juridische aangelegenheden en hoe wordt gewaarborgd dat wordt voldaan aan de wettelijke eisen, bijvoorbeeld de wetgeving voor gegevensbescherming, waarbij in het bijzonder rekening wordt gehouden met de verschillende nationale rechtssystemen als de overeenkomst betrekking heeft op samenwerking met organisaties in andere landen (Code 6.2.2.j, 6.2.3.s)
16. Beperkingen ten aanzien van het kopiëren en bekendmaken van informatie (het toegelaten gebruik) (Code 6.1.5.f, 6.2.3.b.7)
17. Een verplichting tot het bijhouden van een lijst van personen die bevoegd zijn de ter beschikking gestelde dienst te gebruiken, en wat hun rechten en speciale bevoegdheden zijn ten aanzien van een dergelijk gebruik (Code 6.2.3.i.4)
18. Eisen voor continuïteit van dienstverlening, waaronder maatregelen voor beschikbaarheid en betrouwbaarheid, in overeenstemming met de bedrijfsprioriteiten van de organisatie (Code 6.2.3.q)
19. Voorwaarden voor heronderhandeling/beëindigen van overeenkomsten (Code 6.2.3.v)
20. De belangrijkste onderdelen van de 2.17 Beleid voor aanvaardbaar gebruik van bedrijfsmiddelen (Code 8.1.3)
21. Identificatie van gerubriceerde gegevens, aanvullende beveiligingsmaatregelen, evt. beheersmaatregelen m.b.t. cryptografische sleutels. (Code 10.8.2.h, 10.8.2.k)

22. Ondertekening van overeenkomsten en onderliggende documenten door daartoe bevoegde vertegenwoordigers van de partijen

C.14.4. Overeenkomsten inhuur derden

Beheersmaatregel
De overeenkomsten volgens het type: inhuur van derden voldoen aan zodanige eisen dat risico's op het gebied van beveiliging bij de tegenpartij/partner worden beheerst.

Implementatierichtlijnen

1. Eisen voor de geheimhouding inclusief een definitie van de informatie, die moet worden beschermd en de duur van de geheimhouding , ook na afloop van de overeenkomst volgens HBB, paragraaf 2.17 (Code 6.1.5.a, 6.1.5.b)
2. Voorwaarden en maatregelen om de teruggaaf of vernietiging van informatie en bedrijfsmiddelen aan het einde van, of op een overeengekomen punt tijdens de looptijd van het contract te waarborgen (Code 6.1.5.i)
3. De sancties en/of handelingen die moeten worden ondernomen bij het niet leveren van het afgesproken kwaliteitsniveau of bij inbreuk op de overeenkomst (Code 6.1.5.j)
4. Rapportage, kennisgeving en onderzoek naar gecompromitteerde bedrijfsmiddelen (bijvoorbeeld verlies of ongeoorloofde bekendmaking van gegevens) onjuistheden in informatie (bijvoorbeeld persoonsgegevens), verantwoordelijkheid en aansprakelijkheid in geval van informatiebeveiligingsincidenten en lekken in de beveiliging; (Code 6.1.5.h, 6.2.2.a, 6.2.2.e, 6.2.3.j, 10.8.2.g)
5. De respectievelijke aansprakelijkheden van de partijen die bij de overeenkomst betrokken zijn; (Code 6.2.2.i, 6.2.3.r)
6. Het informatiebeveiligingsbeleid (Code 6.2.3.a)
7. Beperkingen ten aanzien van het kopiëren en bekendmaken van informatie (het toegelaten gebruik) (Code 6.1.5.f, 6.2.3.b.7)
8. Voorwaarden voor heronderhandeling/beëindigen van overeenkomsten (Code 6.2.3.v)
9. De belangrijkste onderdelen van de 2.17 Beleid voor aanvaardbaar gebruik van bedrijfsmiddelen (Code 8.1.3)
10. Uit de verklaring omtrent gedrag zijn geen bezwaren af te leiden om medewerkers voor inhuur in aanmerking te laten komen.
11. Ondertekening van overeenkomsten en onderliggende documenten door daartoe bevoegde vertegenwoordigers van de partijen

C.14.5. Overeenkomsten applicatieontwerp en/of bouw

Beheersmaatregel
De overeenkomsten volgens het type: ontwerp en/of bouw van applicaties voldoen aan zodanige eisen dat risico's op het gebied van beveiliging bij de tegenpartij/partner worden beheerst.

