PvIB
Platform voor
InformatieBeveiliging

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Studierapport

Algemene beheersing van IT-diensten

Voorwoord

Met genoegen bieden het bestuur van de NOREA – de beroepsorganisatie van IT-auditors – en het bestuur van het Platform voor Informatiebeveiliging (PvIB) u hierbij het studierapport "Algemene beheersing van IT-diensten" aan. Dit studierapport is het vervolg op het eveneens gezamenlijke NOREA/PvIB-initiatief, het studierapport “Normen voor de beheersing van uitbestede ICT-beheerprocessen” dat in december 2007 is gepubliceerd.

De werkgroep Standaard Normenkader Beheersing en Beveiliging, die beide studierapporten heeft vervaardigd, heeft bij de publicatie in 2007 de lezers uitgenodigd commentaar te leveren. Het ontvangen commentaar is in dit nieuwe studierapport verwerkt door een deel van de oude werkgroep. Dit studierapport kan dan ook gezien worden als een update op het voorgaande studierapport.

Bij de presentatie van het studierapport in 2007 is vastgesteld dat een goede procesuitvoering alleen niet voldoende is voor een adequate beveiliging, maar dat de instellingen van de componenten van de technische ICT-infrastructuur ook moeten worden beoordeeld. De werkgroep heeft deze uitdaging opgepakt, echter dit bleek minder eenvoudig als oorspronkelijk ingeschat.

De complexiteit van de hedendaagse infrastructuren is zodanig groot, dat het beoordelen van een aantal systeemparameters al lang niet meer voldoende is. De beveiliger, systeembeheerder en auditor moeten inzicht weten te krijgen in de totale architectuur en de samenhang van de componenten die samen de infrastructuur vormen. Een audit van alle componenten in hun onderlinge samenhang is zeer complex en omvangrijk en daarmee zeer duur. Er moeten dus keuzes gemaakt worden.

De werkgroep heeft een methodiek uitgewerkt om op basis van risicobenadering te bepalen wat de kritische componenten zijn voor een bepaalde organisatie en welke eisen vanuit beveiligingsoptiek aan deze componenten gesteld moeten worden. Deze methodiek geeft handvatten aan auditors, architecten en informatiebeveiligers om gericht tot goede keuzes te komen in de context van een willekeurige organisatie.

De werkgroep levert met dit nieuwe studierapport een belangrijke bijdrage aan het vakgebied en wij verwachten dan ook dat dit rapport minstens zoveel gebruikt zal worden in de dagelijkse praktijk als het eerste studierapport.

Maart 2015

Samenstelling werkgroep Standaard Normenkader Beheersing en Beveiliging

F. Blom Bc. RE (Frank), Ministerie van Financiën, Auditdienst Rijk

ir. T. de Boer RE CIA CISA CISSP (Tjakko), Technical writer/ITegrity B.V.

B. Bokhorst RE RA (Bart), Ministerie van Financiën (tot mei 2011)

ir. P. Kornelisse RE CISA (Peter), Booking.com

mr. drs. J. Roodnat RE RA (Jan), Auditdienst Rijk

drs. B.J. van Staveren RE (Bart), voorzitter werkgroep/UWV (tot juni 2014)

Lezersforum van de werkgroep

M.M. Buijs RE RI (Maarten) Ministerie van Defensie

ir. A.G. Los (Bert) Sociale Verzekeringsbank (tot april 2014)

drs.ing. N.B. Tewarie RE (Wiedjai) Ministerie van Defensie

NOREA, de beroepsorganisatie van IT-auditors
Postbus 7984
1008 AD Amsterdam
www.norea.nl

PvIB, Platform voor Informatiebeveiliging
Postbus 1058
3860 BB Nijkerk
www.pvib.nl

Inhoud

1 Inleiding

1.1 Probleemstelling en opdracht

Behoefte aan beheersing van IT-diensten

De behoefte aan beheersing van IT-diensten doet zich in principe altijd voor, zowel bij interne als bij externe IT-dienstverlening. De klantorganisatie en de (interne of externe) service-organisatie (IT-dienstverlener) hebben hierbij beiden belang bij eenduidige onderlinge afspraken over de criteria voor de beheersing van IT-diensten, namelijk:

- voor de klantorganisatie in het kader van goed *opdrachtgeverschap* en *toezicht*;
- voor de serviceorganisatie in het kader van een goede *dienstverlening* en *verantwoording*.

De afspraken over de criteria voor de beheersing worden meestal uitgewisseld in de vorm van service levels, aangevuld met een stelsel van beheersingsdoelstellingen en -maatregelen.

Diversiteit aan beheersingscriteria

In de praktijk blijken veel organisaties een eigen criteria te gebruiken voor de beheersing van IT-diensten. Het gebruik van ongelijke beheersingscriteria door klant- en serviceorganisatie wordt dan ondervangen door onderlinge relaties ("cross-references" of "mapping") te leggen van het ene stelsel naar het andere. Dit is veelal een handmatig proces, dat ook subjectieve beslissingen vergt en dus in principe aanleiding kan geven tot discussie. Daarnaast is het handmatige proces tijdrovend en inefficiënt.

Redenen waarom organisaties hebben gekozen voor een eigen stelsel van beheersingscriteria zijn:

- Veel stelsels worden ervaren als te omvangrijk, schrijven te veel detailmaatregelen voor (rule-based) en zijn daardoor minder geschikt voor organisaties;
- Sommige stelsels kunnen teveel geschreven zijn vanuit één visie: die van de auditor, die van de informatiebeveiliger of die van de beheerder van een serviceorganisatie;
- Stelsels kunnen worden ervaren als onoverzichtelijk, hebben een ongeschikte structuur of ongeschikte formuleringen van beheersingsdoelstellingen en -maatregelen (voor bijvoorbeeld assurancerapportages);

- Men had al een eigen stelsel voordat bruikbare andere stelsels voorhanden waren en zijn daaraan vast blijven houden;

- Men geeft sowieso de voorkeur aan een eigen stelsel, omdat daar meer vertrouwen in bestaat en/of daar meer (intern) draagvlak voor aanwezig wordt geacht.

Behoefte aan een stelsel voor uniforme beheersingscriteria

Bij uitbesteding van IT-dienstverlening en bij keteninformatisering is de diversiteit aan partijen groter dan bij interne automatisering en is de behoefte sterker aan een eenduidig, en vooral ook uniform, stelsel van beheersingscriteria. De volgende factoren spelen hierbij een rol:

- Een klantorganisatie heeft te maken met meerdere leveranciers.

  Toelichting:
  Één klantorganisatie kan de IT-dienstverlening in meerdere percelen opsplitsen, die uiteindelijk aan verschillende leveranciers worden gegund (waaronder eventueel ook interne afdelingen). De klantorganisatie heeft doorgaans bij het opstellen van de eigen verantwoording de behoefte om de verantwoordingen van verschillende leveranciers ook weer bij elkaar te kunnen optellen. De klantorganisatie hecht dus aan uniformiteit van de gebruikte beheersingscriteria;

- Eén leverancier levert aan meerdere klantorganisaties.

  Toelichting:
  Eén leverancier heeft doorgaans meerdere klantorganisaties, maar zal in principe proberen om offerten, contracten, audits, service level reports, verantwoordingen en assurancerapportages (zoals ISAE 3402) zoveel mogelijk uniform te houden. Immers, het bedrijfsmodel van gespecialiseerde leveranciers is grotendeels gebaseerd op schaalvoordeel door uniforme bedrijfsprocessen. De leverancier heeft dus eveneens een groot belang bij uniformiteit van de gebruikte beheersingscriteria.

- Meerdere organisaties werken samen in een keten.

  Toelichting:
  Als meerdere organisaties in een keten samenwerken, is voor een totaaloordeel over die keten noodzakelijk dat de verantwoordingen van de individuele organisaties over hun deelbijdrage samenvoegbaar zijn. Ook hier is uniformiteit gewenst.

Eisen aan een stelsel voor uniforme beheersingscriteria

Zoals hiervoor aangegeven is er een belang voor klant- en serviceorganisaties om een referentiekader voor uniforme beheersingscriteria te hanteren voor de onderlinge afstemming

van criteria voor risicobeheersing, verantwoording en toezicht. De eisen voor een dergelijk stelsel dienen te zijn:

- Een overzichtelijke structuur;
- Vooral beschrijvend wat bereikt moet worden; niet hoe dat bereikt moet worden. (Het hoe is vaak elders beschreven in reeds bestaande best-practices);
- Een wijze van beschrijven die voor organisaties van diverse grootte hanteerbaar is;
- Eenvoudig te relateren aan thans gebruikte internationale standaarden.

Opdracht

De opdrachtgevers voor dit studierapport, de Nederlandse Orde van Register IT-auditors (NOREA) en het Platform voor Informatiebeveiliging (PvIB), beogen met dit studierapport bij te dragen aan de onderlinge afstemming van criteria voor risicobeheersing, verantwoording en toezicht voor de "general IT-controls".

Dit studierapport is een uitbreiding en herziening van het studierapport "Normen voor de beheersing van uitbestede ICT-beheerprocessen" uit 2007 [1]. Het bevat een herziening van het stelsel van uniforme beheersingscriteria voor beheerprocessen en is uitgebreid met een stelsel van uniforme beheersingscriteria voor technische instellingen van IT-middelen. Door deze uitbreiding omvat het stelsel nu zowel de technische als procesmatige aspecten van de "general IT-controls".

Tevens is het studierapport uitgebreid met een werkwijze voor de bepaling van relevante beheersingscriteria en voor de selectie van beheersingsmaatregelen voor de IT-diensten. Deze werkwijze is bedoeld voor gebruik door zowel de klantorganisatie (voor bepaling van de beheersingscriteria in het kader van het opdrachtgeverschap en toezicht), de serviceorganisatie (voor selectie van beheersingsmaatregelen en voor het afleggen van verantwoording), als voor gebruik door auditors (voor scoping van de te toetsen beheersingsmaatregelen).

De opdracht voor het stelsel van uniforme beheersingscriteria luidde:

> Ontwikkel een stelsel voor de algemene IT-beheersingsmaatregelen van (uiteindelijk) alle elementen van IT-dienstverlening, dat toepasbaar moet zijn in situaties van uitbesteding van IT-dienstverlening.
>
> Ontwikkel dit stelsel in samenspraak met en maak het bruikbaar voor:
>
> - Klantorganisaties van zowel de overheid als het bedrijfsleven;
> - IT-dienstverleners (intern en extern);
> - IT-auditors (intern en extern).
>
> De opdrachtgevers doen de suggestie om de uitwerking gefaseerd ter hand te nemen en te beginnen met de verwerkingsorganisatie. Daarna zou in ieder geval de ontwikkelorganisatie aan de orde moeten komen.
>
> Er dient rekening te worden gehouden met reeds bestaande referentiekaders zoals, CobiT, ITIL en de Code voor Informatiebeveiliging (ISO/IEC 27001).

De oordeelsvorming over de opzet en werking van het stelsel van beheersingsmaatregelen valt buiten de opdracht van de werkgroep. De werkgroep dient verder geen onderverdeling te maken in criteria voor verschillende risicoklassen. Dit zou de complexiteit te zeer vergroten.

1.2 Opbouw van het studierapport

Het studierapport is, naast deze Inleiding, opgebouwd uit de volgende hoofdstukken:

- Hoofdstuk 2 is een verkenning van het onderzoeksgebied, waarin relevante begrippen worden toegelicht, achtergronden van de problematiek worden geanalyseerd en het onderzoeksgebied wordt afgebakend;
- Hoofdstuk 3 behandelt algemene beheersingsdoelstellingen voor IT-diensten;
- Hoofdstuk 4 beschrijft een werkwijze voor de bepaling van beheersingscriteria en voor de selectie van beheersingsmaatregelen voor de IT-diensten;
- Hoofdstuk 5 (beheersingscriteria voor de technische inrichting van IT-middelen) en hoofdstuk 6 (beheersingscriteria voor IT-beheerprocessen) beschrijven de uniforme beheersingscriteria.

In bijlage A is een casus beschreven waarin de toepassing van de werkwijze en de beheersingscriteria worden geïllustreerd. Tenslotte zijn bijlagen opgenomen voor een begrippenlijst en lijst van geraadpleegde literatuur.

2 Verkenning en afbakening van het onderzoeksgebied

2.1 Vraag en aanbod van IT-diensten

Demand en Supply

Iedere organisatie die gebruik maakt van IT heeft te maken met het bepalen van de eigenschappen waaraan de IT-dienstverlening dient te voldoen en het zorgdragen dat de gewenste IT-diensten worden geleverd. Het coördineren van de vraagzijde en het aansturen van de leverancier van de IT-diensten wordt ook wel aangeduid met Demand Management. Het coördineren van de aanbodzijde wordt aangeduid met Supply Management.

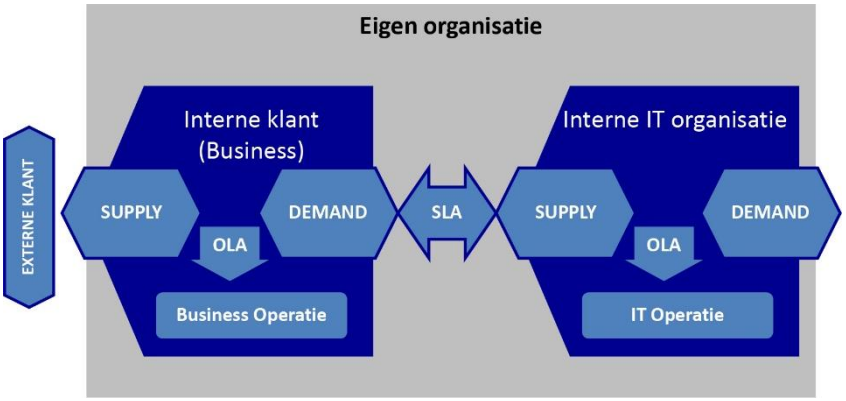
De gewenste eigenschappen van de IT-dienstverlening worden (uiteindelijk) ontleend aan de eisen van klanten in de buitenwereld. Het spreekt voor zich dat deze eisen aan verandering onderhevig zijn en dat dus ook de gewenste eigenschappen van de IT-diensten zullen veranderen in de tijd. De wisselwerking tussen Demand en Supply is hierdoor dynamisch.

Structuren van Demand en Supply

Demand en Supply van de IT-dienstverlening komen in verschillende structuren voor. Hierna worden enkele van deze structuren benoemd, die ook in combinaties naast elkaar kunnen voorkomen.

<u>IT-dienstverlening volledig in eigen beheer</u>

De meest eenvoudige vorm van IT-dienstverlening treft men aan, wanneer in de eigen organisatie een IT-afdeling is ingericht die alles in eigen beheer regelt. Deze structuur is geïllustreerd in afbeelding 1.



Afbeelding 1: IT-dienstverlening in eigen beheer.

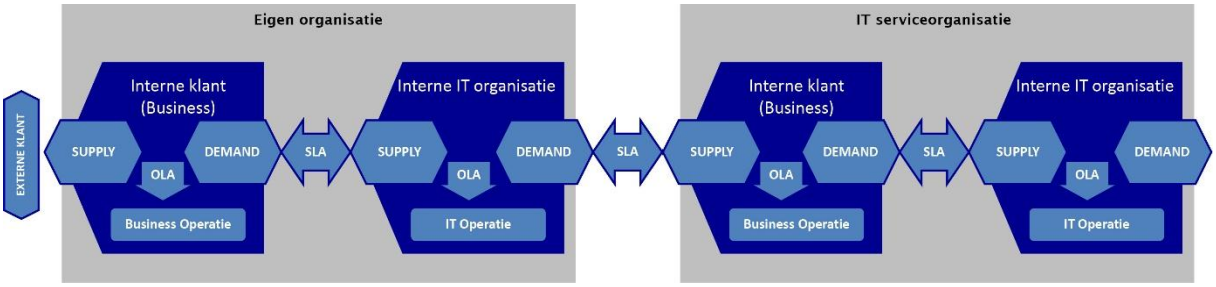
IT-dienstverlening met (gedeeltelijke) uitbesteding

Met de toenemende complexiteit van IT komt het steeds meer voor dat de interne IT-afdeling niet alles meer in eigen beheer regelt, maar bepaalde diensten uitbesteedt aan een externe IT-dienstverlener.

Nu formuleert de interne IT-afdeling op haar beurt de eisen (demands) en sluit een overeenkomst met de leverancier. Deze overeenkomst noemt men ook wel een Underpinning Contract: het is een contract dat ondersteunend is aan de SLA tussen de serviceorganisatie en de klantorganisatie.

Om de leverancier en de uitbestede diensten te beheren wordt in de serviceorganisatie het proces Supply Chain Management ingericht. Men kan zich voorstellen dat de omvang van uitbesteding kan variëren van minimaal (geen Supply Chain Management) tot maximaal, waarbij de serviceorganisatie zich vrijwel alleen bezighoudt met Supply Chain Management. In een organisatie zal altijd sprake zijn van een eigen, interne serviceorganisatie, al kan dat in een zeer rudimentaire vorm zijn.

IT-dienstverlening met (gedeeltelijke) uitbesteding is weergegeven in afbeelding 2.

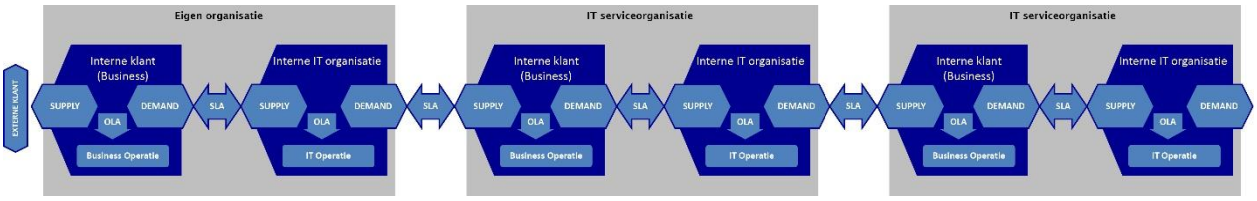


Afbeelding 2: IT-dienstverlening met uitbesteding.

IT-dienstverlening door een keten van leveranciers: een recursief model

Het is belangrijk om te onderkennen dat het voorgaande schema recursief is: omdat een leverancier zèlf ook een organisatie vormt en omdat een leverancier zelf ook weer diensten kan uitbesteden, komt het schema, en dus ook de begrippen “klantorganisatie” en “serviceorganisatie”, op verschillende niveaus terug, zoals weergegeven in afbeelding 3.

Vanwege de recursiviteit zijn de beheersingscriteria in dit studierapport evenzeer van toepassing op elk niveau van recursiviteit.



Afbeelding 3: IT-dienstverlening door een keten van leveranciers.

Klantorganisatie en serviceorganisatie

In dit studierapport wordt de volgende terminologie gehanteerd voor de betrokken partijen bij de risicobeheersing van en verantwoording over IT-diensten:

- **Klantorganisatie**: de (interne of externe) afnemer van de IT-diensten (in de Engelstalige vakliteratuur meestal aangeduid als “user organisation” of “client organisation”);
- **Serviceorganisatie**: de (interne of externe) leverancier van de IT-diensten (in de Engelstalige vakliteratuur meestal aangeduid als “service organisation”); een leverancier van de serviceorganisatie wordt aangeduid als een subserviceorganisatie.
- **Klantauditor**: de (interne of externe) auditor van de klantorganisatie (in de Engelstalige vakliteratuur meestal aangeduid als “user auditor”);
- **Serviceauditor**: de (interne of externe) auditor van de serviceorganisatie (in de Engelstalige vakliteratuur meestal aangeduid als “service auditor”).

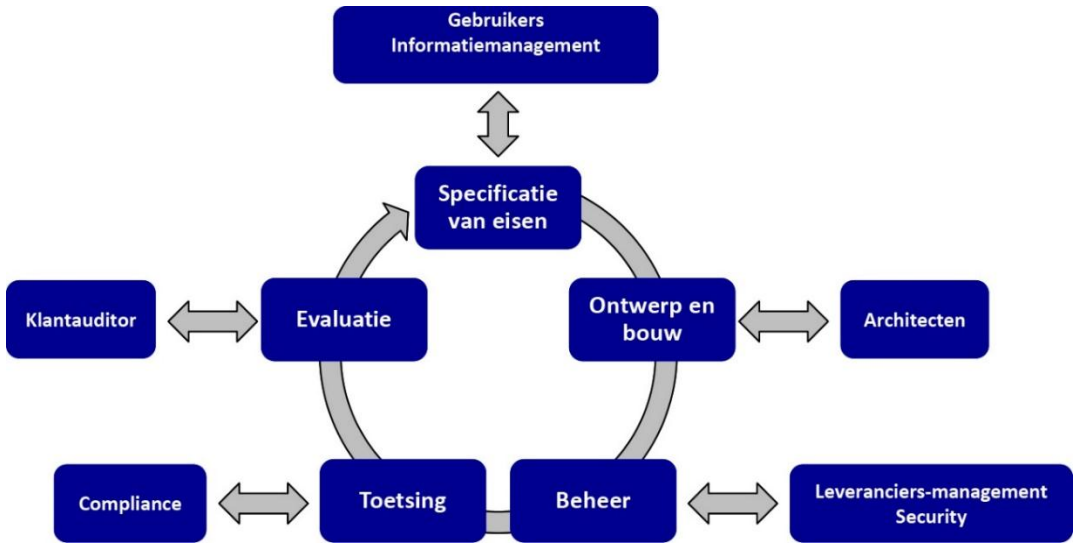
De hierboven genoemde partijen kunnen behoren tot verschillende organisaties, maar kunnen net zo goed allen behoren tot dezelfde organisatie. In dat laatste geval is de serviceorganisatie een interne IT-afdeling en behoren de klant- en serviceauditor tot een interne auditafdeling. Het combineren van de rollen van klant- en serviceauditor vormt in principe geen bezwaar: in feite vervult de auditor dan de rol van auditor van een procesketen. De auditor dient zich vanzelfsprekend te houden aan beroepsregels van onpartijdigheid en van geheimhouding ten aanzien van informatie over de verschillende cliënten.

2.2 Knelpunten bij risicobeheersing van IT-diensten

Binnen de klant-en serviceorganisatie zijn er verschillende rollen die elk betrokken zijn bij risicobeheersing van IT-diensten. Elk van deze rollen dient vanuit de eigen invalshoek knelpunten op te lossen en kan baat hebben bij gemeenschappelijke beheersingscriteria. In deze sectie worden verschillende belanghebbenden van de klant- en serviceorganisatie benoemd met veel voorkomende knelpunten van risicobeheersing.

Voor de klantorganisatie zijn de rollen bijvoorbeeld:

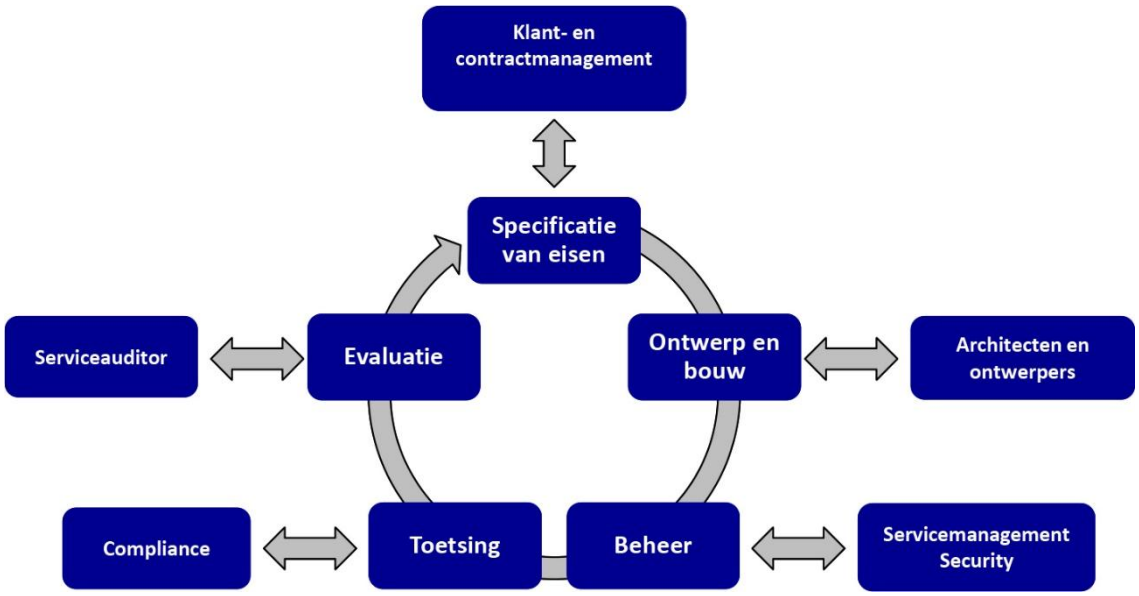
- Partijen belast met het definiëren van de IT-dienstverlening (gebruikersafdelingen; informatiemanagement; architecten);
- Partijen belast met ontwerp en bouw (architecten);
- Partijen belast met het aansturen van IT-dienstverleners (leveranciersmanagement, security);
- Partijen belast met risicobeheersing, beveiliging en compliance;
- De klantauditor (intern en/of extern).



Afbeelding 4: Bij risicobeheersing betrokken partijen bij de klantorganisatie

Voor de serviceorganisatie zijn de rollen bijvoorbeeld:

- Partijen belast met de contractering (klant- en contractmanagement; servicemanagement);
- Partijen belast met het inrichten van IT-diensten (ontwerpers en architecten);
- Partijen belast met de productie en onderhoud van IT-diensten (servicemanagement; operations; security);
- Partijen belast met risicobeheersing, beveiliging en compliance;
- De serviceauditor (intern en/of extern).



Afbeelding 5: Bij risicobeheersing betrokken partijen bij de serviceorganisatie.

In Tabel 1 zijn ter illustratie enkele veel voorkomende knelpunten van risicobeheersing opgesomd per fase van contractering en per belanghebbende van de klant- en serviceorganisatie. Met de in dit studierapport te beschrijven beheersingscriteria en werkwijze wordt beoogd om voor deze knelpunten een handreiking te bieden.

Fase	Knelpunten	Belanghebbenden	
		Klantorganisatie	Serviceorganisatie
Specificatie van eisen / contract-vorming	Welke afspraken moeten worden gemaakt? Hoe dienen afspraken te worden geformuleerd over de risicobeheersing van de IT-diensten? Hoe gedetailleerd dienen beveiligingseisen te worden gespecificeerd?	Gebruikers Informatiebeheer Security	Klant- en contract-management Security
	Hoe zal toezicht worden gehouden op de risicobeheersing? Welke informatie dient te worden verstrekt over de risicobeheersing? Welke inhoud dienen assurancerapporten te hebben?	Audit / Security & Compliance	Audit / Security & Compliance
Ontwerp en bouw	Hoe dient de risicoanalyse te worden uitgevoerd? Welke beheersmaatregelen dienen te worden ingericht?	Leveranciers-management Architecten	Architecten en ontwerpers
Beheer	Welke risico's zijn van belang om te beheersen?	Leveranciers-management	Servicemanagement Security &

	Welke beheersingsmaatregelen dienen te worden ingericht?		Compliance
Toetsing	Op welke risico's dient de IT-dienst te worden getoetst? Hoe dient de risicoanalyse te worden uitgevoerd? Welke beheersings-maatregelen dienen te zijn ingericht?	Compliance Audit	Compliance Audit
Evaluatie	Is de verstrekte assurance-informatie relevant en volledig? Hoe moeten de bevindingen worden geïnterpreteerd?	Gebruikers Audit	Servicemanagement Klant- en contract-management

Tabel 1: Knelpunten bij risicobeheersing van IT-diensten.

2.3 Begrippen voor de risicobeheersing van IT-diensten

Kwaliteitsaspecten van IT-diensten

De mate waarin de IT-diensten voldoen aan de gespecificeerde, of impliciet verwachte, eigenschappen wordt aangeduid met het begrip “kwaliteit”. In het kader van risicobeheersing zal dit studierapport zijn gericht op de volgende kwaliteitsaspecten, waarbij wordt opgemerkt dat het aspect *controleerbaarheid* als afgeleide wordt beschouwd van de eis van het kunnen afleggen van verantwoording en daarom niet apart wordt genoemd:

- Beschikbaarheid. De mate waarin een object (informatie, IT-dienst of IT-middel) continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.
- Integriteit. De mate waarin het object (gegevens, IT-dienst of IT-middel) in overeenstemming is met de beoogde werkelijkheid.
- Exclusiviteit. De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruikmaken van een object (IT-dienst of IT-middel) of toegang hebben tot een object (creëren, wijzigen, verwijderen of lezen van gegevens).

Instrumenten voor toezicht op en verantwoording over risicobeheersing

Voor het toezicht op respectievelijk verantwoording over de risicobeheersing van IT-diensten kan gebruik worden gemaakt van verschillende instrumenten. De meest gangbare instrumenten zijn:

- Contracten. Formele overeenkomsten tussen klant- en serviceorganisatie en daaraan gerelateerde documenten zoals Service Level Agreement en Producten & Diensten Catalogus;
- Service level rapportages. Informatie (periodiek of continu) over de geleverde prestaties van IT-diensten. Deze informatie kan worden verkregen door service level rapportages, besprekingen met de serviceorganisatie of zelfs via geautomatiseerde, continue dashboards. De rapportages worden soms opgesteld door de serviceorganisatie en soms, indien de klantorganisatie de geleverde prestaties zelf kan meten, door de klantorganisatie. In geval van zogenaamde control selfassessments, kan deze informatie ook de risicobeheersing betreffen;
- Assurancerapporten. Informatie over de risicobeheersing van de IT-diensten en over de betrouwbaarheid van de informatievoorziening via servicerapportages. In tegenstelling tot informatie in servicerapportages, betreft dit doorgaans informatie die niet direct

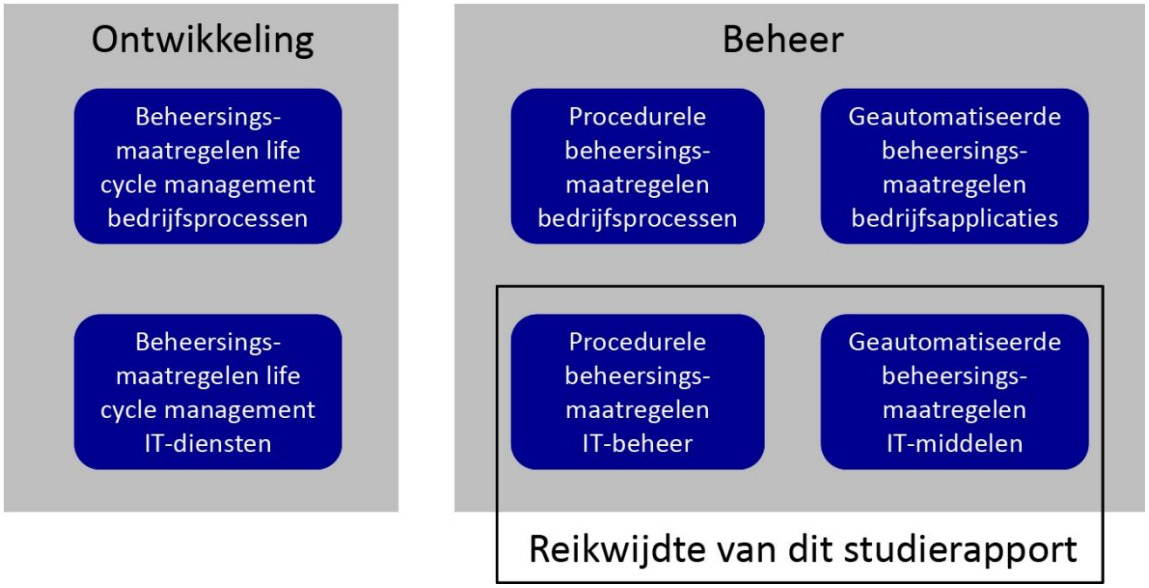
kan worden geverifieerd door de klantorganisatie. Bijvoorbeeld randvoorwaarden opgelegd door de klantorganisatie (zoals wet- en regelgeving, intern beleid, eisen van maatschappelijk verantwoord ondernemen), waar de serviceorganisatie zich aan dient te houden. De auditor die een assurancerapport uitbrengt kan in opdracht werken van de klantorganisatie (op basis van een "right-to-audit" clausule in het contract) of in opdracht van de serviceorganisatie.

Typen van beheersingsmaatregelen

Voor het doel van dit studierapport, als hulpmiddel bij de risicobeheersing van en verantwoording over IT-diensten, is het zinvol om onderscheid te maken in de aard van beheersingsmaatregelen:

- **Beheersingsmaatregelen die onderdeel uitmaken van de bedrijfsprocessen van de klantorganisatie**. Deze beheersingsmaatregelen worden "business process controls" genoemd en zijn verder onder te verdelen in:
    - Geautomatiseerde beheersingsmaatregelen (application controls in bedrijfsapplicaties);
    - Procedurele, handmatige beheersingsmaatregelen ingebed in een bedrijfsproces;
- **Beheersingsmaatregelen die onderdeel uitmaken van de IT-diensten van de serviceorganisatie**. Deze beheersingsmaatregelen worden "general IT controls" genoemd. Deze beheersingsmaatregelen zijn verder onder te verdelen in:
    - Geautomatiseerde beheersingsmaatregelen (technische instellingen van IT-middelen en application controls van beheerapplicaties);
    - Procedurele, handmatige beheersingsmaatregelen ingebed in een IT-beheerproces van de serviceorganisatie;
- **Beheersingsmaatregelen die betrekking hebben op de levenscyclus van bedrijfsprocessen en IT-diensten**. Bedrijfsprocessen en IT-diensten worden ontworpen, gebouwd, getest, operationeel gemaakt, onderhouden en ooit weer uit productie gehaald.

De typen van beheersingsmaatregelen worden in de volgende figuur weergegeven.



Afbeelding 6: Typen van beheersingsmaatregelen.

2.4 Afbakening van het onderzoeksgebied

Dit studierapport richt zich op de "general IT controls" van zowel beheerprocessen als technische componenten (de twee onderste kwadranten in Afbeelding 6).

Beheersingscriteria die betrekking hebben op bedrijfsprocessen en -applicaties van de klantorganisatie (business process controls) en op de levenscyclus van IT-diensten worden niet behandeld. Deze keuze wil echter niet zeggen, dat dergelijke criteria niet van belang zijn bij de beheersing en verantwoording van de IT-dienstverlening tussen klant- en serviceorganisatie. **Integendeel: in veel gevallen van IT-dienstverlening zullen deze beheersingscriteria moeten worden gebruikt naast beheersingscriteria voor bedrijfsprocessen en voor de levenscyclus van IT-diensten.**

3 Algemene beheersingsdoelstellingen voor IT-diensten

3.1 Inleiding

In een demand-supply situatie, zoals geschetst in paragraaf 2.1, zal de klantorganisatie van haar serviceorganisaties verlangen dat de relevante risico's ten aanzien van de beschikbaarheid, integriteit en exclusiviteit van de IT-diensten worden beheerst.

Dit hoofdstuk behandeld beheersingsdoelstellingen die in het algemeen verband houden met de beschikbaarheid, integriteit en exclusiviteit van IT-diensten, ongeacht de aard en functionaliteit van de IT-diensten. Daarom worden deze doelstellingen *algemene* beheersingsdoelstellingen genoemd; de gerelateerde beheersingsmaatregelen worden algemene beheersingsmaatregelen genoemd (Engels: "general IT controls"). Het overzicht van de beheersingsdoelstellingen is gebaseerd op praktijkervaringen en niet noodzakelijkerwijs volledig. De algemene beheersingsdoelstellingen worden opgesomd en toegelicht in paragraaf 3.2.

Ref	Algemene IT-beheersingsdoelstelling	BIV-aspect
A	De inrichting van de IT-middelen dient te worden beperkt tot de strikt noodzakelijke en geautoriseerde functionaliteit.	BIV
B	Toegang tot en gebruik van IT-diensten dient te worden beperkt tot geautoriseerde gebruikers en beheerders.	BIV
C	De IT-dienst dient onder benoemde bedrijfsomstandigheden een overeengekomen werklast te kunnen verwerken.	B
D	De IT-dienst dient, in geval van benoemde typen afwijkende bedrijfsomstandigheden (calamiteiten), tijdig herstelbaar te zijn om een overeengekomen werklast te kunnen verwerken.	B
E	De kenmerken en samenhang van IT-middelen dienen juist en volledig te worden gedocumenteerd.	BIV
F	Wijzigingsaanvragen dienen te worden geautoriseerd met inachtneming van de risico's voor de IT-dienst.	BIV
G	Wijzigingen dienen juist, volledig en tijdig te worden doorgevoerd.	BIV
H	De IT-dienst dient te worden beschermd tegen verstoringen door onjuiste wijzigingen en door ontwikkel- en testactiviteiten.	BIV

I	Incidenten in de IT-dienst dienen tijdig en doeltreffend te worden voorkomen of te worden gesignaleerd en afgehandeld.	BIV
J	Productieopdrachten dienen te worden geautoriseerd.	BIV
K	Productieopdrachten dienen juist, volledig en tijdig te worden verwerkt.	I
L	Relevante gebeurtenissen van beheer, gebruik en (dreigende) verstoring van de IT-dienst dienen te worden vastgelegd.	BIV

Tabel 2: Relatie van IT-beheersingsdoelstellingen met kwaliteitsaspecten Beschikbaarheid (B), Integriteit (I) en Exclusiviteit (V).

3.2 Toelichting van de algemene beheersingsdoelstellingen

A **De inrichting van de IT-middelen dient te worden beperkt tot de strikt noodzakelijke en geautoriseerde functionaliteit.**

Toelichting:
IT-middelen dienen te worden ingericht volgens een geautoriseerd ontwerp (baseline), dat dient te zijn geautoriseerd door of namens de eigenaren van de IT-dienst (al dan niet na instemming van de klantorganisatie).
Het ontwerp dient alleen de strikt noodzakelijke functionaliteit te bevatten, omdat elke overbodige functionaliteit in potentie een bron is van ongeautoriseerd gebruik van het IT-middel en bron van risico's voor de beschikbaarheid, integriteit en exclusiviteit van de IT-dienst. Veel IT-middelen zijn standaard uitgerust met functionaliteiten die overbodig zijn voor de functie waarvoor zij worden ingezet. In het ontwikkelingsproces van een IT-dienst dient men daarom gericht deze overbodige functies te doen deactiveren (Engels: "hardening"). Beheersingscriteria voor het ontwikkelingsproces van de IT-dienst vallen overigens buiten de reikwijdte van dit studierapport.

B **Toegang tot en het gebruik van IT-diensten dient te worden beperkt tot geautoriseerde gebruikers en beheerders.**

Toelichting:
Deze doelstelling heeft betrekking op de logische en fysieke toegang van alle IT-middelen die de IT-dienst vormen. Indien de toegang tot IT-middelen niet is beperkt tot geautoriseerde gebruikers en beheerders, kan ongeautoriseerd gebruik worden gemaakt van de IT-dienst (gebruikerstoegang) of kunnen ongeautoriseerde wijzigingen worden aangebracht aan de IT-dienst (beheerderstoegang). De beschikbaarheid, integriteit en exclusiviteit van de IT-dienst kunnen hierdoor worden aangetast.
Geautoriseerde toegang impliceert een juiste identificatie en authenticatie van gebruikers en beheerders. Geautoriseerd gebruik impliceert juiste autorisaties.
Toegang en gebruik dienen te worden geautoriseerd door of namens de eigenaren van de IT-dienst.

C **De IT-dienst dient onder de gespecificeerde bedrijfsomstandigheden een overseen-gekomen werklast te kunnen verwerken.**

Toelichting:
Deze doelstelling betreft het kunnen verwerken van een afgesproken werklast door de IT-dienst. Hiervoor is voldoende capaciteit en beschikbaarheid nodig van zowel technische als niet-technische middelen, waaronder medewerkers in een juiste samenstelling qua kennis en ervaring.

Om deze beheersingsdoelstelling rationeel en toetsbaar te maken, dienen de "benoemde bedrijfsomstandigheden" expliciet te worden afgesproken tussen klant- en serviceorganisatie, waaronder: openingstijden; de afgesproken/verwachte werklast verdeeld over de tijd; periodieke piekbelastingen zoals spitsuren en hoogseizoenen; kritieke verwerkingen zoals maand- en jaarverwerkingen; en de capaciteit en beschikbaarheid bij benoemde typen "normale" storingen zoals hardware- en stroomstoringen.

D **De IT-dienst dient, in geval van benoemde typen afwijkende bedrijfsomstandigheden (calamiteiten), tijdig herstelbaar te zijn om een overeengekomen werklast te kunnen verwerken.**

Toelichting:
Deze doelstelling betreft het herstelbaar zijn van een IT-dienst na afgesproken typen van calamiteiten. Het gaat hier om uitzonderlijke omstandigheden waarbij de beschikbaarheid en capaciteit van de IT-dienst tijdelijk zijn onderbroken of verlaagd.
Om deze beheersingsdoelstelling rationeel en toetsbaar te maken, dienen de klant- en serviceorganisatie expliciet afspraken te maken over de dienstenniveaus (zoals responstijden, hersteltijden en capaciteiten) per type calamiteit, omdat calamiteiten er in vele soorten en vormen zijn.

E **De kenmerken en samenhang van IT-middelen dienen juist en volledig te worden gedocumenteerd.**

Toelichting:
De kenmerken en samenhang van de IT-middelen dienen juist en volledig te worden gedocumenteerd, zodat de hiervan afhankelijke IT-beheerprocessen van juiste en volledige informatie kunnen worden voorzien. De informatiebehoeften van afhankelijke IT-beheerprocessen en de relevantie van de IT-middelen voor de IT-dienst bepalen de aard en diepgang van de kenmerken, die dienen te worden gedocumenteerd.

F **Wijzigingsaanvragen dienen te worden geautoriseerd met inachtneming van de risico's voor de IT-dienst.**

Toelichting:
Wijzigingsaanvragen dienen te worden geautoriseerd na evaluatie van de risico's, zodat de wijzigingen geen ongewenste (neven)effecten hebben op IT-dienst. Vaak kan de initiator van de wijziging de (neven)effecten niet geheel overzien. Het is daarom van belang om deze effecten gestructureerd in kaart te brengen en de impact af te stemmen met alle belanghebbenden, zoals de eigenaar van de IT-dienst, beheerders van IT-middelen en de betrokkenen van andere IT-beheerprocessen.

G Wijzigingen dienen juist, volledig en tijdig te worden doorgevoerd.

Toelichting:
Wijzigingen dienen juist, volledig en tijdig te worden doorgevoerd, zodat noodzakelijk verbeteringen of de instandhouding van de IT-dienst niet in het gedrang komen. Voorafgaand aan een wijziging dienen alle aspecten te worden geïdentificeerd, die eveneens een wijziging dienen te ondergaan of die worden beïnvloed als gevolg van de wijziging (zoals systeemdocumentatie en continuïteitsplannen).

H De IT-dienst dient te worden beschermd tegen verstoringen door onjuiste wijzigingen en door ontwikkel- en testactiviteiten.

Toelichting:
Onjuiste wijzigingen en het uitvoeren van ontwikkel- en testactiviteiten in de productieomgeving kunnen de IT-dienst verstoren en de beschikbaarheid en integriteit van de IT-dienst aantasten. Bij voorkeur dient de productieomgeving van de IT-dienst te worden geïsoleerd van de omgeving waarin wordt ontwikkeld en getest. Daarnaast dient de doeltreffendheid van wijzigingen eerst te worden geëvalueerd en dienen er geen ongewenste neveneffecten te zijn. Indien wijzigingen niet het beoogde effect blijken te hebben, is het van belang om terug te kunnen keren naar de oorspronkelijke situatie (ook wel: back-out of terugvalscenario).

I Incidenten in de IT-dienst dienen tijdig en doeltreffend te worden voorkomen of te worden gesignaleerd en afgehandeld.

Toelichting:
Het voorkomen of signaleren, analyseren en afhandelen van verstoringen is van belang voor het minimaliseren van de impact van de verstoringen op de IT-dienst en om het afgesproken dienstenniveau te realiseren. De norm voor tijdigheid is afhankelijk van het afgesproken dienstenniveau, vaak in relatie tot de impact en urgentie van de verstoring.

J Productieopdrachten dienen te worden geautoriseerd.

Toelichting:
Onder productieopdrachten worden verstaan: handelingen in de productieomgeving met gebruikersgegevens die worden uitgevoerd door de serviceorganisatie, bijvoorbeeld batchverwerking, backup en restore van gegevens, en mutatie van gebruikersgegevens met beheertools.

Indien productieopdrachten niet juist zijn geautoriseerd, bestaat het risico dat de beschikbaarheid, integriteit en exclusiviteit van de productiegegevens worden aange-

tast. Het is daarom van belang dat productieopdrachten worden geautoriseerd door of namens de klantorganisatie.

K **Productieopdrachten dienen juist, volledig en tijdig te worden verwerkt.**

Toelichting:
Een juiste, volledige en tijdige verwerking van productieopdrachten is van belang om te voldoen aan de overeengekomen dienstenniveaus en mogelijk voor het handhaven van de beschikbaarheid en integriteit van gebruikersgegevens.
In de uitvoering van productieopdrachten is vaak sprake van veel onderlinge afhankelijkheden en complexiteit. De daarmee gepaard gaande risico's van juistheid, volledigheid en tijdigheid kunnen worden beperkt door het toepassen van draaiboeken en automatisch werkende schedulingsoftware.

L **Relevante gebeurtenissen van beheer, gebruik en (dreigende) verstoring van de IT-dienst dienen te worden vastgelegd.**

Toelichting:
Onder relevante gebeurtenissen van beheer, gebruik en (dreigende) verstoring van de IT-dienst worden verstaan:

- het gebruik van beheerfuncties van (middelen van) de IT-dienst;
- het gebruik van gebruikersfuncties van de IT-dienst;
- beveiligingsovertredingen;
- veranderingen in de status van en verstoringen van (middelen van) de IT-dienst.

De doelstelling van het vastleggen van relevante gebeurtenissen is:

- om risico's van de IT-dienst te beheersen, bijvoorbeeld om (dreigende) afwijkingen in de kwaliteit van de IT-dienst tijdig te signaleren, te analyseren en af te handelen;
- om aan te kunnen tonen dat aan overige beheersingsdoelstellingen is voldaan.

De reikwijdte van de vast te leggen gebeurtenissen is afhankelijk van de overige beheersingsdoelstellingen en de relevante risico's.

De methode van vastlegging kan automatische registratie betreffen door de technische configuratie van de IT-middelen (logging), als ook handmatige registratie op basis van beheerprocessen (logboeken).

De reikwijdte en methode van vastlegging dienen te worden bepaald in de ontwerpfase van de IT-dienst en dienen te worden vastgesteld in het geautoriseerde ontwerp.

4 Werkwijze voor risicobeheersing van IT-diensten

In dit hoofdstuk wordt een werkwijze beschreven voor de risicobeheersing van IT-diensten. In de hierna volgende paragrafen wordt achtereenvolgens ingegaan op:

- Stappen te nemen door de klantorganisatie om eisen te formuleren die het stelt aan de risicobeheersing van IT-diensten.
- Stappen te nemen door de serviceorganisatie om invulling te geven aan de eisen aan de risicobeheersing van IT-diensten.

4.1 Werkwijze voor de klantorganisatie

Afbeelding 7: Stappenplan voor de klantorganisatie.

4.1.1 De klantorganisatie bepaalt de bedrijfsrisico's

Uitgangspunt voor de risicobeheersing van IT-diensten zijn de bedrijfsrisico's die de klantorganisatie wenst te beheersen. De klantorganisatie dient daarom ten eerste een risicoanalyse uit te voeren welke bedrijfsrisico's van belang zijn om te beheersen in het kader van de bedrijfsdoelstellingen.

Het is een beslissing van de klantorganisatie – op basis van kosten en baten, regelgeving of anderszins – hoe deze risicoanalyse wordt uitgevoerd, hoe diepgaand en hoe volledig. De klantorganisatie kan er voor kiezen om bijvoorbeeld de risicoanalyse toe te spitsen op specifieke risico's, zoals op specifieke bedrijfstransacties, wetgeving, etcetera. De methodiek van risicoanalyse is geen onderwerp van dit studierapport en de uitkomst van deze risicoanalyse wordt hier als input beschouwd voor de risicobeheersing van IT-diensten.

De relatie tussen bedrijfsrisico's en IT-diensten is vooral te vinden daar waar deze bedrijfsrisico's betrekking hebben op *bedrijfsprocessen* en *bedrijfsgegevens*, omdat IT-diensten met name worden gebruikt ter ondersteuning van bedrijfsprocessen en

bedrijfsgegevens. (Andere klassen van bedrijfsrisico's, zoals strategische, krediet- en marktrisico's, hebben minder verband hebben met de afgenomen IT-diensten).

De uitkomst van deze stap is een beschrijving van de te beheersen bedrijfsrisico's van bedrijfsprocessen en bedrijfsgegevens. (Zie voorbeelden in Tabel 3).