Implementatierichtlijnen

1. Eisen voor de geheimhouding inclusief een definitie van de informatie, die moet worden beschermd en de duur van de geheimhouding , ook na afloop van de overeenkomst volgens HBB, paragraaf 2.17 (Code 6.1.5.a, 6.1.5.b)
2. Het bepalen van de beheerder van gegevens en broncode c.q. overdracht en het vastleggen van de verantwoordelijkheden voor intellectuele eigendomsrechten, licenties van programmatuur (Code 6.1.5.e, 6.2.2.k, 6.2.3.t, 10.8.2.i, 12.5.5.a)
3. Betrokkenheid van een derde partij met onderaannemers, en de beveiligingsmaatregelen die deze onderaannemers moeten implementeren (Code 6.2.3.u)
4. Het recht de in de overeenkomst vastgelegde verantwoordelijkheden te auditen, deze audit door een derde partij te laten uitvoeren en de statutaire rechten van de auditors te benoemen, incl. toegangsrechten voor het uitvoeren van een audit (Code 6.1.5.g, 6.2.3.o, 10.6.2, 12.5.5.b, 12.5.5.d)
5. Communicatie- en escalatieprocedures over de diensten (Code 6.2.3.p)
6. Technische normen voor het opnemen en lezen van informatie en programmatuur (Code 10.8.2.j)
7. Identificatie van gerubriceerde gegevens, aanvullende beveiligingsmaatregelen, evt. beheersmaatregelen m.b.t. cryptografische sleutels. (Code 10.8.2.h, 10.8.2.k)
8. Voldoen aan gedefinieerde kwaliteitseisen (Code 12.5.5.e)

9. Voldoen aan de normen van hoofdstuk 16.3 Geprogrammeerde controles (Code 12.5.5.e)
10. Zekerheidstelling van broncode door middel van escrow in geval een derde partij in gebreke blijft (Code 10.8.2.e, 12.5.5.c)
11. Ondertekening van overeenkomsten en onderliggende documenten door daartoe bevoegde vertegenwoordigers van de partijen

C.14.6. Overeenkomsten dienstverlening algemeen

Beheersmaatregel
De overeenkomsten volgens het type: dienstverlening in het algemeen voldoen aan zodanige eisen dat risico's op het gebied van beveiliging bij de tegenpartij/partner worden beheerst.

Implementatierichtlijnen

1. Eisen voor de geheimhouding inclusief een definitie van de informatie, die moet worden beschermd en de duur van de geheimhouding , ook na afloop van de overeenkomst volgens HBB, paragraaf 2.17 (Code 6.1.5.a, 6.1.5.b)
2. De sancties en/of handelingen die moeten worden ondernomen bij het niet leveren van het afgesproken kwaliteitsniveau of bij inbreuk op de overeenkomst (Code 6.1.5.j)
3. Performance-indicatoren aan de hand waarvan bepaald kan worden of de dienstverlening volgens het overeengekomen kwaliteitsniveau is geleverd, evenals de onaanvaardbare kwaliteitsniveaus (Code 6.2.2.g, 6.2.3.l)
4. Betrokkenheid van een derde partij met onderaannemers, en de beveiligingsmaatregelen die deze onderaannemers moeten implementeren (Code 6.2.3.u)
5. Het voldoen aan het informatiebeveiligingsbeleid (Code 6.2.3.a)
6. Een duidelijke rapportagestructuur en afspraken over de vorm van de rapportage (Code 6.2.3.g)
7. Het recht de in de overeenkomst vastgelegde verantwoordelijkheden te auditen, deze audit door een derde partij te laten uitvoeren en de statutaire rechten van de auditors te benoemen, incl. toegangsrechten voor het uitvoeren van een audit (Code 6.1.5.g, 6.2.3.o, 10.6.2, 12.5.5.b, 12.5.5.d)
8. Communicatie- en escalatieprocedures over de diensten (Code 6.2.3.p)
9. De belangrijkste onderdelen van de 2.17 Beleid voor aanvaardbaar gebruik van bedrijfsmiddelen (Code 8.1.3)
10. De overeengekomen dienstverleningsdefinities en andere aspecten van dienstenbeheer, inclusief de vereiste overdracht en het handhaven van de beveiliging tijdens de overdracht (Code 10.2.1)
11. Wijze waarop over het voldoen aan de performance-indicatoren periodiek, in voor de klantenorganisatie begrijpelijke termen, wordt gerapporteerd
12. Het inzicht geven in de formules die zijn gebruikt voor de berekening van kengetallen
13. Het te hanteren normenkader voor beveiliging (gebaseerd op het eigen HBB-normenkader) dat bij de jaarlijkse audit wordt gehanteerd en de reikwijdte van de audit: opzet, bestaan en werking.
14. Bij samenwerkingsovereenkomsten inzake primaire processen verantwoording af te leggen in jaar- of beheerverslag door middel van een in-control-statement, die onderdeel uitmaakt van de audit als alternatief voor 6.2.3.o
15. Bij samenwerkingsovereenkomsten inzake primaire processen uitvoeren van een ketenbrede risicoanalyse, waarvan de uitkomsten medebepalend zijn voor het te hanteren normenkader voor beveiliging
16. Ondertekening van overeenkomsten en onderliggende documenten door daartoe bevoegde vertegenwoordigers van de partijen