RACI-tabel	Business Management	Proces & Informatie Management	Supplier Management	Operational Risk Management	**Audit**
Stap 1: Bepaal bedrijfsrisico's.	A	C	I	R	C
R = responsible A = accountable C = consulted I = informed					

4.1.2 De klantorganisatie relateert bedrijfsrisico's aan IT-diensten

De klantorganisatie analyseert vervolgens de samenhang van de te beheersen kwaliteitsaspecten van bedrijfsprocessen en bedrijfsgegevens met de afgenomen IT-diensten. IT-diensten zijn er in vele soorten en verschijningen. Zonder te pretenderen een volledige taxonomie van IT-diensten te geven, kan men denken aan functionele IT-diensten zoals:

- Connectiviteit: hardware en software voor netwerken, telecommunicatie en communicatiediensten zoals e-mail en telefonie;
- Informatievoorziening: hardware en software voor werkplekken, werkstations en printers;
- Gegevensverwerking: servers en bedrijfsapplicaties;
- Gegevensopslag: opslagmedia, databases en daaraan gerelateerde toepassingen.

De uitkomst van deze stap is een beschrijving van de te beheersen kwaliteitsaspecten (bijvoorbeeld de beschikbaarheid, integriteit en exclusiviteit) van IT-diensten. (Zie voorbeelden in Tabel 3).

RACI-tabel	Business Management	Proces & Informatie Management	Supplier Management	Operational Risk Management	Audit
Stap 2: Relateer risico's aan IT-diensten.	A	R	I	C	C
R = responsible A = accountable C = consulted I = informed					

4.1.3 De klantorganisatie bepaalt de criteria voor risicobeheersing

De klantorganisatie dient vervolgens de criteria te bepalen voor de beheersing van de risico's van de IT-diensten. Criteria kunnen worden voorgeschreven in termen van doelstellingen (principle-based) of in termen van concreet te treffen maatregelen (rule-based)

- Principle-based. Bij principle-based afspraken heeft de serviceorganisatie de vrijheid en verantwoordelijkheid om een mix van maatregelen te bepalen, rekening houdend met de kosten en baten, die passend zijn bij de dreigingen op de dienstverlening van de serviceorganisatie. Principle-based afspraken kunnen een combinatie zijn van kwalitatieve criteria, zoals beheersingsdoelstellingen (beschreven in hoofdstuk 3), en kwantitatieve criteria, zoals service levels voor prestatie-indicatoren (beschreven in hoofdstuk 6 b.v. beschikbaarheidspercentage), statistische criteria (b.v. kans op afwijkingen van de norm) en financiële impact (b.v. schadebedrag).

- Rule-based. Bij rule-based afspraken neemt de klantorganisatie in feite de verantwoordelijkheid (in ieder geval ten dele) voor de kosten en kwaliteit van de risicobeheersing. Het is hierbij van belang dat de klantorganisatie bekend is met de dreigingen in de omgeving van de serviceorganisatie. Rule-based wordt bijvoorbeeld toegepast wanneer de klantorganisatie te maken heeft met specifieke wet- en regelgeving die bepaalde beheersingsmaatregelen voorschrijven;

De uitkomst van deze stap is een beschrijving van de beheersingscriteria voor de IT-diensten (zie voorbeelden in Tabel 3)
- voorgeschreven beheersingsmaatregelen (rule-based);
- beheersingsdoelstellingen (principle-based);
- service levels, statistische criteria en financiële criteria (principle-based).

RACI-tabel	Business Management	Proces & Informatie Management	Supplier Management	Operational Risk Management	Audit
Stap 3: Bepaal mate van beheersing.	A	I	I	R	C
R = responsible A = accountable C = consulted I = informed					

4.1.4 De klantorganisatie stemt de beheersingscriteria af met de serviceorganisatie

Tenslotte dient de klantorganisatie de beheersingscriteria voor de IT-diensten af te stemmen met de klantorganisatie. Deze beheersingscriteria vormen de input voor de serviceorganisatie om invulling te geven aan de eisen aan de risicobeheersing.

RACI-tabel	Business Management	Proces & Informatie Management	Supplier Management	Operational Risk Management	Audit
Stap 4: Stem af met serviceorganisatie.	A	I	R	I	C
R = responsible A = accountable C = consulted I = informed					

Voorbeelden

In de tabel hieronder zijn voorbeelden opgenomen van kwaliteitsaspecten voor respectievelijk bedrijfsprocessen en bedrijfsgegevens en daaraan gerelateerde kwaliteitsaspecten en beheersingscriteria voor IT-diensten.

Voorbeelden kwaliteitsaspecten bedrijfsprocessen en -gegevens (stap 4.1.1)	Voorbeelden kwaliteitsaspecten IT-diensten (stap 4.1.2)	Voorbeelden beheersingscriteria (stap 4.1.3)
De beschikbaarheid van een hulpverlenings- of beveiligingsproces (b.v. brandweer, EHBO).	De beschikbaarheid van telefoniediensten, werkplekken en systemen van de hulpdienst.	Algemene beheersingsdoel-stellingen (zie hoofdstuk 3); Service levels voor beschikbaarheid en continuiteit.
De integriteit van een elektronisch betaalproces.	De integriteit van: de ontwikkel-, test- en productieomgeving van de betaalapplicatie; netwerkverbindingen; pinapparatuur.	Algemene beheersingsdoel-stellingen (zie hoofdstuk 3); Frequentie / aantal / impact van (beveiligings)incidenten en verkeerde wijzigingen.
De beschikbaarheid van financiële gegevens (b.v. voor de jaarrekeningcontrole).	De beschikbaarheid van een ERP-systeem en databases.	Algemene beheersingsdoel-stellingen (zie hoofdstuk 3); Service levels voor beschikbaarheid en backup.
De integriteit van financiële gegevens.	De integriteit van een ERP-systeem, databases en directory service.	Algemene beheersingsdoel-stellingen (zie hoofdstuk 3); Frequentie / aantal / impact van incidenten en verkeerde wijzigingen.
De vertrouwelijkheid van persoonsgegevens (privacy).	De integriteit van de test- en productieomgeving van applicaties met persoonsregistraties. De integriteit van de directory service. De vertrouwelijkheid van de gebruikersdata.	Algemene beheersingsdoel-stellingen (zie hoofdstuk 3); Frequentie / aantal / impact van beveiligingsincidenten.

Tabel 3: Voorbeeld kwaliteitsaspecten en beheersingscriteria voor IT-diensten.

4.2 Werkwijze voor de serviceorganisatie

Nadat de klantorganisatie de beheersingscriteria voor de relevante IT-diensten heeft vastgesteld, is de serviceorganisatie aan zet om invulling te geven aan de beheersingscriteria en te bepalen met welke set van beheersingsmaatregelen aan de beheersingscriteria kan worden voldaan. In onderstaande figuur zijn de uit te voeren stappen voor de serviceorganisatie weergegeven, die in de volgende paragrafen worden beschreven. De serviceauditor zal op hoofdlijnen vergelijkbare stappen doorlopen om de scope van de audit te bepalen. De werkwijze van de serviceorganisatie en van de serviceauditor zullen daarom samen worden beschreven.

Afbeelding 8: Stappenplan voor de serviceorganisatie.

4.2.1 Stem de beheersingscriteria af met de klantorganisatie

De beheersingscriteria voor de IT-diensten worden afgestemd met de klantorganisatie. Deze beheersingscriteria vormen de input voor de serviceorganisatie om invulling te geven aan de eisen aan de risicobeheersing. De klantorganisatie verstrekt informatie over: de IT-diensten die in de scope van de opdracht zitten; de te beheersen kwaliteitsaspecten (bijvoorbeeld de beschikbaarheid, integriteit en exclusiviteit); en de beheersingscriteria (rule-based en/of principle-based, zie paragraaf 4.1.3).

RACI-tabel	Account / Contract Management	Diensten & Proces Management	Service Management (Beheer)	Operational Risk Management	Audit
Stap 1: Stem beheersingscriteria af met klantorganisatie.	AR	C	C	C	I
R = responsible A = accountable C = consulted I = informed					

4.2.2 Bepaal de relevante objecten van de IT-dienst

Doelstelling van deze stap is het inventariseren van de objecten, die relevant zijn voor de beheersingscriteria voor de IT-dienst. Objecten betreffen IT-middelen, IT-organisaties en beheerprocessen. Indien exclusiviteit als beheersingscriterium meespeelt, dan zijn ook de IT-middelen relevant waarop bedrijfsgegevens worden opgeslagen en getransporteerd.

Een serviceorganisatie die een bestaande IT-dienst gaat aanbieden aan een nieuwe klant, zal de objecten mogelijk al in kaart hebben gebracht. Anders dient de serviceorganisatie de IT-dienst eerst te ontwerpen. De gevolgde ontwerpmethodiek en -werkwijzen zijn voor het doel van dit studierapport niet van belang, behalve dat in het ontwerpproces invulling dient te worden gegeven aan de opgegeven beheersingscriteria (hetgeen niet triviaal is!).

De auditor (evenals andere functionarissen van de serviceorganisatie niet belast met het ontwerp, zoals risk managers) dient de ontwerpers, architecten en andere betrokkenen van de serviceorganisatie te bevragen over het ontwerp van de IT-dienst en de gekozen invulling van de beheersingscriteria. Ook kunnen documentatie en beheertools worden geraadpleegd om de relevante objecten te bepalen, zoals:

- Functioneel en technisch ontwerp van de IT-dienst;
- Configuratieschema's;
- Configuration management database (CMDB);
- Geautomatiseerde scanning tools voor de configuratie;
- Organisatieschema's.

Afhankelijk van de gevolgde ontwerpmethodiek en -werkwijzen kan de ontwerpdocumentatie vele verschillende vormen aannemen (of helaas ook afwezig zijn). Hier bestaat het risico voor de auditor dat objecten over het hoofd worden gezien, doordat iedere bron of vorm van documentatie met een ander doel is vervaardigd dan voor de volledige scopebepaling van de auditor.

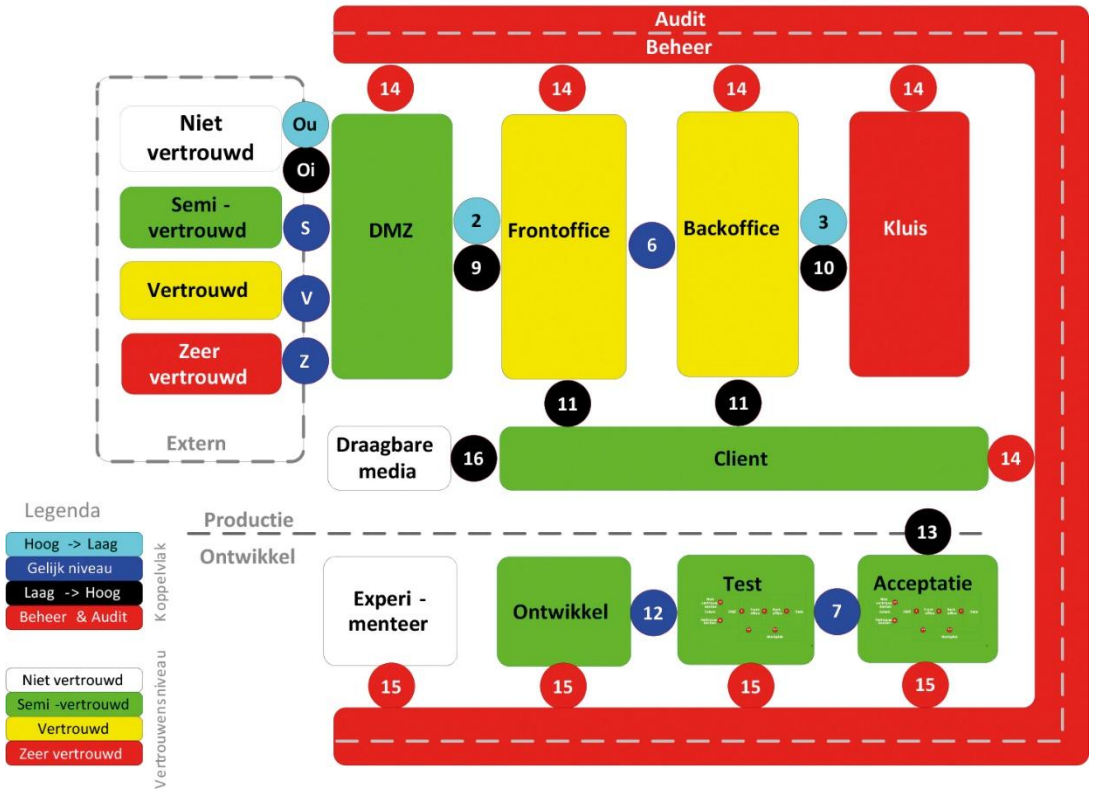
Voor de auditor schetsen we hier daarom een werkwijze, waarbij verschillende attentiepunten of invalshoeken worden beschouwd om informatie te vergaren voor bepaling van de voor de beheersing van de IT-dienst relevante objecten (zie afbeelding 9). De lijst van invalshoeken is niet limitatief.

Afbeelding 9: Invalshoeken voor bepaling van relevante objecten van de IT-dienst.

Invalshoeken (en attentiepunten) voor bepaling van relevante objecten van de IT-dienst (niet limitatief)

- **Applicatiecomponenten en softwarearchitectuur**. De IT-infrastructuur ondersteunt applicaties en data en het is dan ook essentieel om te inventariseren uit welke componenten de applicaties zijn opgebouwd. Applicaties kunnen bestaan uit combinaties van maatwerk en standaardsoftware, uit diverse componenten voor presentatie, rapportage, interfacing (middleware) etc. Daarnaast is ook begrip van de softwarearchitectuur van belang om de samenhang en onderlinge afhankelijkheden van de software op waarde te schatten. Denk bijvoorbeeld aan het gebruik van een centrale diensten voor de toegangsbeveiliging of scheduling. Met deze kennis kan vervolgens de bijbehorende IT-infrastructuur en general IT controls in kaart worden gebracht die relevant zijn voor de applicaties.

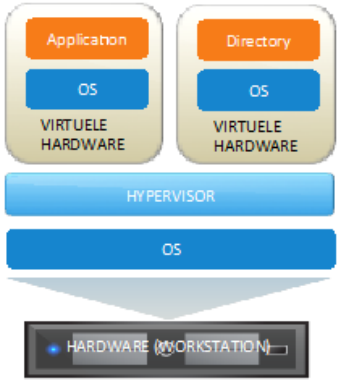
- **Samenhang van IT-middelen**. Beschouw de samenhang van de IT-middelen (top-down), alvorens gedetailleerd individuele IT-middelen te beschouwen. Begrip van de samenhang kan leiden tot een meer gericht, en dus effectiever en efficiënter, onderzoek van de afzonderlijke IT-middelen. Het in [2] beschreven beschouwings-model voor zonering (afbeelding 10) en in [2] beschreven patronen voor informatie-beveiliging kunnen de auditor richting geven bij het in kaart brengen van de IT-configuratie, bij het onderzoeken van de samenhang van de IT-middelen, en bij het beoordelen van de IT-configuratie. Zo worden "single points of failure" opgespoord in het kader van de beschikbaarheid; de mogelijke toegangspaden tot systemen worden duidelijk; en bepaalde risico's kunnen per zone worden onderzocht in plaats van per IT-middel.



Afbeelding 10: Beschouwingsmodel voor zonering (bron: PvIB [2]).

- **Toegangspaden**. Breng de gebruikelijke en mogelijke paden in kaart voor toegang van a) gebruikers naar bedrijfsgegevens, b) beheerders naar IT-middelen en c) applicaties naar applicaties.
  Afbeelding 10 kan hierbij worden gebruikt als hulpmiddel om systematisch de diverse toegangspaden te evalueren. De genummerde cirkels in de afbeelding geven de koppelvlakken weer tussen zones.

- **Fysieke en logische IT-middelen (virtualisatie en 'stack').** Een IT-middel kan uit meerdere deelsystemen bestaan, zoals operating system, DBMS, access control system, scheduler etc. (de 'stack'). Beschouw naast de logische IT-middelen ook de fysieke vorm en de fysieke locaties. Bij virtualisatie zijn er ondersteunende IT-middelen, zoals een onderliggend besturingssysteem en hypervisor.



Afbeelding 11: Een voorbeeld van virtualisatie en 'stack'.

- **Redundante IT-middelen**. Redundante IT-middelen, waarmee de IT-dienst in bijzondere gevallen (b.v. bij uitwijk, nood, ondercapaciteit) wordt geleverd, worden nog al eens over het hoofd gezien. Beschouw hierbij ook IT-middelen waarop reserve kopieën van bedrijfsgegevens zijn opgeslagen (backups, gemirrorde versies).

- **Generieke IT-middelen**. Beschouw het belang van generieke IT-middelen op de beheersingscriteria van de IT-dienst. Generieke IT-middelen zijn middelen waarvan de IT-dienst gebruik maakt, maar die zelf geen gegevens van de klant verwerken. Bijvoorbeeld: domain name service (DNS), DHCP service (uitgifte van dynamische IP-adressen), identity services, stepping stones, etc. Ook IT-middelen die de IT-beheerprocessen ondersteunen. Te denken valt aan IT-middelen voor registratie, logging, signalering, geautomatiseerde besturing, workflow en documentatie.

- **De OTA-omgeving**. Denk aan IT-middelen waarmee de IT-dienst wordt ontwikkeld, getest en geaccepteerd (OTA-omgeving). Deze IT-middelen kunnen van belang zijn bij het waarborgen van de integriteit van de IT-dienst.

- **IT-organisaties, functies en locaties**. Bepaal welke IT-organisaties, afdelingen en functies relevant zijn voor de beheersingscriteria van de IT-dienst. Denk aan **derde partijen** (subserviceorganisaties) aan wie delen van de IT-dienst zijn uitbesteed; evenals aan **generieke functies**, bijvoorbeeld: procesmanagement (administratieve organisatie), kwaliteitsmanagement, operationeel risicomanagement (security management) en personeelsmanagement (screening en opleiding van personeel).

De uitkomst van deze stap is een inventarisatie van de relevante objecten van de IT-dienst.

RACI-tabel	Account / Contract Management	Diensten & Proces Management	Service Management (Beheer)	Operational Risk Management	Audit
Stap 2: Bepaal relevante objecten van de IT-dienst.	A	C	C	R	I
R = responsible A = accountable C = consulted I = informed					

4.2.3 Bepaal de relevante algemene beheersingsmaatregelen van de IT-dienst

Na het inventariseren van de relevante objecten dient de serviceorganisatie activiteiten van risicobeheersing (*risk management*) uit te voeren. Deze activiteiten zijn onderdeel van het beheerproces Security Management (zie sectie 6,3), dat er voor zorgt dat de risicobeheersing periodiek wordt herhaald, zodat het stelsel van beheersingsmaatregelen actueel blijft.

De serviceauditor doorloopt een vergelijkbaar traject als de serviceorganisatie ter vaststelling van de beheersingscriteria voor de IT-dienst en ter toetsing van het ontwerp van het stelsel van beheersingsmaatregelen.

Hoewel de methodiek van risicoanalyse geen onderwerp van dit studierapport is, omvatten de *risk management* activiteiten op hoofdlijnen de volgende stappen:

- **Inventarisatie van bedreigingen en kwetsbaarheden voor de IT-dienst**. Welke bedreigingen en kwetsbaarheden (risico's) zijn er voor de beheersingscriteria van de klantorganisatie en voor de gerelateerde IT-beheersingsdoelstellingen?

  Bedreigingen en kwetsbaarheden kunnen *specifiek* van aard zijn, dat wil zeggen dat ze specifiek van toepassing zijn op de serviceorganisatie door de omstandigheden van de serviceorganisatie. Bijvoorbeeld: risico's van natuurrampen door de geografische ligging; of risico's van continuïteit door het in hoge mate afhankelijk zijn van een

subserviceorganisatie; of risico's van schending van de vertrouwelijkheid door het bedienen van concurrerende klantorganisaties door hetzelfde personeel.

Voor *algemene* bedreigingen en kwetsbaarheden van IT-diensten kunnen de beheersingscriteria in hoofdstuk 5 en hoofdstuk 6 als startpunt worden gebruikt van wat er mogelijk fout kan gaan ten aanzien van IT-middelen en IT-beheerprocessen. De beheersingsmaatregelen zijn immers gericht op het mitigeren van beheersingsrisico's.

- **Inschatting van kans en impact van risico's.** Schat per risico de kans van optreden en de impact op de IT-dienst in. Deze inschatting van risico's bepaalt de mate waarin elk van de objecten (IT-middelen, IT-beheerprocessen, IT-organisatie) van belang is voor het realiseren van de beheersingscriteria. Indien men prioriteiten wilt of moet aanbrengen in de risicobeheersing, bijvoorbeeld bij budgettaire beperkingen voor implementatie van beheersingsmaatregelen of voor audits, biedt deze inschatting van risico's een leidraad.

- **Selectie van maatregelen.** De serviceorganisatie selecteert vervolgens een passend stelsel van beheersingsmaatregelen om de kans en/of impact van de risico's te mitigeren. De uitkomst van deze stap is in feite het beveiligingsontwerp, waarop wordt gedoeld in norm 3 van het beheerproces Security Management, zie sectie 6,3.
  Bij het selecteren van maatregelen kan het beste de volgende top-down benadering worden aangehouden, omdat bij deze benadering minder overbodige maatregelen worden geselecteerd op individueel objectniveau voor risico's die al zijn afgedekt op een samenhangend niveau.

  - Ten eerste de rule-based beheersingsmaatregelen die zijn voorgeschreven door de klantorganisatie;

  - Ten tweede een stelsel van beheersingsmaatregelen om aan de principle-based criteria te voldoen, mede op basis van kosten en baten.

    - Hierbij eerst de beheersingsmaatregelen die betrekking hebben op het geheel van de dienstverlening en op de samenhang van objecten, b.v. zonering en redundantie van de gehele IT-configuratie; fysieke beveiliging van het rekencentrum; en generieke IT-beheerprocessen zoals security en change management.

    - Tenslotte de beheersingsmaatregelen van individuele objecten.

De uitkomst van deze stap is een beschrijving van alle, voor de risicobeheersing relevante, beheersingsmaatregelen van de IT-dienst.

RACI-tabel	Account / Contract Management	Diensten & Proces Management	Service Management (Beheer)	Operational Risk Management	Audit
Stap 4: Bepaal maatregelen.	A	R	C	C	I
R = responsible A = accountable C = consulted I = informed					

4.2.4 Stem de beheersingsmaatregelen af met de klantorganisatie.

De serviceorganisatie heeft een belangrijke verantwoordelijkheid om de risico's van de eigen dienstverlening te beheersen en maakt hiertoe, mede op basis van bedrijfseconomische gronden, een keuze uit verschillende mogelijke maatregelen. Zeker in die gevallen dat een serviceorganisatie aan meerdere klantorganisaties dezelfde dienst levert, zal de service-organisatie deze keuze het liefst zelf willen bepalen.

De serviceorganisatie kan echter de risico's van de klantorganisaties, die samenhangen met het gebruik van de IT-dienst, niet geheel inschatten. Verder kan ook de serviceorganisatie geen absolute zekerheid verschaffen over de beheersing van risico's. Om deze redenen is het aan te bevelen om het te treffen stelsel van beheersingsmaatregelen af te stemmen met de klantorganisaties.

Voor de afstemming van dit stelsel van beheersingsmaatregelen, al dan niet via auditors en hun auditrapportages, is het nodig om de IT-dienst en de relevante beheersingsmaatregelen op een inzichtelijke manier te beschrijven. Zo een beschrijving kan op verschillende manieren en mate van diepgang worden vormgegeven en kan onder meer afhangen van de complexiteit van de IT-dienst en de situatie. Het beschrijven van de uitkomsten en afwegingen van de in dit hoofdstuk beschreven inventarisatie (paragraaf 4.2.2) en selectie van maatregelen op basis van risicoanalyse (paragraaf 4.2.3) zal de afstemming met de klantorganisatie vergemakkelijken.

RACI-tabel	Account / Contract Management	Diensten & Proces Management (Bouw)	Service Management (Beheer)	Operational Risk Management	Audit
Stap 5: Stem maatregelen af met klantorganisatie.	AR	C	C	C	I
R = responsible A = accountable C = consulted I = informed					

5 Algemene IT-beheersingsmaatregelen met technische instellingen

Onder algemene IT-beheersingsmaatregelen met technische instellingen verstaan we de technische beheersingsmaatregelen die zijn ingebed in het technische ontwerp van de IT-dienst en die *algemeen* werkzaam zijn voor applicaties die gebruik maken van die infrastructuur. Deze maatregelen betreffen de eigenschappen van de totale technische configuratie door de functies die de IT-middelen hebben voor de configuratie. Algemene IT-beheersingsmaatregelen in technische instellingen zijn onder te verdelen in:

- Technische beheersingsmaatregelen in de IT-configuratie, die zijn ingebed in de samenhang van de IT-configuratie;
- Technische beheersingsmaatregelen in de afzonderlijke IT-middelen.

Buiten scope

Geprogrammeerde beheersingsmaatregelen die te maken hebben met functionaliteit worden in dit werk buiten beschouwing gelaten, omdat ze worden gerekend tot *application controls* (zoals invoer-, verwerking- en uitvoercontroles) respectievelijk tot van specifieke functionaliteiten van IT-middelen. In dit werk richten we ons op *algemene IT beheersingsmaatregelen* en dus niet op functionaliteit, noch van applicaties noch van technische infrastructuur (zoals print-, communicatie-, opslag-, verwerkingsfuncties etc.).

Technische beheersingsmaatregelen in de IT-configuratie

Technische beheersingsmaatregelen die zijn ingebed in de *samenhang* van de IT-configuratie zijn onder te verdelen in:

- Zonering;
- Redundantie;
- Identificatie, authenticatie, autorisatie;
- Logging;
- Signalering.

Bepaalde maatregelen van identificatie, authenticatie, autorisatie, logging en signalering kunnen ofwel per IT-middel worden geïmplementeerd, ofwel centraal voor de gehele configuratie. Bij een centrale implementatie moeten de afzonderlijke IT-middelen een koppeling maken met de centrale functie. Voorbeelden zijn: een centrale directory/autorisatie service; "single sign-on"; en een centrale logserver.

Technische beheersingsmaatregelen in de IT-middelen

Technische beheersingsmaatregelen die zijn ingebed in de afzonderlijke IT-middelen. Deze maatregelen betreffen de eigenschappen van afzonderlijke IT-middelen door hun technische configuratie. Deze maatregelen zijn onder te verdelen in:

- Identificatie, authenticatie en autorisatie;
- Logging;
- Signalering.

Bepaalde maatregelen van identificatie, authenticatie, autorisatie, logging en signalering kunnen ofwel per IT-middel worden geïmplementeerd, ofwel centraal voor de gehele configuratie. Bij een centrale implementatie moeten de afzonderlijke IT-middelen een koppeling maken met de centrale functie. Voorbeelden zijn: een centrale directory/autorisatie service; "single sign-on"; en een centrale logserver.

In de volgende paragrafen worden de technische beheersingsmaatregelen in de IT-configuratie, respectievelijk IT-middelen, apart gegroepeerd.

5.1 Zonering

5.1.1 Definitie

Zonering is een beveiligingsconcept, waarbij de infrastructuur in afgebakende onderdelen – de zones – wordt verdeeld met elk een eigen risicoprofiel en een eigen, aan het risicoprofiel gerelateerd, stelsel van beheersingsmaatregelen.

5.1.2 Toelichting en afbakening

Het doel van zonering als maatregel van risicobeheersing is enerzijds het delen van een gemeenschappelijk stelsel van beheersingsmaatregelen (beperking van kosten) en anderzijds isolatie van risico's. Zonering wordt veel toegepast in omgevingen waarin onderdelen met verschillende risicoprofielen naast elkaar bestaan. Denk bijvoorbeeld aan:

- aparte omgevingen voor ontwikkeling, test, acceptatie en productie;
- externe onvertrouwde zones (b.v. internet) naast interne vertrouwde zones (b.v. intranet);
- verschillende vestigingen of afdelingen van een organisatie, om te voorkomen dat bedreigingen en incidenten die optreden in een deel van de infrastructuur, doorwerken in een ander deel van de infrastructuur;
- aparte zone (kluis) voor opslag van vertrouwelijke data met bijvoorbeeld dataencryptie als zoneringsmaatregel.

Zonering maakt het hierbij mogelijk om een gemeenschappelijk stelsel van beheersings-maatregelen te hebben per zone, toegespitst op het risicoprofiel van de zone. Zonder zonering zouden de (zwaarste) maatregelen voor het hoogste risicoprofiel op de gehele omgeving moeten worden toegepast.

Met zonering hangt het begrip "filtering" samen en deze begrippen worden vaak samen genoemd. Indien gegevensuitwisseling nodig is tussen een zone en de buitenwereld, dienen gecontroleerde koppelvlakken te worden ingericht. De controle van de gegevensuitwisseling op de koppelvlakken wordt ook wel filtering genoemd en kan gericht zijn tegen Denial of Service attacks, indringers, ongewenste inhoud, virussen en informatie lekkage.

5.1.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
A	De inrichting van de IT-middelen dient te worden beperkt tot de strikt noodzakelijke en geautoriseerde functionaliteit.
B	Toegang tot en gebruik van IT-diensten dient te worden beperkt tot geautoriseerde gebruikers en beheerders
H	De IT-dienst dient te worden beschermd tegen verstoringen door onjuiste wijzigingen en door ontwikkel- en testactiviteiten.

5.1.4 Beheersingsmaatregelen

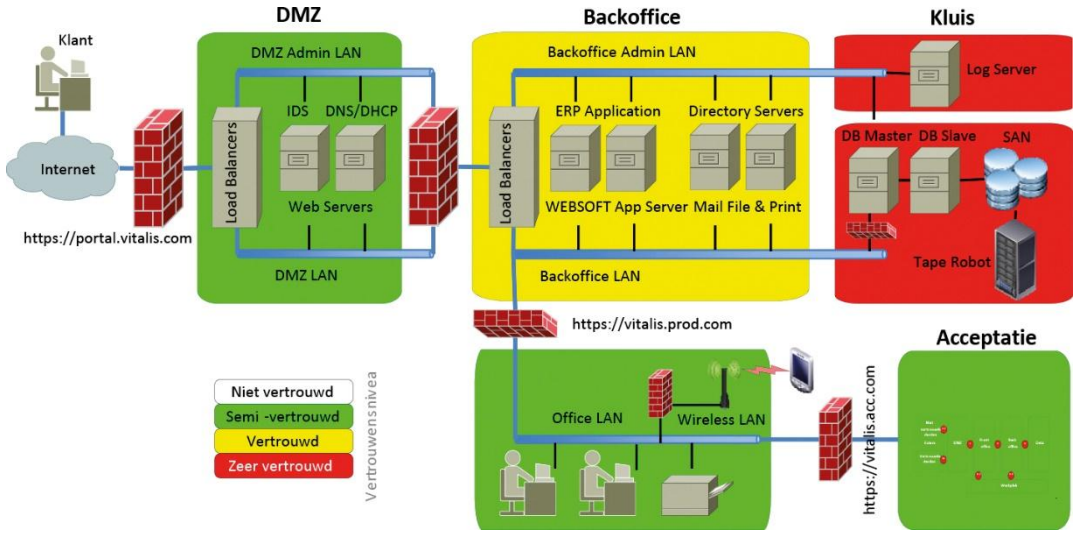
Technische beheersingsmaatregelen in de IT-configuratie

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Beheer van de zonering				
01	Elke zone wordt beheerd onder verantwoordelijkheid van slechts één beheerinstantie.	X	A B H	Technisch ontwerp. Instellingen van gebruikers en rechten per zone.
02	Beheer en controle van zones vinden plaats vanuit een aparte zone.	X	A B H	Technisch ontwerp. Configuratieschema.
03	Werkstations kunnen op één moment uitsluitend aan één zone zijn gekoppeld.		A B H	Technisch ontwerp werkstations.
Criteria voor de zonering				
04	Het beveiligingsniveau van een zone wordt bepaald door de gegevens met het hoogste risicoprofiel in die zone.	X	A B	Technisch ontwerp
05	Gegevens met een sterk verschillend risicoprofiel of gebruikersgroep worden in aparte zones ondergebracht, voor zover bedrijfseconomische en technisch zinvol en mogelijk.		A B	Functioneel e/of Technisch ontwerp

06	Voor de IT-dienst zijn aparte zones ingericht voor Ontwikkeling, Test, Acceptatie en Productie.	X	H	Technisch ontwerp. Configuratieschema.
Gegevensuitwisseling tussen zones (filtering)				
07	Gegevensverkeer tussen zones vindt uitsluitend plaats via gedefinieerde koppelvlakken; van koppelvlakken tussen zones zijn de richting en de poorten (systeemservices) waarover gecommuniceerd worden, exact benoemd (verkeersstromenmatrix).	X	A B H	Technisch ontwerp (verkeersstromenmatrix). Configuratieschema. Technische instellingen koppelvlakken (poorten en verkeersstromenmatrix).
08	Gegevens die zich buiten de zone begeven en waarvan de vertrouwelijkheid en integriteit van belang zijn, waaronder gegevens van beheersessies, worden vercijferd; het encryptiemechanisme waarborgt de vertrouwelijkheid van de vercijfersleutels.		A B	Technisch ontwerp. Technische instellingen communicatieprotocol koppelvlak.
09	Gegevensverkeer vanuit onvertrouwde zones wordt op de koppelvlakken geïnspecteerd op schadelijke inhoud waaronder: inbraakpogingen (Intrusion Detection and Prevention); bovenmatig capaciteitsbeslag (Denial-of-Service aanvallen); en computervirussen (antivirusprogrammatuur).	X	A B	Technisch ontwerp (van IDS / antivirus). Technisch instellingen (van IDS / antivirus)
10	Voor de inspectie van gegevensverkeer vanuit onvertrouwde zones worden producten van verschillende leveranciers toegepast.		A B	Technisch ontwerp.
11	De IT-dienst beperkt en/of signaleert overmatig gebruik door een enkele gebruiker of systeem die de algemene beschikbaarheid van de IT-dienst in gevaar kan brengen (Denial-of-Service).		A B	Technische instellingen en scripts logging en signalering.

Voorbeeld uit casus VITALIS

Leverancier SCCS van VITALIS onderkent een aantal netwerkzones, waaronder een acceptatie- en productieomgeving. Deze zones worden gerealiseerd door firewalls en routers. Alle beheersingsmaatregelen voor zonering worden door SCCS toegepast.



5.2 Redundantie

5.2.1 Definitie

Redundantie van IT-middelen is de techniek van het inrichten van extra capaciteit, zodat bij uitval van een enkele IT-component de IT-dienst beschikbaar blijft.

5.2.2 Toelichting en afbakening

Redundantie van IT-middelen is gericht op het waarborgen van de beschikbaarheid van de IT-dienst, door het voorkomen van zogenaamde “single points of failure”. Op verschillende manieren kan redundantie van IT-middelen worden bereikt:

- de redundante IT-middelen kunnen standby staan en bij uitval van de primaire IT-middelen worden geactiveerd (b.v. reserve onderdelen, uitwijkcentrum, databackup);
- de redundante IT-middelen kunnen actief meedraaien met de primaire IT-middelen (load balancing, mirroring, disjuncte netwerkpaden).

5.2.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
C	De IT-dienst dient onder de benoemde bedrijfsomstandigheden een overeengekomen werklast te kunnen verwerken.
D	De IT-dienst dient, in geval van benoemde typen afwijkende bedrijfsomstandigheden (calamiteiten), tijdig herstelbaar te zijn om een overeengekomen werklast te kunnen verwerken.

5.2.4 Beheersingsmaatregelen

Technische beheersingsmaatregelen in de IT-configuratie

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Redundantie				
01	De middelen van de IT-dienst zijn redundant uitgevoerd, voor zover bedrijfseconomisch en technisch zinvol en mogelijk (beperking van single-points-of-failure).	X	C	Technisch ontwerp. Configuratieschema.
02	Er zijn reservekopieën (back-ups / mirroring) en routines voor back-up en restore voor software van de IT-dienst (databestanden, instellingen en programmatuur).	X	C D	Procedures, scripts en logs voor back-up en restore(tests).
03	Redundante middelen van de IT-dienst zijn fysiek gescheiden. Reservekopieën van de software zijn fysiek gescheiden opgeslagen van de primaire versies.	X	C D	Schema's van fysieke configuraties van datacenter(s), hardware en netwerken.
04	De IT-dienst beschikt over automatisch werkende mechanismen om redundante middelen te activeren (automatic fail-over, load balancing).		C	Technisch ontwerp. Technische instellingen en testresultaten van failover.
05	Beheer van de IT-dienst is niet gebonden aan één fysieke locatie.		C D	

Voorbeeld uit casus VITALIS

Beschikbaarheidseis van 99% en een hersteltijd van 48 uur zijn niet bijzonder stringent. Wat technische beheersingsmaatregelen betreft kan SCCS daarom volstaan met de implementatie van maatregelen 02 en 03 in bovenstaande tabel. Daarnaast zijn wel beheersingsmaatregelen van beheerprocessen (availability en continuity management) nodig om een tijdig herstel te ondersteunen.

5.3 Identificatie, Authenticatie & Autorisatie

5.3.1 Definitie

Identificeren is het bekend maken van de identiteit van personen of systemen aan een IT-dienst. Authenticeren is het aantonen dat de persoon of het systeem ook daadwerkelijk degene is die zich identificeert. Autoriseren is het toekennen van rechten voor toegang tot systeemfuncties en/of gegevens.

5.3.2 Toelichting en afbakening

Identificatie, authenticatie en autorisatie zijn van belang voor: het handhaven van functiescheidingen; het herleiden van handelingen in systemen tot personen of systemen; en het beperken van de toegang tot systemen en gegevens. Soms worden handelingen (transacties) in systemen uitgevoerd door systemen (via batchverwerking met produktie-accounts) of door beheerders in opdracht van klanten of gebruikers: we spreken dan van productieopdrachten.

5.3.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
B	Toegang tot en gebruik van IT-diensten dient te worden beperkt tot geautoriseerde gebruikers en beheerders.
J	Productieopdrachten dienen te worden geautoriseerd.

5.3.4 Beheersingsmaatregelen

Technische beheersingsmaatregelen in de IT-configuratie

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Identificatie				
01	Voor het identificeren van gebruikers, beheerders en productie-accounts gelden naamgevingconventies ter bevordering van de onderhoudbaarheid van het beheer.		B	Naamgevingsconventies.
02	De registratie van gebruikers is zoveel mogelijk centraal geregeld ter bevordering van de onderhoudbaarheid van het beheer (centrale directory service).	X	B	Technisch ontwerp / beveiligingsarchitectuur / Configuratieschema.
03	Toegang voor beheerders tot IT-middelen is alleen mogelijk na aanmelding in een aparte zone (stepping stone).		B	
Authenticatie				
04	Vanuit onvertrouwde zones worden gebruikers minimaal geauthentiseerd op basis van twee authenticatiefactoren b.v. kennis en bezit. Voor het uitvoeren van beheerhandelingen is het vierogenprincipe een alternatief voor een tweede authenticatiefactor.	X	B	Technische instellingen van toegangsbeveiliging (policies).
05	Voor het inloggen vanuit een niet-vertrouwde zone wordt een maximumtijd en een minimumtijd vastgesteld; indien deze tijd wordt overschreden, beëindigt het systeem het inlogproces.		B	Technische instellingen van toegangsbeveiliging (policies).
Autorisatie				
06	Voor het inrichten van toegangsrechten gelden naamgevingconventies en een systematiek van toegangsrechten per gebruikersgroep en/of rol ter bevordering van de onderhoudbaarheid van het beheer.		B	Naamgevingsconventies en ontwerp autorisatiebeheer. (Partiële) uitdraai van autorisaties.

07	De registratie van toegangsrechten is zoveel mogelijk centraal geregeld ter bevordering van de onderhoudbaarheid van het beheer (centrale directory service).		B	Technisch ontwerp / beveiligingsarchitectuur / Configuratieschema.
08	In de productieomgeving zijn er geen hulpmiddelen om bedrijfsapplicaties en bedrijfsgegevens te benaderen buiten de geautoriseerde toegangspaden om (b.v. bestandsviewers, editors, compilers).		B	Uitdraai van tools in productieomgeving.

Technische beheersingsmaatregelen in de IT-middelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Identificatie				
01	Gebruikers (inclusief beheerders) worden geïdentificeerd door hun unieke gebruikersnaam. Groepsaccounts zijn alleen toegestaan met leesrechten tot niet-vertrouwelijke informatie.	X	B	Technisch ontwerp. Technische instellingen van toegangsbeveiliging (gebruikers, groepen).
02	Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account).	X	B J	Technisch ontwerp. Technische instellingen van toegangsbeveiliging (gebruikers, groepen).
03	Generieke beheeraccounts (root, administrator) zijn geblokkeerd of alleen te gebruiken onder registratie en toezicht (zoals gebruik via individuele accounts (substitute user), gesloten-enveloppeprocedure, vierogenprincipe door gesplitste wachtwoorden). .		B	Technische instellingen van toegangsbeveiliging (gebruikers, groepen).
04	Beheerders voeren werkzaamheden als beheerder en werkzaamheden als gewone gebruiker onder twee verschillende gebruikersnamen uit.		B	Technische instellingen van toegangsbeveiliging (gebruikers, groepen, rechten).

05	De geldigheid van gebruikersnamen van tijdelijke gebruikers wordt beperkt door expiratiedata in het systeem.		B	Technische instellingen van toegangsbeveiliging (policies).
Authenticatie				
06	Binnen vertrouwde zones worden gebruikers minimaal geauthentiseerd op basis van één authenticatiefactor b.v. kennis (wachtwoord) of bezit (pas).	X	B	Technische instellingen van toegangsbeveiliging (policies).
07	Het systeem dwingt zodanige wachtwoorden af, dat wachtwoorden niet binnen redelijke tijd kunnen worden achterhaald met huidige geautomatiseerde hulpmiddelen. Bijvoorbeeld door middel van regels voor: minimumlengte; combinatie van numerieke, alfanumerieke, hoofdletters en bijzondere tekens; beperking van hergebruik van historische wachtwoorden; minimaal verschil met voorgaande wachtwoorden).	X	B	Technische instellingen van toegangsbeveiliging (policies).
08	De default en installatiewachtwoorden worden tijdens of direct na installatie verwijderd of gewijzigd.	X	B	Technische instellingen van toegangsbeveiliging (gebruikers, groepen).
09	Gebruikers en beheerders hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen.	X	B	Technische instellingen van toegangsbeveiliging (policies).
10	Initiële wachtwoorden en wachtwoorden die gereset zijn, voldoen aan de wachtwoordconventies en daarbij wordt door het systeem afgedwongen dat bij het eerste gebruik dit wachtwoord wordt gewijzigd.	X	B	Technische instellingen van toegangsbeveiliging (policies).
11	Automatisch aanmelden, zonder dat de gebruiker binnen de sessie een wachtwoord wordt ingegeven, is niet toegestaan voor interactieve gebruikers.		B	Technische instellingen van toegangsbeveiliging (policies).
12	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.		B	Technische instellingen van toegangsbeveiliging (policies).

13	Voordat een geslaagde aanmelding op een systeem heeft plaatsgevonden toont het systeem uitsluitend informatie die noodzakelijk is voor de aanmelding.		B	Technische instellingen van toegangsbeveiliging (policies).
14	Wachtwoorden worden niet getoond op het scherm tijdens het ingeven van het wachtwoord. Het is wel toegestaan dat toetsaanslagen worden weergegeven door een algemeen teken.	X	B	Foto/screenshot van aanlogscherm.
15	Nadat voor een gebruikersnaam een ingesteld aantal keer een foutief wachtwoord is gegeven, wordt de gebruikersnaam geblokkeerd gedurende een ingestelde of onbeperkte termijn.	X	B	Technische instellingen van toegangsbeveiliging (policies).
16	Zodra een inlogproces succesvol is voltooid, wordt de datum en tijd van de voorgaande succesvolle login getoond.		B	Foto/screenshot van melding / Technische instellingen.
17	Wachtwoorden worden versleuteld over het netwerk verzonden.	X	B	Technische instellingen / technische documentatie van systeemeigenschappen.
18	Opgeslagen wachtwoorden worden one-way versleuteld.	X	B	Technische instellingen / technische documentatie van systeemeigenschappen.
19	Na een ingestelde periode van inactiviteit wordt de informatie op het beeldscherm onleesbaar gemaakt, waarna de gebruiker zich opnieuw dient te authentiseren (b.v. door middel van een screensaver),	X	B	Technische instellingen van toegangsbeveiliging (policies).
Autorisatie				
20	Toegangsbeveiliging is geïmplementeerd volgens het principe “niets mag, tenzij nodig” op alle IT-middelen.	X	B	Autorisatiebeleid, -matrix en -instellingen.
21	Gebruikers krijgen alleen beschikking over commando’s / functies waartoe zij zijn geautoriseerd (geen algemene commando-omgeving). Beheertaken verlopen zoveel mogelijk via een menusysteem.		B	Technische instellingen / gebruikersprofielen en aanlogroutines.

22	Toepassingen mogen niet onnodig en niet langer dan noodzakelijk met bijzondere privileges draaien.		B J	
23	Rechten van generieke beheeraccounts (root, administrator) zijn gescheiden over verschillende functies zodanig dat interne controle mogelijk is (functiescheiding).		B	Technische instellingen van toegangsbeveiliging (gebruikers, groepen).

Voorbeeld uit casus VITALIS

In deze casus zijn er verschillende typen gebruikers:

- Vanaf Internet: klanten, medewerkers VITALIS;

- Vanaf SCCS: beheerders.

Vanwege de vertrouwelijkheid van de klantgegevens (medische en betaalgegevens) dienen gebruikers naast gebruikersnaam en wachtwoord nog een tweede factor voor authenticatie toe te passen (criterium 04 in bovenstaande tabel).

5.4 Logging

5.4.1 Definitie

Logging (vastleggen van gebeurtenissen) betreft het geautomatiseerd vastleggen door de IT-middelen van gegevens over de toestand van de IT-middelen en over het gebruik van IT-middelen.

5.4.2 Toelichting en afbakening

Het vastleggen van gebeurtenissen over de toestand en het gebruik van IT-middelen is noodzakelijk om achteraf controle te kunnen uitoefenen en/of om foutsituaties te kunnen uitzoeken. Verder kunnen de vastleggingen dienen als basis voor automatische alarmering en rapportage (zie ook de volgende sectie over signalering). Het gebruik van de vastleggingen en rapportages vindt grotendeels plaats als onderdeel van de IT-beheerprocessen, zoals Capacity, Availability, Access en Operations Management (hoofdstuk 6).

Het vastleggen kan tevens noodzakelijk zijn als bewijsmiddel voor private- of strafrechtelijke vordering. Het betreft hier het vastleggen van handelingen van natuurlijke personen (gebruik) en gebeurtenissen in systeemsoftware en hardware (toestand), zoals capaciteitsbeslag, activering, storingen en andere gebruikstoestanden.

Het vastleggen van gebeurtenissen die behoren bij toepassingssystemen (audit-trails) vallen buiten de reikwijdte van vastleggingen in het kader van de algemene beheersingsmaatregelen, waar we het hier over hebben. Die categorie van vastleggingen valt onder de geprogrammeerde controles of application controls.

5.4.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
B	Toegang tot en gebruik van IT-diensten dient te worden beperkt tot geautoriseerde gebruikers en beheerders.
L	Relevante gebeurtenissen van beheer, gebruik en (dreigende) verstoring van de IT-dienst dienen te worden vastgelegd.

5.4.4 Beheersingsmaatregelen

Technische beheersingsmaatregelen in de IT-configuratie

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Logging				
01	Loggegevens worden centraal opgeslagen in een aparte (audit)zone, gescheiden van de IT-middelen waarop de logging betrekking heeft.	X	L	Technisch ontwerp Technische instellingen en scripts voor logging
02	Systeemklokken worden regelmatig gesynchroniseerd met een atoomklok.		L	Technische instellingen.
03	De volledigheid van de logbestanden is vast te stellen (bijvoorbeeld met behulp van opeenvolgende nummers van gebeurtenissen).	X	L	Overzicht van opeenvolgende logfiles en inhoud van logs.
04	Uitsluitend geautoriseerde processen mogen logregels schrijven.	X	L	Technische instellingen / baseline.
05	De toegang tot logbestanden is beperkt tot leesrechten.	X	L	Technische instellingen / baseline.

06	Beheerders hebben niet de toegangsrechten om de instellingen van de logging te wijzigen of logbestanden te verwijderen (tenzij het specifiek hiervoor bevoegde beheerders zijn en de gebruikte techniek geen automatisch beheer ondersteunt).	X	L	Technische instellingen / baseline / Instellingen van gebruikers en rechten per zone.
07	Loginformatie wordt bewaard en is toegankelijk (achterwaartse compatibiliteit) totdat de bewaartermijnen verstreken zijn. De bewaartermijn is afgestemd op de eisen van wet- en regelgeving en op de controle- en auditcyclus van de betreffende gegevens.	X	L	Technische instellingen en scripts voor logging.