C.14.7. Overeenkomsten Technisch Beheer en Exploitatie IT

Doelstelling
Het (contractueel) vastleggen van de afspraken tussen leverancier en afnemer over het technisch beheer en exploitatie van IT-diensten.

Afbakening
Op dit type overeenkomst is zijn tevens de normen van paragraaf 14 Diverse overeenkomsten, onderdeel dienstverleningsovereenkomsten algemeen van toepassing.

Beheersmaatregel
De dienstverleningsovereenkomsten regelen de beheersdoelstellingen van de afnemer van het technisch

beheer en exploitatie van IT.

Implementatierichtlijnen
Extra voor netwerkdiensten (Code 10.6.2)
1. In de dienstverleningsovereenkomst voor netwerkdiensten worden de beveiligingskenmerken vastgelegd van de:
a. Technologie toegepast voor de beveiliging van netwerkdiensten, zoals authenticatie, encryptie en netwerkverbindingscontroles;
b. Technische parameters vereist voor beveiligde verbinding met de netwerkdiensten in overeenstemming met de beveiligings- en netwerkaansluitingsregels;
c. Procedures voor het gebruik van netwerkdiensten om de toegang tot netwerkdiensten of toepassingen, waar nodig, te beperken.

Capacity (Code 10.2.1)
2. In de dienstverleningsovereenkomst is een capaciteitsparagraaf opgenomen waarin is vastgelegd:
a. De te leveren performance, zonodig gesplitst per voorziening van de onderkende dienst (bijvoorbeeld batch en on-line), gesplitst naar tijdsperiode, plaats en/of klant/afdeling;
b. De werklast waarop de gegarandeerde performance is gebaseerd, inclusief definitie van toelaatbare piekbelastingen;
c. De minimaal en maximaal te leveren capaciteit, in duidelijk omschreven leveringseenheden (bijvoorbeeld gigabytes diskopslag, Mbps netwerktransportcapaciteit);
d. De minimale (en maximale) verwerkingsduur voor capaciteitsaanpassingen.

Availability
3. In de dienstverleningsovereenkomst is een beschikbaarheidsparagraaf opgenomen waarin is vastgelegd:
a. Op welke onderdelen van de dienst het afgesproken beschikbaarheidsniveau betrekking heeft (bijvoorbeeld in de vorm van een configuratieschema);
b. Op welke tijdsperiode het afgesproken beschikbaarheidsniveau betrekking heeft;
c. Welke periode voor gepland onderhoud beschikbaar is ("onderhoudswindow") en of niet-beschikbaarheid vanwege gepland onderhoud wel of niet meetelt in het afgesproken beschikbaarheidspercentage;
d. Wat de maximaal toelaatbare storingsduur is;
e. Wat het maximaal toelaatbaar aantal storingen is;
f. Wat het totaal te leveren beschikbaarheidspercentage is en hoe dit wordt berekend.

IT Service Continuity Management
4. In de dienstverleningsovereenkomst is een calamiteitenparagraaf opgenomen waarin is vastgelegd:
a. wanneer er sprake is van een calamiteit;
b. hoe bij calamiteiten de communicatie tussen IT-organisatie en klantenorganisatie verloopt;
c. binnen welke termijn de IT-dienstverlening na het optreden van een calamiteit moet worden hervat;
d. wat het maximale gegevensverlies is bij het optreden van een calamiteit;
e. welk dienstenniveau na herstel in een calamiteitensituatie van toepassing is;
f. in welke mate en met welke frequentie de calamiteitbeheersingsmaatregelen worden getest en hoe de klantenorganisatie over de testresultaten wordt geïnformeerd;
g. als voor het uitvoeren van testen medewerking van de klantenorganisatie nodig is, welke afspraken daarvoor gelden.