Technische beheersingsmaatregelen in de IT-middelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Logging				
01	Gebeurtenissen over het verloop van productieopdrachten en van beheer van de IT-diensten zijn gedefinieerd en worden geregistreerd. De volgende typen gebeurtenissen worden geregistreerd: • Gebruik van technische beheerfuncties; • Gebruik van functionele beheerfuncties; • Handelingen van beveiligingsbeheer; • Beveiligingsovertredingen; • Verstoringen in het productieproces; • Handelingen van systeemtoegang; • Toegang tot gebruikersbestanden door beheerders; • Het vollopen van het opslagmedium voor de logbestanden; • Het overschrijven of verwijderen van logbestanden (dit wordt gelogd in de nieuw aangelegde log).	X	B L	Technisch ontwerp. Technische instellingen en scripts voor logging. Logs.

02	De volgende informatie wordt per gebeurtenis geregistreerd: • De gebruikersnaam die de gebeurtenis initieerde; • Het soort gebeurtenis; • Het werkstation of locatie waarvandaan de gebeurtenis werd geïnitieerd; • Het object waarop de gebeurtenis optrad; • Het resultaat van de gebeurtenis; • Datum en tijdstip van de gebeurtenis. Er worden geen vertrouwelijke gegevens geregistreerd over beveiligingsmaatregelen.	X	B L	Technisch ontwerp. Technische instellingen en scripts voor logging. Logs.
03	De volledigheid van de logbestanden is vast te stellen (bijvoorbeeld met behulp van opeenvolgende nummers van gebeurtenissen).	X	L	Overzicht van opeenvolgende logfiles en inhoud van logs.
04	Uitsluitend geautoriseerde processen mogen logregels schrijven.	X	L	Technische instellingen / baseline.
05	De toegang tot logbestanden is beperkt tot leesrechten.	X	L	Technische instellingen / baseline.
06	Beheerders hebben niet de toegangsrechten om de instellingen van de logging te wijzigen of logbestanden te verwijderen (tenzij het specifiek hiervoor bevoegde beheerders zijn en de gebruikte techniek geen automatisch beheer ondersteunt).	X	L	Technische instellingen / baseline / Instellingen van gebruikers en rechten per zone.
07	Loginformatie wordt bewaard en is toegankelijk (achterwaartse compatibiliteit) totdat de bewaartermijnen verstreken zijn. De bewaartermijn is afgestemd op de eisen van wet- en regelgeving en op de controle- en auditcyclus van de betreffende gegevens.	X	L	Technische instellingen en scripts voor logging.

Voorbeeld uit casus VITALIS

Voor VITALIS is de relevantie van logging onderkend. Er is dan ook sprake van een specifieke kluis. Gegeven de gevoeligheid van de dienst en de traceerbaarheid van acties, zijn alle beheersingscriteria van toepassing.

5.5 Signalering

5.5.1 Definitie

Signalering in de technische infrastructuur heeft betrekking op geautomatiseerde controle, alarmering en rapportering. “Controle” heeft hierbij betrekking op het toetsen of een configuratie is ingesteld conform het geautoriseerde ontwerp. Met “alarmering” wordt gedoeld op het afgeven van signalen aan systeembeheerders wanneer beleidsregels en/of grens-waarden worden overschreden. “Rapportering” maakt het mogelijk om (beveiligings)incidenten te onderkennen op basis van analyse en correlatie van vastleggingen.

5.5.2 Toelichting en afbakening

Door de groeiende volwassenheid van de hulpmiddelen in de markt krijgt signalering meer en meer betekenis voor het beheer van de IT-diensten. Dit type maatregelen is noodzakelijk om verstoringen in de productieverwerking te voorkomen of om potentiële risico’s in de werking van een infrastructuur te kunnen beheersen. De procedurele handelingen van bewaking (monitoring) die naar aanleiding van de signalering dienen te volgen vallen niet onder “Signalering”, maar onder het beheerproces Operations Management.

5.5.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
A	De inrichting van de IT-middelen dient te worden beperkt tot de strikt noodzakelijke en geautoriseerde functionaliteit.
B	Toegang tot en gebruik van IT-diensten dient te worden beperkt tot geautoriseerde gebruikers en beheerders.
C	De IT-dienst dient onder de benoemde bedrijfsomstandigheden een overeengekomen werklast te kunnen verwerken.

I	Incidenten in de IT-dienst dienen tijdig en doeltreffend te worden voorkomen of te worden gesignaleerd en afgehandeld.
K	Productieopdrachten dienen juist, volledig en tijdig te worden verwerkt.

5.5.4 Beheersingsmaatregelen

Technische beheersingsmaatregelen in de IT-configuratie

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Signalering				
01	Automatische routines (scripts) voor beheer en controle worden beheerd op en geïnitieerd vanuit een aparte (beheer)zone.		A B C I K	
02	Automatische routines zijn geïmplementeerd voor het inspecteren van gegevensverkeer vanuit onvertrouwde zones op schadelijke inhoud (malicious software) en voor het zo nodig signaleren van de beheerorganisatie. Detectiedefinities worden regelmatig en geautomatiseerd actueel gehouden.	X	A	Technische instellingen en scripts voor signalering. Rapportages van signalering.

Technische beheersingsmaatregelen in de IT-middelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Signalering				
01	Automatische routines zijn geïmplementeerd voor het controleren van de technische inrichting van de IT-dienst op afwijkingen van het geautoriseerde ontwerp en voor het zo nodig signaleren van de beheerorganisatie (soll-ist vergelijking; baseline scan). De volgende typen instellingen worden gecontroleerd: • functionele werking (alleen geautoriseerde functionaliteit / netwerkdiensten toegestaan); • objectbeveiliging (files en directories); • zonering; • redundantie; • identificatie; • authenticatie (geen netwerkdiensten met wachtwoorden in klare tekst); • autorisatie; • logging; en • capaciteit.		A C	Technische instellingen en scripts voor signalering. Rapportages van signalering.
02	Automatische routines zijn geïmplementeerd voor het controleren van de technische inrichting van de IT-dienst op het gebruik van ondersteunde en actuele software (versie van software en patch-level) en voor het zo nodig signaleren van de beheerorganisatie.		A C	Technische instellingen en scripts voor signalering. Rapportages van signalering.
03	Automatische routines zijn geïmplementeerd voor het inspecteren van het IT-middel op schadelijke inhoud (malicious software) en voor het zo nodig signaleren van de beheerorganisatie. Detectiedefinities worden regelmatig en geautomatiseerd actueel gehouden.	X	A	Technische instellingen en scripts voor signalering. Rapportages van signalering.

04	Automatische routines en drempelwaarden zijn geïmplementeerd voor het alarmeren van de beheerorganisatie wanneer beleidsregels en prestatieniveaus zijn of dreigen te worden overschreden.		B C I K	Technische instellingen (drempelwaarden) en scripts voor signalering. Rapportages van signalering.
05	Automatische routines zijn geïmplementeerd voor het analyseren van vastleggingen en het rapporteren van (dreigende) incidenten, trends en relevante gebeurtenissen.		B C I	Technische instellingen en scripts voor signalering. Rapportages van signalering.

Voorbeeld uit casus VITALIS

Een eventuele inbraak op de IT-dienst heeft ernstige gevolgen, zowel voor ontsluiten naar derden van zowel persoonsgegevens als creditcardgegevens. Pogingen deze te benaderen dienen dan ook direct te worden gesignaleerd. Alle beheersingscriteria worden door SCCS toegepast.

6 Algemene IT-beheersingsmaatregelen in IT-beheerprocessen

6.1 Generieke beheersingsaspecten beheerprocessen (GEN)

6.1.1 Definitie

Generieke beheersingsaspecten zijn aspecten die op ieder beheerproces afzonderlijk van toepassing zijn.

6.1.2 Toelichting en afbakening

De generieke beheersingsaspecten zijn van toepassing op ieder van de IT-beheerprocessen, die in dit hoofdstuk worden behandeld. De generieke beheersingsaspecten worden hier apart behandeld om redundantie in de beschrijvingen van de beheerprocessen te beperken.

De generieke beheersingsmaatregelen hebben met name betrekking het volwassenheidsniveau van de beheerprocessen. Zonder de generieke beheersingsmaatregelen hebben de beheer-processen een basisniveau van volwassenheid, die te kenmerken is als informeel, ad hoc, ongedefinieerd en/of flexibel (in termen van CobiT 5 [3] "managed process"). De generieke beheersingsmaatregelen brengen de volwassenheid naar hogere niveau's:

- Formeel gedefinieerd en ingericht (CobiT 5 "established process");
- Meetbaar en beheersbaar (CobiT 5 "predictable process");
- Voldoet aan de actuele eisen (CobiT 5 "optimising process").

Verder is het van belang het verschil te onderkennen tussen de hier genoemde generieke beheersingsmaatregelen en de specifieke beheersingsmaatregelen van de beheerprocessen zelf: de generieke beheersingsmaatregelen hebben betrekking op het *beheerproces* en niet op de *IT-dienst*. Bijvoorbeeld: het capacity management *proces* wordt periodiek geëvalueerd en positief bevonden, terwijl er tekortkomingen worden geconstateerd in de *capaciteit van de IT-dienst* in de periodieke evaluatie door het capacity management proces.

6.1.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
W	Belanghebbenden dienen juist en volledig over het proces te worden geïnformeerd.
X	Het proces dient formeel te zijn gedefinieerd en ingericht.
Y	Het proces dient meetbaar en beheersbaar te zijn.
Z	Het proces dient te voldoen aan de actuele vereisten.

W Belanghebbenden dienen juist en volledig over het proces te worden geïnformeerd.

Toelichting:
Indien belanghebbenden onjuist of onvolledig (hieronder ook de tijdigheid begrepen) over de uitkomsten en kenmerken van het proces worden geïnformeerd, bestaat het risico dat deze belanghebbenden verkeerde beslissingen nemen op grond van deze informatie. Voor de serviceorganisatie kan dit een schending betekenen van overeenkomsten en kan dit leiden tot reputatie- en financiële schade. Belanghebbenden zijn onder meer: de klantorganisaties; de eigenaren van de IT-middelen; en de betrokkenen van andere tactische en operationele IT-beheerprocessen.

X Het proces dient formeel te zijn gedefinieerd en ingericht.

Toelichting:
Deze doelstelling houdt een volwassenheidsniveau van het proces in, waarbij het proces op een vaste en eenduidige wijze wordt uitgevoerd, ongeacht de betrokken personen. Het proces is beschreven, door management geaccordeerd en bekend bij alle betrokkenen. Het risico bestaat echter wel dat de doelstellingen van het proces niet worden behaald, doordat het proces niet tijdig wordt bijgesteld aan de veranderende omgeving.

Y Het proces dient meetbaar en beheersbaar te zijn.

Toelichting:
Deze doelstelling houdt een volwassenheidsniveau van het proces in, waarbij de doelstellingen van het proces worden vastgesteld en de uitvoering van het proces meetbaar is. Doordat het proces meetbaar is, zal men achteraf kunnen evalueren of de

doelstellingen van het proces zijn behaald. Het risico bestaat echter wel dat de doelstellingen niet worden behaald, doordat het proces niet tijdig wordt bijgesteld aan de veranderende omgeving.

Z **Het proces dient te voldoen aan de actuele vereisten.**

Toelichting:
Deze doelstelling houdt een volwassenheidsniveau van het proces in, waarbij het proces zo nodig wordt bijgesteld aan de actuele omstandigheden om het behalen van de doelstellingen van het proces te borgen. De uitkomsten van het proces hebben hierdoor een zekere voorspelbaarheid.

6.1.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Het proces dient formeel te zijn gedefinieerd en ingericht.				
01	Management van de serviceorganisatie heeft beleid vastgesteld voor het proces over de reikwijdte, randvoorwaarden, relaties met aanverwante processen, prioriteiten en werkwijze van het proces.	X	X Y Z	Beleidsplan.
02	Het proces, waaronder de procesgang en rollen, is gedocumenteerd, geaccordeerd door management en bekend gemaakt bij alle betrokkenen.	X	X Y Z	Procesdocumentatie.
03	De verantwoordelijkheden voor het proces zijn toegewezen.	X	X Y Z	Beschrijving van taken en verantwoordelijkheden.
04	De serviceorganisatie beschikt over voldoende middelen, deskundigheid en capaciteit (door intern personeel en/of externe dienstverleners, inclusief vervangend personeel in geval van tijdelijke afwezigheid) om het proces uit te voeren.	X	X Y Z	Organisatieschema en -beschrijving.
Het proces dient meetbaar en beheersbaar te zijn.				
05	Management van de serviceorganisatie heeft kwaliteits- en prestatiedoelstellingen vastgesteld voor het proces.	X	Y Z	Kwaliteits- en prestatiedoelstellingen.

06	Relevante gebeurtenissen, beheeractiviteiten en uitkomsten van het proces worden gemeten en geregistreerd.	X	Y Z	Logboek Registraties van het proces.
07	Een toegespitst informatiesysteem wordt gebruikt ter ondersteuning van de procesgang, registraties en informatievoorziening van het proces.		Y Z	Systeem- en gebruikersdocumentatie.
08	Periodiek worden de kwaliteit en prestaties van het proces geëvalueerd ten opzichte van de doelstellingen en worden de inrichting en/of capaciteit van het proces zo nodig bijgesteld.	X	Y Z	Procesrapportage.
Het proces dient te voldoen aan de actuele vereisten.				
09	Drempelwaarden zijn gedefinieerd voor de (automatische) signalering van (dreigende) overschrijdingen van kwaliteits- en prestatiedoelstellingen.		Z	Procesdocumentatie.
10	Het proces wordt continu gemonitord op het borgen van de kwaliteits- en prestatiedoelstellingen. Bij (dreigende) overschrijdingen wordt de inrichting en/of capaciteit van het beheerproces zo nodig bijgesteld.	X	Z	Werkinstructies. Correspondentie.
11	Medewerkers worden periodiek bijgeschoold in relevante nieuwe ontwikkelingen en procesaanpassingen.		Z	Opleidingsprogramma.
12	Periodiek worden het beleid, het proces en de kwaliteits- en prestatiedoelstellingen geëvalueerd met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door het management ge(her)accordeerd.	X	Z	Procesrapportage.
Belanghebbenden dienen juist en volledig over het proces te worden geïnformeerd.				

13	Rapportages aan belanghebbenden over de prestaties en beheersing van de IT-dienst worden gecontroleerd op juistheid en volledigheid (waaronder tijdigheid).	X	W	Interne rapportages. Werkinstructies. Correspondentie.
14	Er is functiescheiding tussen de functionarissen belast met: beleid en doelstellingen voor het proces; uitvoering van het proces; en registratie/rapportage over het proces.	X	W	Procesdocumentatie. Organisatieschema.

6.1.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
01	Periodiciteit van rapportage aan de klantorganisatie over de beheersingsdoelstellingen. (I)
02	Snelheid van rapportages aan de klantorganisatie (periode tussen de datum van rapportage en de einddatum waarover wordt gerapporteerd). (I)
Prestatie-indicatoren te meten door de serviceorganisatie	
03	Periodiciteit van de evaluatie van het beheerproces en de beheersingsdoelstellingen. (I)
04	Mate van afwijking van de gerealiseerde versus afgesproken beheersingsdoelstellingen per evaluatieperiode. (R)
05	Periodiciteit van rapportages aan belanghebbenden van de serviceorganisatie. (I)

6.2 Supply Chain Management (SCM)

6.2.1 Definitie

Supply Chain Management draagt zorg voor het bewaken van de levering van de afgesproken dienstverlening door zowel interne afdelingen als door externe leveranciers.

6.2.2 Toelichting en afbakening

Dit proces is belast met het borgen van de aansluiting tussen vraag en aanbod van IT-diensten tussen de serviceorganisatie en de (interne en/of externe) leveranciers. Deze aansluiting wordt geformaliseerd door het afsluiten en onderhouden van zogenaamde underpinning contracts met Service Level Agreements (bij externe leveranciers, ook wel subserviceorganisaties genoemd) en/of Operational Level Agreements (bij interne leveranciers).

Supply Chain Management omvat het definiëren, meten, bewaken en doen verbeteren van de IT-dienstverlening door de (interne en externe) leveranciers aan de serviceorganisatie. Buiten het Suppy Chain Management proces vallen de besluitvorming over de bron van levering (ook wel aangeduid als "sourcing" of "make-or-buy" besluitvorming) en over de selectie van de (interne of externe) leverancier (inkoop).

In serviceorganisaties zijn vaak aparte *afdelingen* ingericht voor het aansturen van enerzijds interne leveranciers, vaak aangeduid met Service Management, en anderzijds externe leveranciers, vaak aangeduid met Vendor Management. Vanuit oogpunt van beheerprocessen en beheersingsmaatregelen zijn op beide activiteiten dezelfde beheersingscriteria van toepassing, zoals in deze sectie beschreven.

Vanwege de recursiviteit, omdat de serviceorganisatie op haar beurt zèlf leverancier is van de klantorganisatie, zal ook de klantorganisatie een eigen Supply Chain Management proces inrichten voor de aansturing van de serviceorganisatie: de serviceorganisatie zit dan "aan de andere kant van de tafel" en zal zich moeten verantwoorden over de beheersingsmaatregelen en prestatieniveaus van de IT-dienst. De hiermee gepaard gaande activiteiten van de serviceorganisatie, soms aangeduid als Service Level Management, zijn ofwel transparant voor de klantorganisatie (b.v. het afsluiten van een contract, het voeren van periodiek overleg) ofwel maken onderdeel uit van de in dit hoofdstuk beschreven beheerprocessen: het beschrijven van een apart proces vinden wij daarom niet nodig.

6.2.3 Beheersingsdoelstellingen

Supply Chain Management kan zich op elk van de IT-beheersingsdoelstellingen richten, afhankelijk van de IT-dienst die de leverancier levert. Naast deze doelstellingen van interne

beheersing, richt dit beheerproces zich op het voldoen aan de vereiste beleidspunten (zoals wet- en regelgeving en intern beleidsregels) en prestatieniveaus (service levels) die zijn afgesproken met de klantorganisaties.

6.2.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	Periodiek worden de IT-diensten van (interne en externe) leveranciers en de daarbij horende voorwaarden (beleidspunten, prestatiecriteria, beheersingscriteria en geautoriseerde ontvangers van IT-diensten) geëvalueerd, met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door de daartoe bevoegden van de betrokken partijen ge(her)accordeerd.	X	Alle	Contracten (underpinning contracts) en onderliggende documenten.
02	Communicatie- en escalatieprocedures, waaronder rapportagevorm, -periodiciteit en -inhoud, worden overeengekomen met (interne en externe) leveranciers en worden ingericht binnen de serviceorganisatie.		Alle	Procedurebeschrijvingen.
03	Communicatie- en escalatieprocedures worden overeengekomen met de klantorganisaties en worden ingericht binnen de serviceorganisatie.		Alle	Procedurebeschrijving.
Uitvoering				
04	Prestatie-indicatoren, -normen en drempelwaarden zijn gedefinieerd voor de (automatische) signalering van (dreigende) overschrijdingen van prestatieniveaus.	X	Alle	Drempelwaarden (parameters) en signaalberichten.

05	Prestaties van IT-diensten worden continu (geautomatiseerd) gemeten, geregistreerd en vergeleken met drempelwaarden, al dan niet met gebruik van automatische signaleringsrapportages; zo nodig worden incidenten ingediend.	X	Alle	Registratie van metingen. Vastleggingen van analyses. Service level rapportages. Third party en auditrapportages.
06	Periodiek wordt overlegd met de (interne en externe) leveranciers over de gerealiseerde prestatieniveaus, geplande en uitgevoerde wijzigingen, opgetreden incidenten en de perceptie van de kwaliteit van de IT-diensten.	X	Alle	Notulen Service Level Meetings. Service level rapportages. Correspondentie.
Bewaking				
07	Periodiek worden (audit)rapportages over de gerealiseerde beheersingscriteria geanalyseerd ten opzichte van de gestelde eisen; zo nodig worden wijzigingsvoorstellen ingediend.	X	Alle	Auditrapportages.
08	Periodiek worden de prestaties van IT-diensten, en (dreigende) overschrijdingen van prestatieniveaus geanalyseerd ten opzichte van de gestelde eisen; zo nodig worden wijzigingsvoorstellen ingediend.	X	Alle	Registratie van metingen. Vastleggingen van analyses. Service level rapportages.

6.2.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
–	–
Prestatie-indicatoren te meten door de serviceorganisatie	
01	Periodiciteit van beoordeling van rapportages over gerealiseerde prestatieniveaus (service level rapportages van de leverancier) en beheersingsdoelstellingen (auditrapportages van de leverancier) door de leverancier. (I)
02	Snelheid van rapportage door leveranciers (periode tussen de datum van rapportage en de einddatum waarover wordt gerapporteerd). (I)
03	Periodiciteit van evaluatiebesprekingen per leverancier (service level meetings) per periode. (I)
04	Aantal supplier management bewakingsuren per periode. (I)
05	Periodiciteit van evaluatie van de contracten per leverancier. (I)
06	Aantal afwijkingen in het nakomen van afspraken per leverancier per periode. (R)
07	Aantal incidenten per leverancier per impactcategorie per periode. (I)

6.3 Security Management (SEC)

6.3.1 Definitie

Security Management draagt zorg voor het in kaart brengen en adresseren van de risico's van exclusiviteit, integriteit en beschikbaarheid die van toepassing zijn op de IT-dienst.

6.3.2 Toelichting en afbakening

Het doel van Security Management is om te waarborgen dat alle risico's van exclusiviteit, integriteit en beschikbaarheid *systematisch* in kaart worden gebracht en *in samenhang* worden geadresseerd.

Security Management kan worden beschouwd als een verbijzonderde vorm van Risico Management, namelijk Risico Management gericht op *operationele* risico's van *exclusiviteit, integriteit en beschikbaarheid* (dus exclusief, bijvoorbeeld, strategische en financiële risico's en risico's ten aanzien van effectiviteit en efficiëntie).

De reikwijdte van Security Management omvat zowel de ontwikkel- als de exploitatiefase van de IT-dienst. Tijdens de ontwikkelfase van de IT-dienst dient een risicoanalyse plaats te vinden en dient een ontwerp te worden gemaakt voor de wijze van risicobeheersing.

Dit stelsel richt zich echter uitsluitend op de exploitatiefase van een IT-dienst, waarin dus het ontwerp van de risicobeheersing (waaronder de security architectuur) als gegeven wordt beschouwd. In de exploitatiefase dienen de beheersingsmaatregelen in stand te worden gehouden conform het ontwerp en dient actie te worden ondernomen op relevante gebeurtenissen.

In relatie tot de andere tactische beheerprocessen (Infrastructure, Access, Capacity, Continuity en Availability Management), als ook in relatie tot technische instellingen (zonering, redundantie etc.), dient Security Management te worden gezien als een overkoepelend beheerproces die zorgdraagt voor de algehele samenhang.

6.3.3 Beheersingsdoelstellingen

Security Management richt zich op alle beheersingsdoelstellingen van de IT-dienst.

6.3.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	De serviceorganisatie heeft een beveiligingsbeleid voor de IT-dienst in overeenstemming met de beleidspunten van klantorganisaties.	X	Alle	Beveiligingsbeleid.
02	Periodiek wordt een risicoanalyse voor de IT-dienst uitgevoerd, gedocumenteerd en door het management geaccordeerd.	X	Alle	Risicoanalyse.
03	Periodiek wordt het beveiligingsontwerp van de IT-dienst geëvalueerd met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door het management ge(her)accordeerd. Niet afgedekte (rest)risico's zijn hierbij door het management geaccordeerd.	X	Alle	Beveiligingsontwerp (en -architectuur) met geselecteerde beheersingsmaatregelen.
04	Testplannen zijn opgesteld voor het testen van de kwetsbaarheid van (onderdelen van) de IT-dienst.	X	Alle	Testplannen
Uitvoering				
05	Meldingen van beveiligingsrisico's door externe instanties worden ontvangen en beoordeeld.	X	Alle	CERT-advisories en correspondentie.

06	Continu worden (registraties van) relevante gebeurtenissen van de IT-dienst onderzocht op bedreigingen voor de beveiliging, op afwijkingen van beleidsregels, en op afwijkingen van het beveiligingsontwerp; al dan niet met gebruik van automatische signaleringsrapportages. Zo nodig worden incidenten ingediend. De volgende typen gebeurtenissen worden onderzocht: • Gebruik van technische beheerfuncties; • Gebruik van functionele beheerfuncties; • Handelingen van beveiligingsbeheer; • Beveiligingsovertredingen; • Verstoringen in het productieproces; • Handelingen van systeemtoegang; • Toegang tot gebruikersbestanden door beheerders; • Het vollopen van het opslagmedium voor de logbestanden; • Het overschrijven of verwijderen van logbestanden (dit wordt gelogd in de nieuw aangelegde log).	X	Alle	
07	Periodiek wordt de IT-dienst getest op het bestaan van kwetsbaarheden (b.v. penetratietesten); zo nodig worden wijzigingsvoorstellen ingediend.	X	Alle	Testresultaten
Bewaking				
08	Periodiek wordt de beveiliging van de IT-dienst getoetst op naleving van het beveiligingsontwerp; zo nodig worden incidenten of wijzigingsvoorstellen ingediend.	X	Alle	Testresultaten

6.3.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
–	–
Prestatie-indicatoren te meten door de serviceorganisatie	
01	Periodiciteit van de evaluatie van risico's en van het beveiligingsontwerp. (I)
02	Aantal beveiligingsincidenten per impactcategorie per evaluatieperiode. (I)
03	Periodiciteit van het testen op kwetsbaarheden. (I)
04	Aantal bewakingsuren voor security management per periode. (I)

6.4 Infrastructure Management (INF)

6.4.1 Definitie

Infrastructure Management draagt zorg voor de handhaving van correcte inrichting van de IT-middelen.