Change Management
5. In de dienstverleningsovereenkomst is wijzigingenparagraaf opgenomen waarin procedures zijn vastgelegd over:
a. het indienen van wijzigingsverzoeken door de klant, de verschillende categorieën wijzigingen die daarbij worden onderkend alsmede criteria voor indeling van deze categorieën en per onderkende wijzigingscategorie de tijd die geldt voor het doorvoeren van de betreffende wijziging;
b. de wijze waarop (belangrijke) wijzigingen binnen de IT-organisatie die impact kunnen hebben voor de klantorganisatie, of waarbij inbreng van de klantorganisatie nodig is, met de klantorganisatie worden afgestemd. (Code 10.2.3.b)

Operations Management
6. In de dienstverleningsovereenkomst worden afspraken gemaakt over:
a. de bewaartermijnen van bestanden;
b. de behandeling en ter beschikkingstelling van output in relatie tot de classificatie hiervan;
c. te hanteren procedures voor incidentele bestandsingrepen, met als uitgangspunten dat controleverslagen

met de gegevens voor en na de correctie in de bestanden worden verstrekt en dat er garanties zijn voor de volledigheid van de verstrekte verslagen;
e. het borgen dat voor exploitatiedoeleinden verzamelde gegevens van klanten (uit logging bijv.) niet voor andere doeleinden beschikbaar zijn.

Loketfunctie
7. In de dienstverleningsovereenkomst worden afspraken gemaakt over:
a. openstellingstijd, bereikbaarheid en reactietijd van de Loketfunctie; b. procedures voor het bij- en actueel houden van een overzicht van de personen die geautoriseerd zijn om werkopdrachten te plaatsen;
c. het melden en classificeren van vragen, verzoeken, incidenten, opdrachten (bepalen prioriteit) en de voor elk onderkend type dienstverlening geldende maximale verwerkingsduur;
d. escalatieprocedures voor die situaties dat afgesproken normtijden worden overschreden.

Overige implementatierichtlijnen
1. Het bepalen van de beheerder van gegevens en broncode c.q. overdracht en het vastleggen van de verantwoordelijkheden voor intellectuele eigendomsrechten, licenties van programmatuur (Code 6.1.5.e, 6.2.2.k, 6.2.3.t, 10.8.2.i, 12.5.5.a)
2. Identificatie van eventuele gerubriceerde gegevens, aanvullende beveiligingsmaatregelen, evt. beheersmaatregelen m.b.t. cryptografische sleutels. (Code 10.8.2.h, 10.8.2.k)
3. Het voldoen aan de privacywetgeving inzake het niet-opslaan/doorgeven van privacygevoelige gegevens buiten de EU, zie hoofdstuk 11 WBP.

C.14.8. Overeenkomsten voor aanschaf IT-voorzieningen

Doelstelling
Het (contractueel) vastleggen van de voorwaarden van levering van IT-voorzieningen.

Beheersmaatregel
De overeenkomsten inzake aanschaf van IT-voorzieningen voorkomen dan wel leiden tot beheersing van beveiligingsrisico's bij het gebruik ervan, voor zover die door de leverancier veroorzaakt voorkomen hadden kunnen worden.

Implementatierichtlijnen
1. Afspraken en overwegingen die betrekking hebben op de aanschaf van IT-voorzieningen bevatten de volgende zaken:
a. voldoen aan algemeen geaccepteerde (industrie)standaards;
b. zijn gecertificeerd volgens ISO/IEC 15408. Dit certificaat is niet voor alle type producten een haalbare eis, vergelijkbare producten die een dergelijk certificaat wel hebben verdienen de voorkeur bij selectie; (Code 12.1.1)
c. voldoen aan de instelbare normen van hoofdstuk 16. IT-voorzieningen
d. geboden functies komen overeen met de productspecificaties en bevatten geen andere functies: statement of integrity;
e. ontwikkelingen (releases) van gerelateerde besturingsprogrammatuur worden binnen een bepaalde periode gevolgd.
f. zijn compatibel met andere systeemvoorzieningen (Code 6.1.4.b)
2. Programmatuur wordt alleen aangeschaft via bekende en erkende leveranciers om te waarborgen dat geen auteursrechten worden geschonden. (Code 15.1.2.b)

C.15. Fasedocumenten ontwerp en invoering IT

Doelstelling
Fasedocumenten voor het ontwerp en invoeren van IT scheppen de voorwaarden voor een betrouwbare informatieverwerking, voor zover dat afhankelijk is van IT-voorzieningen.