6.4.2 Toelichting en afbakening

De levenscyclus van een IT-dienst omvat enerzijds een ontwikkelfase en anderzijds een exploitatiefase. De ontwikkelfase, die buiten de reikwijdte van dit document valt, wordt vooronderstelt zorg te dragen voor een geautoriseerd en getest (en dus juist en effectief) ontwerp van de IT-dienst. Na overdracht vanuit de ontwikkelfase naar de exploitatiefase is het beheerproces Infrastructure Management belast met het handhaven en onderhouden van de juiste inrichting in overeenstemming met het geautoriseerde ontwerp.

6.4.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
A	De inrichting van de IT-middelen dient te worden beperkt tot de strikt noodzakelijke en geautoriseerde functionaliteit.

6.4.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	Periodiek wordt het technische ontwerp van de IT-dienst geëvalueerd met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door het management ge(her)accordeerd. Niet afgedekte (rest)risico's zijn hierbij door het management geaccordeerd.	X	A	Technisch ontwerp

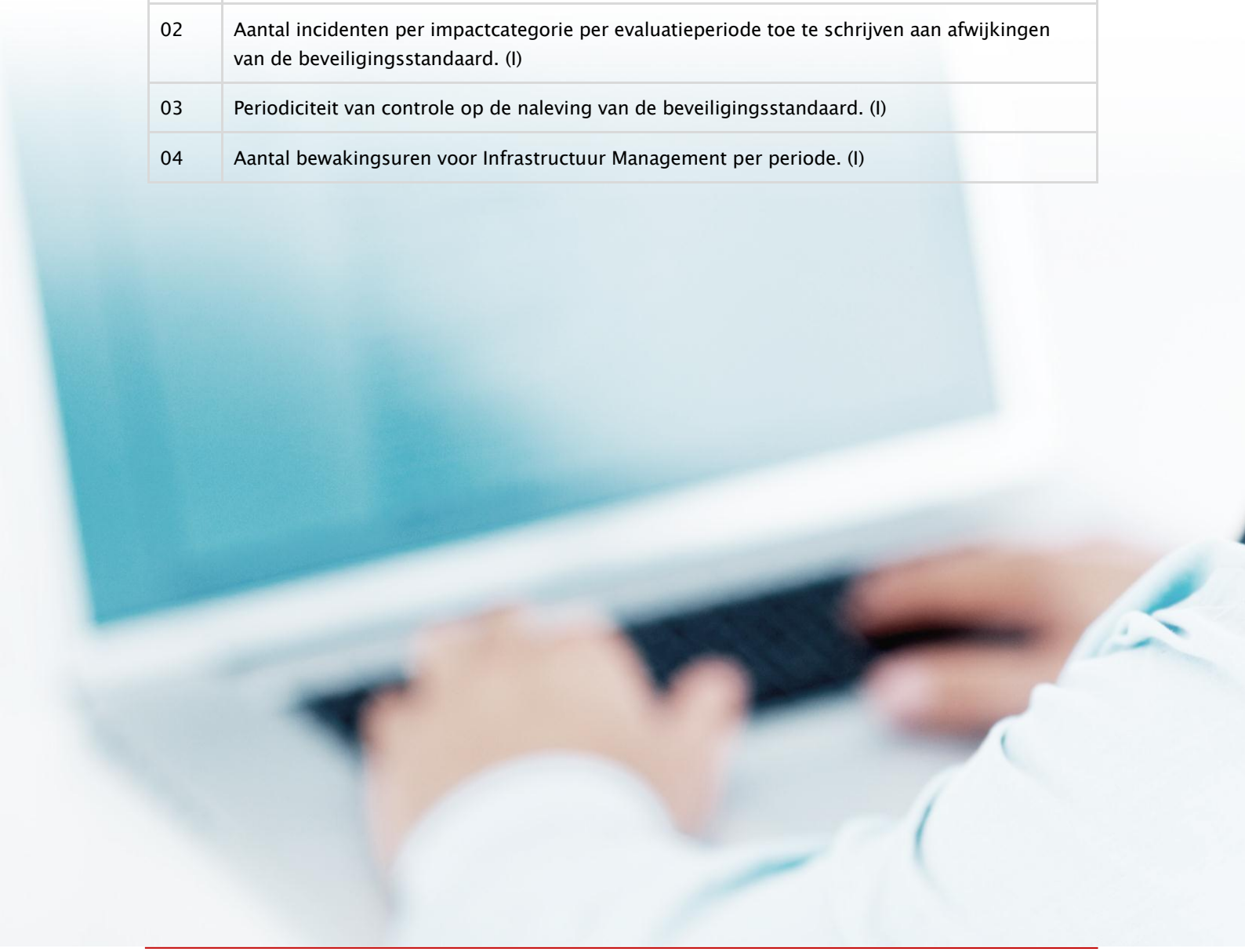
02	Testplannen zijn opgesteld voor het testen van de kwetsbaarheid van IT-middelen van de IT-dienst (waaronder penetratietests).		A	Testplannen
Uitvoering				
03	De technische inrichting van IT-middelen wordt vastgelegd (of "bevroren"), zodanig dat ongeautoriseerde wijzigingen van die instellingen kunnen worden gesignaleerd. De volgende typen instellingen worden vastgelegd: • functionele werking (alleen geautoriseerde functionaliteit / netwerkdiensten toegestaan); • objectbeveiliging (files en directories); • zonering; • redundantie; • identificatie; • authenticatie (geen netwerkdiensten met wachtwoorden in klare tekst); • autorisatie; • logging; en • capaciteit.	X	A	Technische baseline.
04	Meldingen van leveranciers van beveiligingsrisico's en aanbevolen wijzigingen (patches) worden ontvangen en beoordeeld, alvorens zo nodig via Change Management te worden doorgevoerd.	X	A	Release notes van patches en gerelateerde interne documentatie.
05	Behoudens de door de leverancier goedgekeurde updates (waaronder patches) worden er geen wijzigingen aangebracht in standaard systeemsoftware.		A	
06	De werking van automatische routines voor controle, alarmering en rapportage van de inrichting van de IT-middelen wordt periodiek gecontroleerd.		A	

07	Continu worden wijzigingen van technische instellingen en (registraties van) relevante gebeurtenissen op de IT-middelen onderzocht op bedreigingen voor de technische werking, op afwijkingen van beleidsregels, en op afwijkingen van het technische ontwerp; al dan niet met gebruik van automatische signaleringsrapportages; zo nodig worden incidenten ingediend.	X	A	
08	Periodiek worden de IT-middelen getest op het bestaan van kwetsbaarheden (in overeenstemming met de testplannen / penetratietests); eventuele tekortkomingen worden geanalyseerd en zo nodig worden wijzigingsvoorstellen ingediend.		A	Testplannen
Bewaking				
09	Periodiek worden de IT-middelen getoetst op naleving van het technische ontwerp en op het gebruik van ondersteunde en actuele software (versie van software en patch-level); zo nodig worden incidenten of wijzigingsvoorstellen ingediend.	X	A	Testresultaten

6.4.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
-	-
Prestatie-indicatoren te meten door de serviceorganisatie	
01	Periodiciteit van de evaluatie van de beveiligingsstandaard. (I)
02	Aantal incidenten per impactcategorie per evaluatieperiode toe te schrijven aan afwijkingen van de beveiligingsstandaard. (I)
03	Periodiciteit van controle op de naleving van de beveiligingsstandaard. (I)
04	Aantal bewakingsuren voor Infrastructuur Management per periode. (I)



6.5 Access Management (ACC)

6.5.1 Definitie

Access Management draagt zorg voor het beheren van de fysieke en logische toegang tot de IT-diensten en de IT-middelen.

6.5.2 Toelichting en afbakening

Het doel van toegangsbeveiliging is het beschermen van de IT-diensten en IT-middelen tegen ongeautoriseerd gebruik, aanpassing, bekendmaking en vernietiging. Access Management is van toepassing op zowel logische als fysieke beveiliging.

6.5.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
B	Toegang tot en gebruik van IT-diensten dient te worden beperkt tot geautoriseerde gebruikers en beheerders.

6.5.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	Periodiek worden de ontwerpen van de toegangsbeveiliging en van de autorisatiematrix geëvalueerd met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door het management ge(her)accordeerd. Niet afgedekte (rest)risico's zijn hierbij door het management geaccordeerd.	X	B	Autorisatiematrix. Beveiligingsstandaard.
Uitvoering				

02	Unieke identiteitskenmerken (zoals gebruikersnamen en pasjes) worden toegekend aan gebruikers en beheerders na controle van de identiteit van de gebruikers en beheerders en na goedkeuring door of namens het verantwoordelijke management.	X	B	Werkinstructies / standaard change
03	Individuele en geheime authenticatiemiddelen worden uitgegeven aan gebruikers en beheerders zodanig dat deze middelen niet in handen komen van ongeautoriseerde personen.	X	B	Werkinstructies / standaard change
04	Toegangsrechten worden uitgegeven aan gebruikers en beheerders na goedkeuring door het verantwoordelijke management.	X	B	Werkinstructies / standaard change
05	Functiewijzigingen en uitdiensttredingen worden bewaakt voor aanpassen van de toegangsrechten en voor intrekken van de identiteits- en authenticatiemiddelen.	X	B	Procedures beheer toegangsrechten. Informatie van management/ personeelszaken over functiewijzigingen.
06	Toegangsrechten en de identiteits- en authenticatiemiddelen worden gedeactiveerd of ingetrokken nadat hiervan gedurende een vastgestelde periode geen gebruik is gemaakt.		B	Procedure/beschrijving technische maatregelen
07	Continu worden toegang en toegangspogingen tot de IT-dienst en de IT-middelen onderzocht op bedreigingen voor de toegangsbeveiliging; al dan niet met gebruik van automatische signaleringsrapportages. Zo nodig worden incidenten ingediend.	X	B	
Bewaking				
08	Periodiek worden toegangsrechten op actualiteit getoetst en herbevestigd door het verantwoordelijke management; zo nodig worden incidenten of wijzigingsvoorstellen ingediend.	X	B	Controleverslag. Door management geaccordeerde overzichten van aanwezige autorisaties.

6.5.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
01	Periodiciteit van controle op de naleving van de autorisatiematrix (voor toegang door gebruikers van de klantorganisatie). (I)
Prestatie-indicatoren te meten door de serviceorganisatie	
02	Periodiciteit van de evaluatie van de autorisatiematrix (voor toegang door gebruikers en beheerders van de serviceorganisatie). (I)
03	Periodiciteit van controle op de naleving van de toegangsprocedures (voor toegang door gebruikers en beheerders van de serviceorganisatie). (I)
04	Aantal incidenten per impactcategorie per evaluatieperiode toe te schrijven aan afwijkingen van de autorisatiematrix (voor toegang door gebruikers en beheerders van de service- en klantorganisatie). (R)

6.6 Capacity Management (CAP)

6.6.1 Definitie

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

6.6.2 Toelichting en afbakening

Het doel van Capacity Management is het realiseren van de benodigde capaciteit van de IT-middelen die de IT-diensten moeten realiseren. Uit de capaciteitsbehoefte van de klantorganisatie dient de capaciteitsbehoefte voor de IT-middelen te worden afgeleid door de serviceorganisatie. Capacity Management is belast met:

- Planning van de capaciteit op basis van de afgesproken niveaus van dienstverlening;
- Bewaking van de prestaties en belasting van de IT-diensten en IT-middelen;
- Zo nodig uitbreiding van de capaciteit van de IT-middelen door het indienen van wijzigingsverzoeken via Change Management.

6.6.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
C	De IT-dienst dient onder benoemde bedrijfsomstandigheden een overeengekomen werklast te kunnen verwerken.

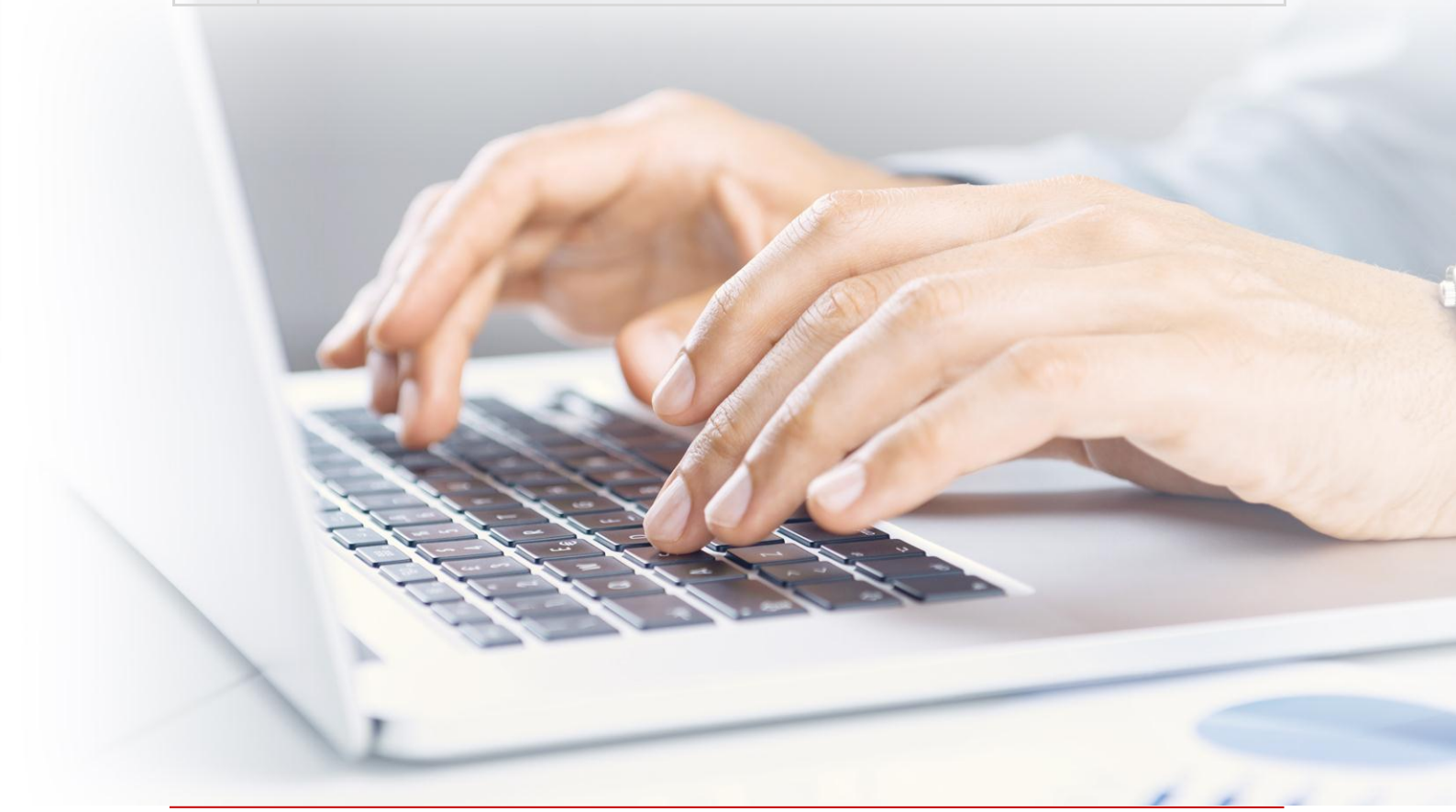
6.6.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	Periodiek wordt het capaciteitsplan van de IT-dienst geëvalueerd met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door het management ge(her)accordeerd. Niet afgedekte (rest)risico's zijn hierbij door het management geaccordeerd.	X	C	Capaciteitsplan
Uitvoering				
02	Drempelwaarden zijn gedefinieerd voor de (automatische) signalering van (dreigende) capaciteitsoverschrijdingen.	X	C	Capaciteitsregistratie
03	Capaciteitsverbruik wordt continu gemeten, geregistreerd en vergeleken met drempelwaarden, al dan niet met gebruik van automatische signaleringsrapportages; zo nodig worden incidenten ingediend.	X	C	Capaciteitsregistratie
Bewaking				
04	Periodiek worden de capaciteit, het capaciteitsverbruik en (dreigende) capaciteitsoverschrijdingen geanalyseerd ten opzichte van de gestelde eisen; zo nodig worden wijzigingsvoorstellen ingediend.	X	C	Capaciteitsrapportage

6.6.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
01	Karakteristiek van de belasting van de IT-dienst, zoals de gemiddelde belasting, piekbelasting en verdeling van de belasting. (I)
02	Responsetijd van de IT-dienst. (I)
03	Aantal afwijkingen in de beschikbaarheid dat niet vooraf door de serviceorganisatie is aangekondigd of gesignaleerd. (R)
Prestatie-indicatoren te meten door de serviceorganisatie	
04	Periodiciteit van de evaluatie van het capaciteitsplan. (I)
05	Aantal capaciteitsincidenten per impactcategorie per evaluatieperiode. (I)
06	Aantal bewakingsuren voor Capacity Management per periode. (I)



6.7 Availability Management (AVA)

6.7.1 Definitie

Availability Management draagt zorg voor het beschikbaar houden van de IT-dienst onder normale bedrijfsomstandigheden en op de normale productielocatie, in overeenstemming met het afgesproken niveau van dienstverlening.

6.7.2 Toelichting en afbakening

Het doel van Availability Management is om de IT-dienst beschikbaar te houden in overeenstemming met de afgesproken beschikbaarheid en met de eisen van het management van de serviceorganisatie. Availability Management richt zich daarbij alleen op normale, met de klant afgesproken bedrijfsomstandigheden en niet op de beschikbaarheid van de IT-dienst na het optreden van en tijdens calamiteiten: het beheersen van calamiteitensituaties behoort tot het proces Continuity Management.

Het proces Availability Management start bij het treffen van maatregelen om aan de beschikbaarheidseisen te kunnen voldoen. Het bepalen van de beschikbaarheidseisen is de verantwoordelijkheid van de klantorganisatie en van het management van de service-organisatie.

6.7.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
C	De IT-dienst dient onder benoemde bedrijfsomstandigheden een overeengekomen werklast te kunnen verwerken.

6.7.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	Periodiek wordt het ontwerp van de beschikbaarheid van de IT-dienst geëvalueerd met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door het management ge(her)accordeerd. Niet afgedekte (rest)risico's zijn hierbij door het management geaccordeerd.	X	C	Beschikbaarheidsplan / technisch ontwerp
02	Testplannen zijn opgesteld voor het testen van redundante IT-middelen en hun activeringsmechanismen.	X	C	Testplannen
Uitvoering				
03	De IT-middelen zijn onderworpen aan een onderhouds- en vervangingsplan; periodiek worden de IT-middelen onderhouden en/of vervangen in overeenstemming met het onderhouds- en vervangingsplan.		C	Onderhoudscontracten Controleverslag
04	Tijdsblokken zijn afgesproken met klanten voor het uitvoeren van onderhoud aan de IT-middelen (geplande down-time).		C	Onderhoudsrooster
05	De mate van beschikbaarheid van de IT-dienst wordt continu (geautomatiseerd) gemeten en geregistreerd, al dan niet met gebruik van automatische signaleringsrapportages; zo nodig worden incidenten ingediend.	X	C	Beschikbaarheidsregistratie
06	Periodiek worden de redundante IT-middelen en hun activeringsmechanismen getest in overeenstemming met de testplannen; eventuele tekortkomingen worden geanalyseerd en zo nodig worden wijzigingsvoorstellen ingediend.	X	C	Testresultaten

Bewaking				
07	Periodiek wordt de feitelijke beschikbaarheid geanalyseerd ten opzichte van de gestelde eisen; zo nodig worden wijzigingsvoorstellen ingediend.	X	C	Beschikbaarheidsrapportage

6.7.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
01	Percentage gerealiseerde beschikbaarheid ten opzichte van de afgesproken beschikbaarheid. (R)
02	Aantal afwijkingen in de beschikbaarheid dat niet vooraf door de serviceorganisatie is aangekondigd of gesignaleerd. (R)
Prestatie-indicatoren te meten door de serviceorganisatie	
04	Periodiciteit van de evaluatie van het beschikbaarheidsplan. (I)
05	Aantal beschikbaarheidsincidenten per impactcategorie per evaluatieperiode. (I)
06	Aantal bewakingsuren voor Availability Management per periode. (I)

6.8 Continuity Management (CTY)

6.8.1 Definitie

Continuity Management draagt zorg voor het herstellen en voortzetten van de IT-dienst na het optreden van een calamiteit in overeenstemming met het afgesproken niveau van dienstverlening.

6.8.2 Toelichting en afbakening

Het doel van Continuity Management is om zeker te stellen dat de IT-dienst na en tijdens het optreden van een calamiteit weer wordt hersteld binnen de afspraken die hierover met de klanten zijn gemaakt. Continuity Management houdt zich niet bezig met het beschikbaar zijn van de IT-dienst onder normale bedrijfsomstandigheden: het beheersen van de normale beschikbaarheid behoort tot het proces Availability Management.

Het proces Continuity Management start bij het treffen van maatregelen om te kunnen voldoen aan de continuïteitseisen, die zijn afgesproken met klantorganisaties. Om er zeker van te zijn dat de gekozen maatregelen ook daadwerkelijk werken wordt de uitwijkbaarheid en herstelbaarheid periodiek getest. Het bepalen van de continuïteitseisen is de verantwoordelijkheid van de klantorganisatie (Business Continuity Management).

6.8.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
D	De IT-dienst dient, in geval van benoemde typen afwijkende bedrijfsomstandigheden (calamiteiten), tijdig herstelbaar te zijn om een overeengekomen werklast te kunnen verwerken.

6.8.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	Periodiek wordt het continuïteitsplan van de IT-dienst geëvalueerd met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door het management ge(her)accordeerd. Niet afgedekte (rest)risico's zijn hierbij door het management geaccordeerd.	X	D	Continuïteitsplan.
02	Testplannen zijn opgesteld voor het testen van (onderdelen van) het continuïteitsplan.	X	D	Testplannen
Uitvoering				
03	Procedures zijn ingericht om (onderdelen van) het continuïteitsplan te onderhouden bij het doorvoeren van wijzigingen.	X	D	Procedurebeschrijving en -vastleggingen
04	Procedures zijn ingericht om (onderdelen van) het continuïteitsplan tijdig en geautoriseerd te activeren na het optreden van calamiteiten.	X	D	Procedurebeschrijving en -vastleggingen
05	Periodiek wordt het continuïteitsplan getest in overeenstemming met de testplannen; eventuele tekortkomingen worden geanalyseerd en zo nodig wordt het continuïteitsplan bijgesteld.	X	E	Testresultaten
Bewaking				
06	Periodiek worden de continuïteit van de IT-dienst geanalyseerd ten opzichte van de gestelde eisen; zo nodig wordt het continuïteitsplan bijgesteld.	X	C	Beschikbaarheidsrapportage

6.8.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
01	Hersteltijd (RTO – recovery time objective) van de IT-dienst per soort calamiteit. (R)
02	Herstelpunt (RPO – recovery point objective) van de IT-dienst per soort calamiteit, het punt in de tijd waarvan alle data wordt hersteld. (R)
Prestatie-indicatoren te meten door de serviceorganisatie	
03	Periodiciteit van de evaluatie van het continuïteitsplan. (I)
04	Percentage van het continuïteitsplan dat succesvol is getest per evaluatieperiode. (R)

6.9 Configuration Management (CON)

6.9.1 Definitie

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

6.9.2 Toelichting en afbakening

Het doel van Configuration Management is het leveren van actuele en relevante informatie aan andere IT-beheerprocessen over de IT-middelen, hun onderlinge relaties en de relaties met de IT-diensten. Met dit doel worden IT-middelen ("configuration items") geïdentificeerd, worden gegevens over de configuration items vastgelegd, bij voorkeur in een geautomatiseerde database (de "Configuration Management Data Base" of "CMDB"), en wordt de registratie periodiek vergeleken, en in overeenstemming gebracht, met de werkelijkheid.