C.15.1. Beveiligingsparagraaf procesontwerp

Beheersmaatregel
In de faseproducten van het ontwerp en onderhoud van processen en applicaties wordt in een beveiligingsparagraaf aangegeven op welke wijze de normen voor beveiliging zijn geïmplementeerd.

Implementatierichtlijnen (Code 12.1.1.)
1. Er wordt een beveiligingsparagraaf in de fasedocumenten opgenomen, waarbij de hierna volgende richtlijnen – per fase in toenemende mate van detail - worden uitgewerkt.
2. In een zo vroeg mogelijk ontwerpstadium wordt vastgesteld:
a. of er sprake is van afwijkingen van het basis beveiligingsniveau; (Code 11.6.2.a)
b. of er door of aan derden beveiligingseisen worden gesteld i.v.m. externe insourcing of uitbesteding van primaire- en/of exploitatietaken;
c. of de bestaande beveiligingsuitgangspunten dan wel –maatregelen aanpassing behoeven door nieuwe ontwikkelingen op het gebied van technologie dan wel ander gebruik daarvan;
d. of er sprake is van de specifieke invoerings- en conversieproblematiek
Bij afwijkingen wordt advies gevraagd aan beveiligingsfunctionarissen.
3. Er zijn criteria opgesteld op waarmee een risicoanalyse wordt toegepast, die mede richtinggevend is voor de implementatie van de beveiligingsmaatregelen. Criteria zijn onder meer: geheel nieuwe processen van significante betekenis, ketensamenwerking bij primaire processen, gebruik nieuwe technologie of aan te schaffen, nieuwe IT-voorzieningen al dan niet met bekende kwetsbaarheden. Zie ook 15.3.3
4. Wanneer een applicaties met een hoger beveiligingsniveau in een gemeenschappelijke omgeving wordt uitgevoerd, worden de applicaties waarmee de zone in de technische infrastructuur wordt gedeeld, vastgesteld en goedgekeurd door de procesbeheerder van die applicatie. (Code 11.6.2.b)
5. Geaccepteerde (rest)risico's worden expliciet vastgelegd met een motivering waarom hiervoor (nog) geen beveiligingsmaatregelen worden getroffen.
6. Er is vastgesteld of de uitgangspunten van de bedrijfscontinuïteitsplannen nog van toepassing zijn in de nieuwe of gewijzigde situatie. Het betreft:
a. de maximaal toegestane uitvalsduur (MTU);
b. het maximaal toegestaan digitaal gegevens verlies (MDV);
c. aanvullende maatregelen als a en b niet geheel met de standaard mogelijkheden van Beheer en Exploitatie IT-voorzieningen worden ingevuld;
c. reconstructie niet-digitale informatie.
7. Er wordt vastgesteld of voldaan moet worden aan het melden van de privacyaspecten aan de privacyfunctionaris.
8. Het verwerken van informatie aan andere informatiesystemen en derden voldoet aan het doelbindingsbeginsel voor de privacybescherming.
9. De bewaartijden van informatiebronnen en registraties (papier, digitaal) zijn vastgesteld in een bewaarschema. (Code 15.1.3.b, 15.1.3.c)
10. Maatregelen van beveiliging worden getroffen op basis van paragraaf 16.3 Geprogrammeerde controles en de paragrafen 5.2 Inrichten processen, 5.3 Documenteren processen, 5.4 Reguliere procesuitvoering, 5.8 Rapporteren over het proces.

C.15.2. Implementatieplan processen en applicaties

Beheersmaatregel
Bij de invoering van nieuwe of gewijzigde processen en applicaties wordt een implementatieplan gemaakt.

Implementatierichtlijnen
1. In het implementatieplan worden de volgende onderdelen uitgewerkt:
a. benodigde mens- en middelencapaciteit voor de invoering bij alle betrokken partijen;
b. voorlichting en training in het gebruik van het informatiesysteem;
c. conversietraject;
d. interne controle bij conversie van gegevens op de juistheid en volledigheid van de overgang van de oude