De procesgang en beheersingsmaatregelen van Configuration Management zijn in principe ook van toepassing op het beheer van verwijderbare opslagmedia, hoewel men dit beheer vaak apart aanduidt als Tape Management. Het doel is een betrouwbare registratie te onderhouden van de verwijderbare opslagmedia, zodat de bedrijfs- en IT-processen hier gebruik van kunnen maken voor dataopslag

Configuration Management dient niet te worden verward met Asset Management. Onder het proces Asset Management worden in het bijzonder financiële gegevens over IT-middelen vastgelegd, die minder of niet relevant zijn voor de IT-beheerprocessen ten aanzien van de betrouwbaarheid en continuïteit van de dienstverlening.

6.9.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
E	De kenmerken en samenhang van IT-middelen dienen juist en volledig te worden gedocumenteerd.

6.9.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	Periodiek wordt het ontwerp van de gestructureerde registratie van configuration items van de IT-dienst geëvalueerd met inachtneming van de actuele eisen, actuele risico's en opgetreden incidenten en problemen, zo nodig geactualiseerd en door het management ge(her)accordeerd. Niet afgedekte (rest)risico's zijn hierbij door het management geaccordeerd.	X	E	CMDB-ontwerp. Technische documentatie
02	Inventarisatieplannen zijn opgesteld voor het verifiëren van juistheid en volledigheid van de registratie van configuration items.	X	E	Testplannen
Uitvoering				
03	Configuration items worden gekenmerkt in overeenstemming met naamgevingconventies.	X	E	Werkinstructie en vastleggingen, naamgevingconventies
04	Procedures zijn ingericht om nieuwe, gewijzigde en verwijderde configuration items te identificeren en te registreren.	X	E	Procedurebeschrijving en -vastleggingen
05	Periodiek wordt de registratie van configuration items geverifieerd op juistheid en volledigheid in overeenstemming met de inventarisatieplannen; eventuele verschillen worden geanalyseerd en zo nodig wordt de registratie van configuration items bijgesteld.	X	E	Procedurebeschrijving en -vastleggingen
Bewaking				
06	Periodiek wordt het ontwerp van de gestructureerde registratie van configuration items geanalyseerd ten opzichte van de gestelde eisen; zo nodig worden wijzigingsvoorstellen ingediend.	X	E	

6.9.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
-	-
Prestatie-indicatoren te meten door de serviceorganisatie	
01	Periodiciteit van de evaluatie van de structuur van de configuratie-informatie. (I)
02	Periodiciteit van controle op de juistheid en volledigheid van de configuratie-informatie. (I)
03	Aantal incidenten per impactcategorie per evaluatieperiode toe te schrijven aan afwijkingen in de configuratie-informatie. (R)

6.10 Change Management (CHA)

6.10.1 Definitie

Change Management draagt zorg voor het doorvoeren van wijzigingen in de IT-middelen en IT-diensten.

6.10.2 Toelichting en afbakening

Het doel van Change Management is om wijzigingen in de IT-middelen en IT-diensten te kunnen realiseren, zodanig dat de kans op verstoring van de dienstverlening wordt geminimaliseerd en zodanig dat de IT-dienstverlening blijvend voldoet aan de eisen van belanghebbenden. Onder de belanghebbenden kunnen worden gerekend: de klant-organisaties, de eigenaren van IT-middelen; en de beheerders van de IT-middelen en IT-diensten.

Wijzigingen kunnen voortkomen uit diverse behoeften, zoals nieuwe eisen gesteld door klantorganisaties, nieuwe eisen gesteld door eigenaren van de IT-middelen en oplossingen voor problemen. Change Management draagt hierdoor in de regel bij aan verbetering en instandhouding van de IT-dienstverlening, mits wijzigingen niet leiden tot verstoring van de IT-dienstverlening.

6.10.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
F	Wijzigingsaanvragen dienen te worden geautoriseerd met inachtneming van de risico's voor de IT-dienst.
G	Wijzigingen dienen juist, volledig en tijdig te worden doorgevoerd.
H	De IT-dienst dient te zijn beschermd tegen verstoringen door onjuiste wijzigingen en door ontwikkel- en testactiviteiten.

6.10.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Identificatie				
01	Voorgestelde wijzigingen worden systematisch geclassificeerd op impact en urgentie.	X	F G H	Wijzigingsregistratie met impactanalyse.
02	Voorgestelde wijzigingen worden geautoriseerd met in achtneming van de impactanalyse en acceptatiecriteria.	X	F H	Notulen wijzigingsoverleg. Wijzigingsregistratie.
03	Standaardtypen van wijzigingen, die een verkorte procedure mogen doorlopen, worden vooraf geclassificeerd, geautoriseerd en gedocumenteerd.		F G	Lijst van standaardtypen. Notulen met besluiten over standaardtypen.
Planning				
04	Voorgestelde wijzigingen worden geprioriteerd en gepland in overleg met alle belanghebbenden.	X	G	Notulen wijzigingsoverleg. Correspondentie.
05	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.		F G	Procedurebeschrijving.
Uitvoering				
06	Wijzigingen worden buiten de productieomgeving ontwikkeld en getest en worden getest in een omgeving die representatief is voor de productieomgeving.	X	F G H	Testresultaten.
07	Wijzigingen worden getoetst aan vooraf opgestelde criteria van doeltreffendheid en autorisatie, waarna de toetsingsresultaten worden geaccordeerd door verantwoordelijken.	X	F G H	Acceptatiecriteria. Testplan. Testresultaten.

08	De toetsing op doeltreffendheid van wijzigingen is functioneel gescheiden van de uitvoering van wijzigingen.	X	F G H	Beschrijving van taken en verantwoordelijkheden.
09	Voorafgaand aan een wijziging wordt een back-out procedure opgesteld.		F H	Wijzigingsregistratie- en/of documentatie.
10	Bekende fouten van wijzigingen, die desondanks toch worden geïmplementeerd, worden geregistreerd ten behoeve van incident management.		F G H	Documentatie van standaarden en procedures. Wijzigingsregistratie. Probleemregistratie.
11	Een wijziging wordt pas afgesloten, na controle op afronding van alle activiteiten en registraties voor de wijziging.	X	G	Documentatie van standaarden en procedures. Wijzigingsregistratie.
Bewaking				
12	Voortgangsbewaking wordt uitgeoefend op de afhandeling van (voorgestelde) wijzigingen; wijzigingen die afspraken over tijdslimieten dreigen te overschrijden worden geëscaleerd.	X	G	Documentatie van standaarden en procedures. Wijzigingenregistratie. Correspondentie.
13	Prioriteren en voortgangsbewaking van wijzigingen zijn functioneel gescheiden van de uitvoering van wijzigingen.		G	Beschrijving van taken en verantwoordelijkheden.

6.10.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
–	–
Prestatie-indicatoren te meten door de serviceorganisatie	
01	Het aantal of het percentage van wijzigingen dat per periode wordt gesignaleerd zonder registratie en autorisatie. (R)
02	Het aantal of het percentage incidenten per impactcategorie dat uit wijzigingen voortkomt. (R)
03	Het aantal of het percentage wijzigingen dat binnen de geplande doorlooptijd en budget is uitgevoerd. (R)
04	Het gerealiseerde budget of het aantal bestede uren aan wijzigingen per periode. (I)

6.11 Incident Management (INC)

6.11.1 Definitie

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

6.11.2 Toelichting en afbakening

Het doel van Incident Management is om verstoringen van de IT-dienstverlening tijdig te herstellen tot een afgesproken niveau van dienstverlening. Bij het herstel is de inzet van tijdelijke reparaties (work-arounds) geoorloofd. Ook kan een wijzigingsverzoek worden ingediend via het proces Change Management.

Het afhandelen van gebruikersverzoeken om ondersteuning, levering van informatie, advies of documentatie (ook wel aangeduid als "Service Request") valt niet onder het proces Incident Management en is verder niet expliciet uitgewerkt. Afhandeling van deze categorie gebruikersverzoeken, die vallen onder het proces Service Desk, verloopt overigens wel op een zelfde wijze als de afhandeling van incidenten.

Soms worden aan de afhandeling van bepaalde categorieën van incidenten, zoals beveiligingsincidenten, specifieke eisen gesteld. Dit stelsel houdt rekening met dergelijke categorieën van incidenten.

6.11.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
I	Incidenten in de IT-dienst dienen tijdig en doeltreffend te worden voorkomen of te worden gesignaleerd en afgehandeld.

6.11.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Identificatie				
01	Voor alle typen incidenten is een formeel en bereikbaar loket ingesteld.	X	I	Organogram. Procedurebeschrijving. Voorlichtingsmateriaal.
Planning				
02	Capaciteit is gereserveerd ter afhandeling van incidenten.	X	I	Bezettingsoverzicht.
03	Op basis van risicoanalyse is vastgesteld voor welk type incidenten er aparte oplosgroepen fungeren, waarin onder meer deelname van specialistische functionarissen is geborgd.		I	Beleidsdocument.
Uitvoering				
04	Incidenten worden systematisch geregistreerd, geclassificeerd op impact en urgentie, en geprioriteerd in overeenstemming de afspraken over het prestatieniveau.	X	I	Documentatie van standaarden en procedures. Incidentregistratie. Beleidsdocument.
05	Oplosgroepen beschikken over informatie over bekende fouten en beschikbare standaardoplossingen.		I	Documentatie van bekende fouten en work-arounds.
06	Bij (een vermoeden van) het overtreden van beveiligingsregels worden gegevens die betekenis hebben bij de bewijsvoering veiliggesteld.		I	Incidentregistratie.
07	Een incident wordt afgesloten nadat de melder heeft bevestigd dat het incident is opgelost en nadat is vastgesteld dat alle vereiste gegevens zijn geregistreerd.	X	I	Documentatie van standaarden en procedures. Incidentregistratie.
Bewaking				

08	Voortgangsbewaking wordt uitgeoefend op de afhandeling van incidenten; incidenten die afspraken over tijdslimieten dreigen te overschrijden worden geëscaleerd.	X	I	Documentatie van standaarden en procedures. Incidentregistratie. Correspondentie.
09	Prioriteren en voortgangsbewaking van incidenten zijn functioneel gescheiden van de oplosgroepen.		I	Beschrijving van taken en verantwoordelijkheden.

6.11.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
01	Mate van bereikbaarheid van loketten voor aanmelding van incidenten. (R)
Prestatie-indicatoren te meten door de serviceorganisatie	
02	Percentage van binnen de normtijd opgeloste incidenten per impactcategorie. (R)
03	Percentage van heropende incidenten. (R)
04	Het budget of het aantal uren gereserveerd voor Incident Management per periode. (I)

6.12 Problem Management (PRO)

6.12.1 Definitie

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

6.12.2 Toelichting en afbakening

Het doel van Problem Management is om de structurele fouten in van de IT-dienstverlening te minimaliseren en daarmee het aantal en de impact van potentiële incidenten te verminderen. Het proces van Problem Management tracht dit doel te bereiken door het proactief 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 Change Management.

6.12.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
I	Incidenten in de IT-dienst dienen tijdig en doeltreffend te worden voorkomen of te worden gesignaleerd en afgehandeld.

6.12.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Identificatie				
01	Incidenten worden systematisch geanalyseerd ter identificatie van problemen (reactief).	X	I	Documentatie van standaarden en procedures. Probleemregistraties. Beleidsdocument.
02	Externe bronnen (leveranciers, gebruikersgroepen, conferenties) worden systematisch geraadpleegd ter identificatie van problemen (proactief).		I	Documentatie van standaarden en procedures. Probleemregistraties.
Planning				

04	Capaciteit is gereserveerd voor onderzoek en afhandeling van problemen.	X	I	Bezettingsoverzicht.
Uitvoering				
03	Problemen worden geprioriteerd en toegewezen aan oplosgroepen in overeenstemming met het beleid.	X	I	Documentatie van standaarden en procedures. Probleemregistraties. Beleidsdocument.
05	Een probleem wordt pas afgesloten nadat is vastgesteld dat het probleem doeltreffend is opgelost en nadat is vastgesteld dat alle vereiste gegevens zijn geregistreerd.	X	I	Documentatie van standaarden en procedures.
Bewaking				
06	Voortgangsbewaking wordt uitgeoefend op de diagnose en oplossing van problemen.	X	I	Documentatie van standaarden en procedures. Probleemregistraties. Correspondentie.
07	Prioriteren en voortgangsbewaking van problemen zijn functioneel gescheiden van de oplosgroepen.		I	Taken en verantwoordelijkheden.

6.12.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
-	-
Prestatie-indicatoren te meten door de serviceorganisatie	
01	Percentage van binnen de planning opgeloste problemen. (R)
02	Percentage van heropende/terugkerende problemen. (R)
03	Het budget of het aantal uren gereserveerd voor Problem Management per periode in verhouding tot het aantal incidenten. (I)

6.13 Operations Management (OPS)

6.13.1 Definitie

Operations Management draagt zorg voor het operationeel houden van de IT-dienst.

6.13.2 Toelichting en afbakening

Het operationeel houden van de IT-dienst via Operations Management geschiedt door:

- Het bedienen en bewaken van de IT-middelen en het daarmee beschikbaar stellen van de IT-dienst aan gebruikers, bijvoorbeeld het opstarten en afsluiten van systemen. Bij de bewaking van de IT-middelen en productieverwerking worden signalen uit de IT-middelen afgehandeld, zodat de IT-dienst operationeel blijft. Tevens kunnen hierbij incidenten worden gesignaleerd die via het proces Incident Management worden afgehandeld. (Deze bewaking dient niet te worden verward met de bewakingsactiviteiten van Capacity, Availability en Continuity Management, die meer een tactisch karakter hebben en een lagere intensiteit. Deze taktische bewaking wordt veelal door Operations personeel uitgevoerd, maar als onderdeel van die beheerprocessen); en
- Het planmatig uitvoeren van incidentele en periodieke productieopdrachten. Onder productieopdrachten worden verstaan: handelingen in de productieomgeving met gebruikersgegevens die worden uitgevoerd door de serviceorganisatie, bijvoorbeeld batchverwerking, backup en restore van gegevens, en mutatie van gebruikersgegevens met beheertools. Productieopdrachten kunnen incidenteel of periodiek zijn.

6.13.3 Beheersingsdoelstellingen

Ref.	Beheersingsdoelstellingen
I	Incidenten in de IT-dienst dienen tijdig en doeltreffend te worden voorkomen of te worden gesignaleerd en afgehandeld.
J	Productieopdrachten dienen te worden geautoriseerd.
K	Productieopdrachten dienen juist, volledig en tijdig te worden verwerkt.
L	Relevante gebeurtenissen van beheer, gebruik en (dreigende) verstoring van de IT-dienst dienen te worden vastgelegd.

6.13.4 Beheersingsmaatregelen

Nr.	Beheersingsmaatregel	Key	Doel	Vastleggingen
Planning en onderhoud				
01	Periodiek wordt de productieplanning van de IT-dienst geëvalueerd met inachtneming van de actuele eisen en risico's, zo nodig geactualiseerd, gedocumenteerd en door het management geaccordeerd.	X	J K	Productieplanning.
02	Criteria zijn opgesteld voor de acceptatie van productieopdrachten.	X	J K	Productiecriteria.
Uitvoering				
03	Productieopdrachten (en wijzigingen daarop) worden geautoriseerd door de klantorganisatie of door de eigenaar van de IT-dienst met inachtneming van de acceptatiecriteria.	X	J K	Notulen van overleg. Correspondentie.
04	Productieopdrachten worden geprioriteerd en gepland in overleg met alle belanghebbenden.	X	K	Notulen van overleg. Correspondentie.
05	Bij het samenstellen van productieruns wordt vastgesteld dat rekening is gehouden met onderlinge afhankelijkheden van de verwerking.	X	K	Technisch ontwerp. Productiedraaiboek. Output planningspakket. Output scheduler.
06	Op urgente productieopdrachten, die niet volledig volgens de reguliere procedure kunnen worden afgehandeld, is een bijzondere procedure van toepassing.		J K	Procedurebeschrijving.
07	De uitvoering van productieopdrachten en de bediening van de IT-middelen verloopt volgens gedocumenteerde standaardwerkwijzen.	X	K	Productiedocumentatie. Herstartinstructies. Output scheduler.
08	Uitgevoerde bedieningshandelingen worden geregistreerd.	X	I L	Productielogboek.

Bewaking				
09	De uitvoering van productieopdrachten, de beschikbaarheid van de IT-dienst en de capaciteit van de IT-dienst worden bewaakt; gesignaleerde gebeurtenissen en (dreigende) afwijkingen worden als incident geregistreerd.	X	I K L	Registraties.

6.13.5 Prestatie-indicatoren

Prestatie-indicatoren waarmee het prestatieniveau kan worden afgesproken tussen de klant- en serviceorganisatie, zijn onder andere:

Nr.	Prestatie-indicator
Prestatie-indicatoren te meten door de klantorganisatie	
-	-
Prestatie-indicatoren te meten door de serviceorganisatie	
01	Het aantal of het percentage productieopdrachten dat juist en volledig (tijdig) is uitgevoerd. (R)
02	Aantal incidenten per impactcategorie per evaluatieperiode toe te schrijven aan afwijkingen in operationele procedures. (R)

Bijlage A: Casus ter illustratie van de werkwijze

VITALIS[1] is een verzekeringsmaatschappij die levensverzekeringen rechtstreeks aanbiedt aan particulieren via internet. Klanten kunnen via webapplicaties productinformatie en advies inwinnen, offertes aanvragen op basis van ingevoerde gegevens, contracten afsluiten, betaling van de verzekeringen verrichten, en hun persoonlijke dossier onderhouden. Onderdeel van het afsluiten van contracten is het beantwoorden van een uitgebreide vragenlijst over onder meer de leefgewoonten en de medische historie van de verzekerde. Ook worden in bepaalde gevallen gegevens ingevoerd door een medische keuringsinstantie over bloedonderzoek van de verzekerde en andere uitgevoerde medische controles.

De webapplicaties zijn ontwikkeld en worden onderhouden door de softwarefirma WEBSOFT op een eigen IT-infrastructuur. De hosting van de acceptatie- en productieomgevingen voor de webapplicaties, evenals het technisch beheer voor deze omgevingen is uitbesteed aan een serviceorganisatie genaamd Secure Cloud Computing Services (SCCS).

VITALIS vindt het van groot belang voor haar reputatie en commerciële succes dat SCCS zorgdraagt voor een goede beheersing van de IT-diensten. De beide organisaties besluiten daartoe te werk te gaan volgens de werkwijze voor risicobeheersing in dit studierapport.

VITALIS onderkent dat ook de beheersingsmaatregelen in de bedrijfsprocessen en applicaties integraal onderdeel uitmaken van haar totale risicobeheersing, waaronder ook maatregelen om de webapplicaties te beschermen tegen typische dreigingen voor webapplicaties, zoals de OWASP Top 10-risico's. De beheersingsmaatregelen in de webapplicaties zijn als ontwerpeisen neergelegd bij WEBSOFT en vallen buiten de opdracht aan SCCS.

Stap 1.1 VITALIS bepaalt de bedrijfsrisico's

De uitkomst van deze stap is een beschrijving van de te beheersen bedrijfsrisico's van bedrijfsprocessen en bedrijfsgegevens.

Na uitvoering van een risicoanalyse door VITALIS, waaronder de beschouwing van dreigingen en kwetsbaarheden, trekt VITALIS de volgende conclusies:

- **De vertrouwelijkheid van de klantgegevens** dient te worden gewaarborgd. **Het risicoprofiel is hoog** in verband met de geldende privacywetgeving, de verwerking van creditcardbetalingen en de grote impact van reputatieverlies en claims bij incidenten.

[1] Deze casus is volledig fictief. Enige overeenkomst van bedrijfsnamen, systeemnamen, organisatiestructuur, configuratie of criteria met werkelijke situaties berust op toeval.

De business accepteert hooguit 1 beveiligingsincident per 7 jaar. Door het ontbreken van statistische gegevens over het effect van beheersingsmaatregelen, dient deze eis te worden geïnterpreteerd als een "zeer hoog niveau van beveiliging". Het risico blijkt niet verzekerbaar op een bedrijfseconomisch verantwoord kostenniveau, vanwege de beperkte winstmarges en een groot aantal recente incidenten in de branche.

- **De beschikbaarheid van het verkoopproces** – de webapplicaties – dient te worden gewaarborgd. Het **risicoprofiel is gemiddeld**, omdat bij een te lage beschikbaarheid en responsetijd potentiele klanten gemakkelijk naar concurrenten op internet overstappen en de reputatie van VITALIS schade oploopt, tenzij de verminderde beschikbaarheid algemeen geld voor de nationale markt (landelijke storingen en calamiteiten). De business wenst een beschikbaarheid van 99% dagelijks tussen 06.00 en 01.00 uur. In geval van ernstige calamiteiten dient uitwijk binnen 48 uur te zijn gerealiseerd en dient deze jaarlijks te worden getest.

- **De integriteit van het verkoopproces** – de webapplicaties – dient te worden gewaarborgd. Het **risicoprofiel is gemiddeld**, omdat een beperking van de integriteit kan leiden tot imagoschade en tot extra operationele kosten van herstel. Door de combinatie van procedurele en applicatieve beheersingsmaatregelen worden de financiële risico's minder dan hoog ingeschat.

Stap 1.2 VITALIS relateert de bedrijfsrisico's aan IT-diensten

De uitkomst van deze stap is een beschrijving van de te beheersen kwaliteitsaspecten (bijvoorbeeld de beschikbaarheid, integriteit en exclusiviteit) van IT-diensten.

De bedrijfsrisico's worden gerelateerd aan de volgende IT-diensten. (Er is tevens een e-maildienst en een telefonische helpdesk voor de klantenservice die beiden van belang zijn voor het verkoopproces, maar deze worden voor de eenvoud van de casus buiten beschouwing gelaten).

- De exclusiviteit van de productieomgeving van de webapplicaties dient te worden gewaarborgd, in het bijzonder de componenten waarop zich klantgegevens en creditcardgegevens (tijdelijk) bevinden en de componenten waarmee de toegangsbeveiliging wordt geregeld (two-factor authenticatiesysteem en directory server). (risicoprofiel: hoog).

  (De exclusiviteit binnen de webapplicaties, waaronder de applicatieve toegangsbeveiliging voor klanten en de end-to-end dataencryptie van de client-server communicatie door het SSL protocol, wordt geregeld binnen de applicaties en is voor

de eenvoud van deze casus de verantwoordelijkheid van WEBSOFT. VITALIS draagt zorg voor representatieve, fictieve (geanonimiseerde) data voor de acceptatieomgeving).

- De beschikbaarheid van de productieomgeving van de webapplicaties dient te worden gewaarborgd (risicoprofiel: gemiddeld).

  (De beschikbaarheid van de acceptatieomgeving is niet essentieel).

- De integriteit van de productieomgeving van de webapplicaties dient te worden gewaarborgd (risicoprofiel: gemiddeld).

- De integriteit van de acceptatieomgeving van de webapplicaties dient te worden gewaarborgd (risicoprofiel: laag).

Stap 1.3 VITALIS bepaalt de criteria voor risicobeheersing

De uitkomst van deze stap is een beschrijving van de beheersingscriteria voor de IT-diensten:
- voorgeschreven beheersingsmaatregelen (rule-based);
- beheersingsdoelstellingen (principle-based);
- service levels, statistische criteria en financiële criteria (principle-based).

Principle-based criteria

VITALIS wil SCCS zo veel mogelijk de vrijheid en verantwoordelijkheid geven om een mix van beheersingsmaatregelen te bepalen, rekening houdend met de kosten en baten, die passend zijn bij de actuele dreigingen op de dienstverlening en om schaalvoordelen te kunnen realiseren met haar dienstverlening aan andere klanten. Daarom stelt VITALIS "principle-based" de beheersingsdoelstellingen van toepassing volgens hoofdstuk 3 uit dit studie-rapport voor de acceptatie- en productieomgeving van de webapplicaties (omdat zowel de beschikbaarheid, integriteit als exclusiviteit van toepassing zijn, zijn alle beheersings-doelstellingen van hoofdstuk 3 van toepassing op de productieomgeving). Voor de beheersingsdoelstellingen worden service levels overeengekomen, die hier niet verder zijn uitgewerkt (b.v. de beschikbaarheid van 99% tussen 06.00 uur en 01.00 uur en de hersteltijd van 48 uur).

Rule-based criteria

De applicatieleverancier WEBSOFT draagt zorg voor de dataencryptie van de client-server communicatie. Daarom hoeft VITALIS op deze punten geen rule-based criteria te stellen aan SCCS. (Anders had zij specifieke eisen gesteld aan de encryptiemethode en sleutellengte).

VITALIS stelt de volgende rule-based criteria, vanwege hun invloed op het kostenniveau van de dienstverlening en vanwege van toepassing zijnde regelgeving:

a. Er dient een DMZ te worden gerealiseerd in het koppelvlak tussen de productie-omgeving en de onvertrouwde buitenwereld, inclusief Intrusion Detection System (IDS).

b. De productieomgeving van VITALIS dient two-factor authenticatie af te dwingen.

c. Alle toegang (intern/extern; lezen/muteren) tot medische klantgegevens dient te worden gelogd. De toegang dient herleidbaar te zijn tot individuele personen. De logging dient op een apart beheerde server te worden opgeslagen en dient minstens 18 maanden beschikbaar te zijn voor audits.

d. De medische klantgegevens dienen te worden vercijferd met het AES algoritme en een sleutellengte van tenminste 256 bits, of een sterkere methode, wanneer deze worden opgeslagen in een database of (tijdelijk) bestand.

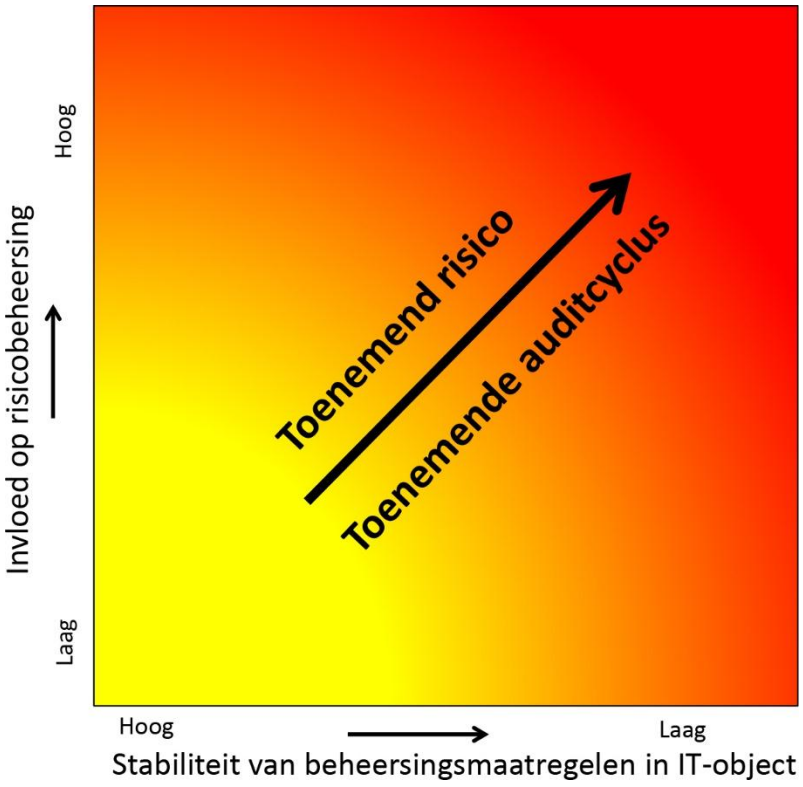
e. Vanwege de acceptatie van creditcards dient de omgeving te voldoen aan eisen van de PCI Data Security Standard.

<u>Assurance</u>

VITALIS verlangt periodiek een assurancerapport van de serviceorganisatie. Op basis van een risicoanalyse bepaalt VITALIS de periodiciteit en scope van het assurancerapport. Hierbij zijn met name van belang:

- De stabiliteit van de beheersingsmaatregelen in een object, de mate van verandering in de tijd, dynamiek en foutgevoeligheid (geautomatiseerde of handmatige maatregelen;
- Andere te ontvangen informatie inzake SCCS naast assurancerapport, denk aan service level rapportages. Hier zijn de periodiciteit en scope van deze service level rapportages van belang;
- Uitkomsten van voorgaande assurancerapportages, indien relevante afwijkingen zijn geconstateerd, is eerder een update gewenst;
- Geconstateerde incidenten.

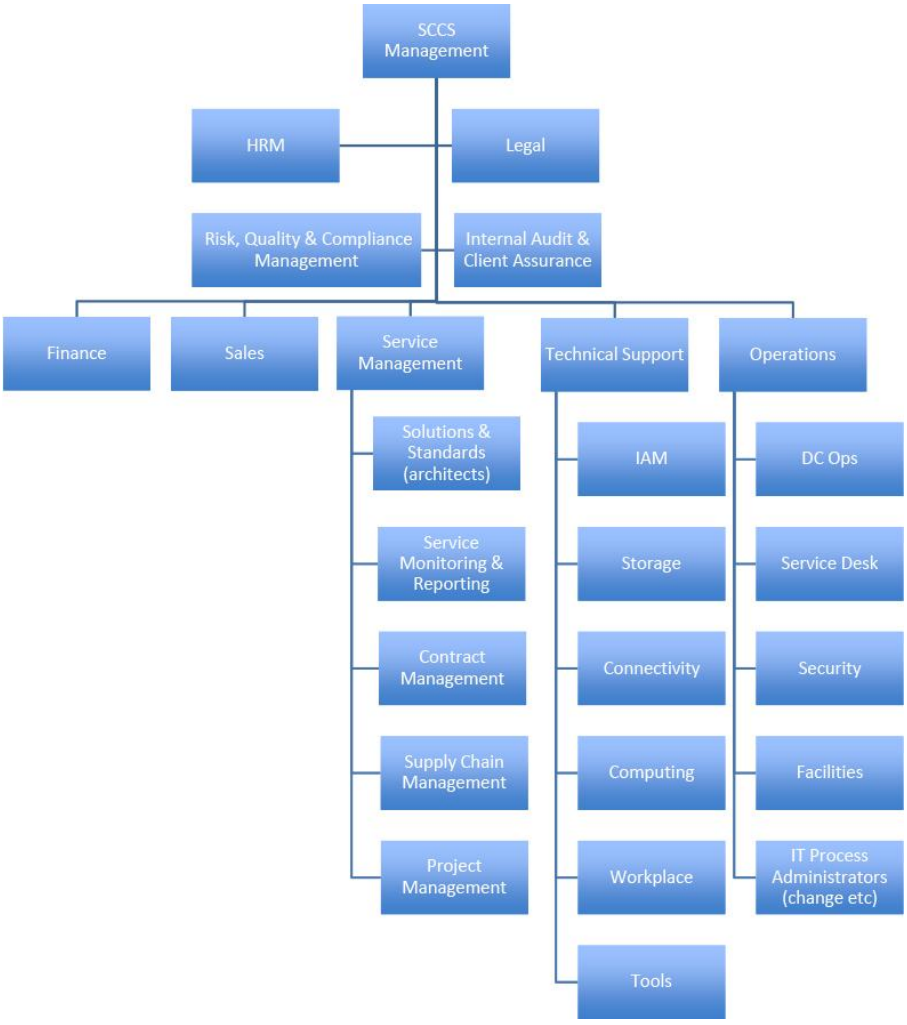
De scope en periodiciteit bepalen de assurancekosten, die door VITALIS worden gedragen.



Stap 2.2 Bepaal de relevante objecten van de IT-dienst

De uitkomst van deze stap is een inventarisatie van de objecten (IT-middelen, IT-beheerprocessen en organisatie) van de IT-dienst.

De serviceorganisatie SCCS ontwerpt de productieomgeving en acceptatieomgeving van de webapplicaties op basis van specificaties, die zijn verkregen van applicatiebouwer WEBSOFT. SCCS geeft hierbij invulling aan de opgegeven beheersingscriteria van VITALIS. Naast de productieomgeving en acceptatieomgeving ontwerpt SCCS ook de IT-organisatie en IT-beheerprocessen, althans voor zover die nog niet aanwezig waren.



Afbeelding 12: Organogram SCCS.

De serviceauditor inventariseert de relevante objecten van de IT-dienst, waarbij verschillende invalshoeken kunnen worden belicht (zie onderstaande afbeelding).

Afbeelding 13: Invalshoeken voor bepaling van relevante objecten van de IT-dienst.

De serviceauditor vergaart documentatie en interviewt medewerkers, zoals architecten, ontwerpers en beheerders van SCCS, om inzicht te krijgen in de voor de beheersing relevante objecten van de IT-dienst, waaronder:

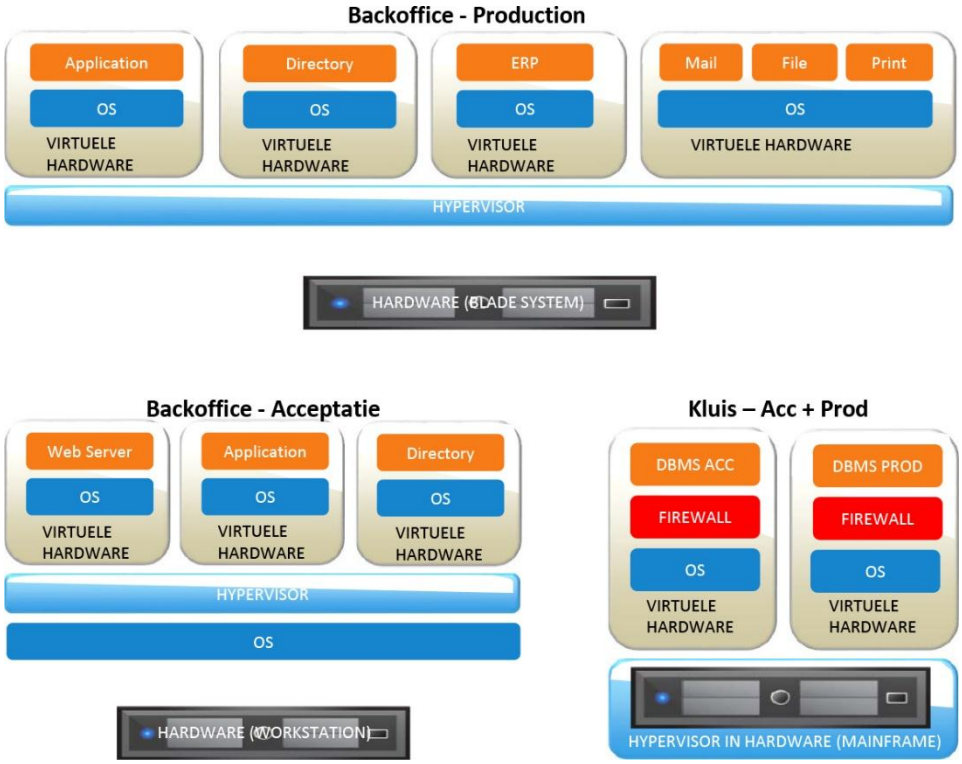
- Technisch ontwerp van WEBSOFT, om inzicht te krijgen in de relevante componenten van de webapplicaties.
- Technisch ontwerp van de infrastructuur met configuratieschema, opgesteld door de architecten van SCCS.
- Lijst van de relevante hardware en software configuration items (CI) uit de Configuration Management Database (CMDB), inclusief de acceptatieomgeving, de redundante middelen, virtuele en reële servers, met hun unieke CI-nummers, merk en typen.

Zoals bovenstaand is aangegeven, kan de serviceauditor afhankelijk van de beschikbare documentatie en medewerkers de invalshoeken kiezen, via welke de inventarisatie van IT-middelen geschiedt. Zo kan een serviceauditor er voor kiezen verkeerstromen te analyseren om zo volledig mogelijk infrastructurele en applicatieve IT-middelen in kaart te brengen, door drie typen verkeerstromen te analyseren:

- van applicatie naar applicatie;
- van gebruiker naar te benaderen gegevens;
- van beheerder naar beheerde IT-middelen.

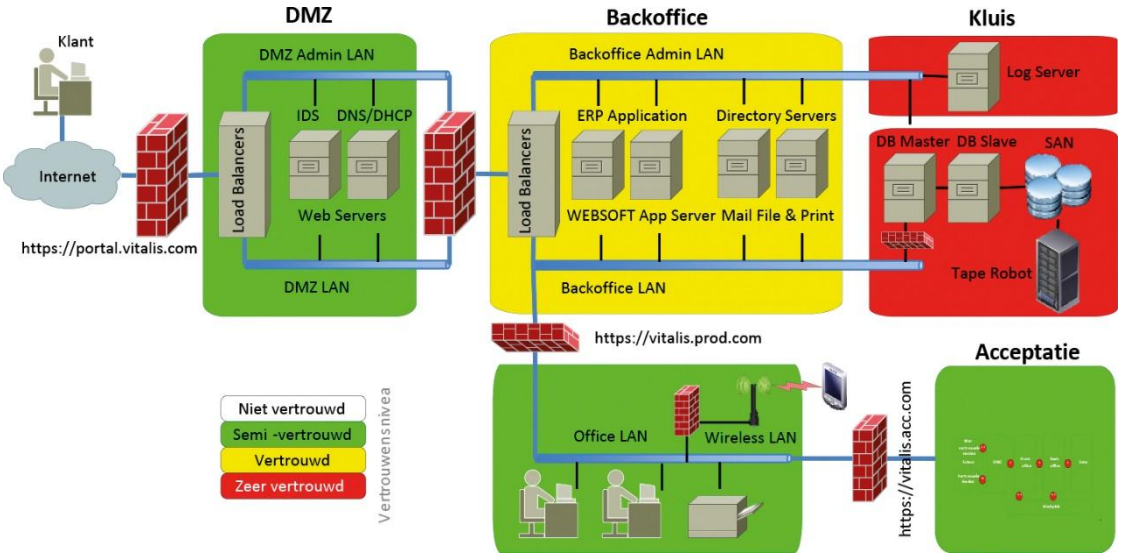
Zo is het in de casus VITALIS nuttig het toegangspad te analyseren van de internetgebruiker en van de interne medewerker, die elk toegang hebben tot data in de kluis. Ook is het van belang te constateren dat de beheerder in geen enkele afbeelding is weergegeven, maar er zal wel een toegangspad zijn van beheerder naar de beheerde IT-middelen. Via interviews kan de analyse van verkeerstromen dan ook leiden tot een juist en volledig beeld van IT-middelen.

De serviceauditor gaat voor iedere applicatie- en datacomponent na op welk IT-middel deze zich bevindt. Ook gaat de serviceauditor na, mede aan de hand van het beschouwingsmodel voor zonering en de overige attentiepunten in afbeelding 13, of er geen relevante IT-middelen over het hoofd worden gezien. Zodoende identificeert de auditor dat er voor een aantal systemen virtualisatie wordt toegepast, zie afbeelding 14. De overige systemen (DMZ-systemen,logserver) zijn standalone servers. Ook wordt opgemerkt, dat op de productie blade server ook virtuele servers draaien van andere klanten van SCCS.



Afbeelding 14: Virtualisatie van backoffice servers.

De serviceauditor krijgt het volgende beeld van de relevante infrastructuur en stemt dit beeld af met de serviceorganisatie.



Afbeelding 15: Configuratieschema SCCS infrastructuur voor VITALIS.

De serviceauditor inventariseert de relevante IT-beheerprocessen aan de hand van paragraaf 3.2 (relatie tussen beheersingsdoelstellingen en beheerprocessen). Ook identificeert de serviceauditor IT-middelen die worden gebruikt ter ondersteuning van de IT-beheerprocessen, b.v. software voor scheduling, signalering & monitoring, change management.

De serviceauditor inventariseert vervolgens de organisaties (afdelingen, vestigingen, externe leveranciers) die verantwoordelijk zijn voor de beheerprocessen per relevante IT-component en voor het technisch beheer per IT-component.

Hierbij blijkt dat het grootste deel van de "kluis"-omgeving wordt beheerd door een gespecialiseerde leverancier van oplossingen voor dataopslag, Enterprise Mass Storage Systems (EMS²). EMS² beheert het mainframe, inclusief operating systems, access control subsysteem en DBMS; verder ook het Storage Area Network (SAN) en tape robot met tape management systeem. Deze systemen staan opgesteld in een apart deel van het rekencentrum van SCCS, waarvan de fysieke beveiliging de verantwoordelijkheid is van SCCS. Het contract met EMS² stelt de auditor in staat om de kluisomgeving volledig in de scope van de audit te betrekken.

Stap 2.3 Bepaal de relevante algemene beheersingsmaatregelen van de IT-dienst

De uitkomst van deze stap is een beschrijving van alle, voor de risicobeheersing relevante, beheersingsmaatregelen van de IT-dienst.

Het bepalen van de algemene beheersingsmaatregelen hangt samen met de bedreigingen en kwetsbaarheden (risico's) voor de beheersingscriteria en IT-beheersingsdoelstellingen. De gevoeligheid van de IT-diensten en het dreigingsbeeld moeten de keuze bepalen van de beheersingsmaatregelen. Externe dreigingen betreffen bijvoorbeeld hackers en virussen, maar ook 'Acts of God' zoals brand- en wateroverlast. Interne dreigingen betreffende bijvoorbeeld fouten en fraude, maar ook technische mankementen aan IT-middelen.

De serviceorganisatie selecteert een passend stelsel van beheersingsmaatregelen en legt dit vast in een beveiligingsontwerp. Hierbij wordt een passende combinatie van maatregelen geselecteerd voor de IT-configuratie (samenhang tussen IT-componenten, zie hoofdstuk 5), voor de IT-middelen (inrichting van individuele IT-middelen, zie hoofdstuk 5) en voor de IT-beheerprocessen (zie hoofdstuk 6), rekening houdend met de rule-based beheersings-maatregelen die zijn voorgeschreven door VITALIS.

De serviceauditor toetst of het geselecteerde stelsel van beheersingsmaatregelen passend is gegeven de bedreigingen en kwetsbaarheden, althans voor dat deel van de dienstverlening waarvoor de klantorganisatie een audit wenst. (Zoals in stap 1.3 is aangegeven, zal de kantorganisatie de scope en periodiciteit van audits bepalen, mede rekening houdend met de kosten die dat met zich meebrengt).

Einde casus VITALIS

Bijlage B: Begrippenlijst

- Assurance-rapport (voorheen ook wel Third Party Mededeling of TPM). Een rapport van een onafhankelijke auditor ten behoeve van de klantorganisatie(s) over beheersingsaspecten van een serviceorganisatie.

- Baseline. Een verzameling van technische beheersingsmaatregelen of instellingen voor de inrichting van een IT-middel, zonder rekening te houden met de eisen van een specifieke IT-dienst. Een baseline fungeert als uitgangspunt voor de beveiligingsstandaarden van specifieke IT-diensten.

- Beheersbaarheid. De mate waarin het object kan worden aangestuurd en/of bijgestuurd, zodat het object bij voortduring aan de daaraan te stellen eisen kan voldoen.

- Bekende fout (known-error). Een probleem waarvan de basisoorzaak bekend is en waarvoor een tijdelijke work-around of een permanent alternatief bekend is. Een known error bestaat totdat het probleem permanent is opgelost.

- Beschikbaarheid. De mate waarin een object (informatie, IT-dienst of IT-middel) continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.

- Beveiligingsontwerp. Een verzameling van zowel procedurele als technische beheersingsmaatregelen gericht op de afdekking van risico's van exclusiviteit, integriteit, beschikbaarheid en controleerbaarheid voor een (groep van) IT-dienst(en).

- Beveiligingsstandaard. Een verzameling van technische beheersingsmaatregelen of instellingen voor de inrichting van een IT-middel gericht op een specifieke IT-dienst.

- Beveiligingsplan. Een (verbeter)plan van te implementeren beheersingsmaatregelen van het beveiligingsontwerp.

- Calamiteit. Een calamiteit wordt gedefinieerd als een ongeplande situatie waarbij verwacht wordt dat de duur van het niet-beschikbaar zijn van één of meer IT-diensten afgesproken drempelwaarden zal overschrijden en de herstelde IT-diensten enkel en alleen op een andere IT-middel en/of op een andere locatie kan worden voortgezet waarbij de daarvoor benodigde acties niet tot de dagelijke routine behoren.

- Configuration item (CI). IT-middel dat van belang is voor een te leveren IT-dienst.

- Configuration management database (CMDB). Een gestructureerde verzameling van gegevens (database) van relevante details van configuration items en gegevens over hun onderlinge relaties.

- Controleerbaarheid. De mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en werking van een object. Tevens omvat dit kwaliteitsaspect de mate waarin het mogelijk is vast te stellen dat de gegevensverwerking in overeenstemming met de eisen ten aanzien van de overige kwaliteitsaspecten is uitgevoerd.

- Exclusiviteit. De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruikmaken van een object (IT-dienst of IT-middel) of toegang hebben tot een object (creëren, wijzigen, verwijderen of lezen van gegevens).

- IT-beheerproces. Een IT-beheerproces is een bedrijfsproces van een serviceorganisatie dat zich richt op het beheer van een IT-dienst.

- IT-dienst. De functie die (een groep van) IT-middelen vervullen voor de klantorganisatie. Een IT-dienst dient niet te worden verward met een IT-beheerproces. Een serviceorganisatie kan zowel een IT-dienst als een IT-beheerproces als dienst leveren aan een klantorganisatie.

- IT-middel. Een (fysiek of logisch) technisch middel (zoals hardware, software, applicatie of faciliteit) waarmee een IT-dienst, geheel of gedeeltelijk en direct of indirect, wordt gerealiseerd.

- Incident. Onder incident wordt verstaan elke gebeurtenis, die niet tot de standaardoperatie van een IT-service behoort en die een interruptie in of een vermindering van de kwaliteit van die service kan veroorzaken. Onder incident worden niet verstaan: elk verzoek van de gebruiker om ondersteuning, levering van informatie, advies of documentatie (ook wel aangeduid als “Service Request”).

- Integriteit. De mate waarin het object (gegevens, IT-dienst of IT-middel) in overeenstemming is met de beoogde werkelijkheid.

- Key-control. Beheersingsmaatregel die in iedere organisatie, groot of klein, aanwezig mag worden geacht. Het ontbreken van de maatregel is ongebruikelijk en vraagt om onderbouwing. Key-controls hoeven niet in iedere situatie afdoende te zijn om de risico’s volledig af te dekken. Elke organisatie dient te evalueren of overige maatregelen nodig zijn in de eigen situatie.

- Klantauditor. De (interne of externe) auditor van de klantorganisatie (in de Engelstalige vakliteratuur meestal aangeduid als “user auditor”);
- Klantorganisatie. De (interne of externe) afnemer van IT-diensten (in de Engelstalige vakliteratuur meestal aangeduid als “user organisation” of “client organisation”);
- Normale bedrijfsomstandigheden. Bedrijfsomstandigheden waarbij de IT-diensten beschikbaar zijn, dan wel waarbij het niet-beschikbaar zijn is afgesproken of een afgesproken drempelwaarde niet overschrijdt.
- Operational level agreement. Een interne overeenkomst tussen onderdelen van de serviceorganisatie over de levering van IT-diensten.
- Prestatie-indicator. Een maatstaf die een indicatie geeft van de prestatie van het proces.
- Prestatieniveau (service level). Een concrete waarde van een prestatie-indicator.
- Probleem. Een onbekende, achterliggende oorzaak van één of meer incidenten.
- Productieopdracht. Een handeling in de productieomgeving met gebruikersgegevens die wordt uitgevoerd door de serviceorganisatie in opdracht van de klantorganisatie, bijvoorbeeld batchverwerking, backup en restore van gegevens, en mutatie van gebruikersgegevens met beheertools.
- Service Level Agreement. Een overeenkomst tussen de serviceorganisatie en een klantorganisatie waarin afspraken worden vastgelegd over de te leveren IT-diensten. Het Service Level Agreement dient, gedurende de looptijd, als norm voor het meten en sturen van de IT-dienst.
- Serviceauditor. de (interne of externe) auditor van de serviceorganisatie (in de Engelstalige vakliteratuur meestal aangeduid als “service auditor”).
- Serviceorganisatie. De (interne of externe) leverancier of beheerder van IT-diensten ten behoeve van een klantorganisatie (in de Engelstalige vakliteratuur meestal aangeduid als “service organisation”); een serviceorganisatie van een serviceorganisatie wordt aangeduid als een subserviceorganisatie.
- Subserviceorganisatie. De (interne of externe) leverancier of beheerder van IT-diensten ten behoeve van een serviceorganisatie.

- Vertrouwelijkheid. De mate waarin uitsluitend geautoriseerde personen via geautoriseerde procedures en beperkte bevoegdheden kennisnemen van gegevens. (Vertrouwelijkheid kan worden gezien als een subset van exclusiviteit).
- Wijziging. Elke toevoeging, verandering of verwijdering in een IT-dienst of IT-middel.
- Work-around. Een methode om een incident of probleem te voorkomen, enerzijds door een tijdelijke oplossing (fix) of anderzijds door de klant niet meer afhankelijk te maken van de service waarbij het probleem is geconstateerd.

Bijlage C: Literatuurverwijzingen

1. Studierapport NOREA / PvIB, Normen voor de beheersing van uitbestede ICT-beheerprocessen, 2007.

2. Patronen informatiebeveiliging versie 1.0, Platform Informatiebeveiliging (PvIB), 2013.

3. CobiT 5, IT Governance Institute, ISBN 978-1-60420-237-3, 2012.