COMPACT

TIJDSCHRIFT EDP-AUDITING

NORMERING

1996/1

Prinses Margrietlaan 3
2404 HA Alphen aan den Rijn
Postbus 4
2400 MA Alphen aan den Rijn
Telefax (0172) 47 59 33

Postbank 6204
Bankrelatie:
ABN-AMRO Bank N.V.
Alphen aan den Rijn
Rekeningnr. 56 91 39 449

Samsom BedrijfsInformatie bv

Telefoon (0172)	ons kenmerk	datum
466800	OR/96094/idk	februari 1996

Betreft: Compact 1996

Geachte lezer,

Compact heeft een goed jaar achter de rug. Uit ons recent gehouden onderzoek onder de lezers komt naar voren dat Compact bijzonder goed gewaardeerd wordt. Compact wordt gezien als hét tijdschrift op het vakgebied EDP-auditing, een vakgebied dat nog steeds volop in ontwikkeling is. Om nu goed te kunnen inspelen op al die ontwikkelingen is besloten dit jaar **zesmaal** te verschijnen.

Dit jaar verschijnt Compact in februari, april, juni, augustus, oktober en december. Het nummer dat voor u ligt kent het thema "normering".

Wij vertrouwen erop dat u veel profijt zult hebben van de verhoging van de frequentie van Compact.

Met vriendelijke groet,
Samsom BedrijfsInformatie bv

Oscar Rouwendal
uitgever

Compact ®
Jaargang 23, nummer 1
Een uitgave van KPMG EDP Auditors NV en Samsom Bedrijfs-Informatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers
Drs. R.G.A. Fijneman RE RA
Drs. P. Veltman RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Prof.dr. J.C. Arnbak
J.H. Buisman RA
Mr. P. van Dijken
Prof.mr. H. Franken
Dr. K.IJ. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Redactiesecretariaat
Mw. I. de Koning, Samsom Bedrijfsinformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 746
Fax : 0172 – 466 569
Vormgeving
Bureau Karakter, Delft
Opmaak
Sander Pinkse Boekproduktie, Amsterdam
Abonnementen
f 165,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom BedrijfsInformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax : 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

Uitgever
Drs. ing. O.A. Rouwendal

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: • beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG, KPMG EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij Samsom Bedrijfsinformatie BV, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

Voor de EDP-auditor vormen normen en standaarden een onontbeerlijk instrument bij de beroepsuitoefening. Indien een EDP-audit wordt uitgevoerd zonder eenduidige normen of standaarden, aldus Paans, begeeft de EDP-auditor zich op dezelfde weg als de informatici die een informatiesysteem bouwen zonder functioneel ontwerp. Het gevolg is dat de audit wordt gekenmerkt door ongestructureerdheid en incompleetheid. In zijn inaugurele rede komt Moonen dan ook onder meer tot de aanbeveling dat gestructureerd overleg in gang wordt gezet tussen informatiekundigen en EDP-auditors over standaardisatie van het kwaliteitsbegrip op het gebied van de informatievoorziening en de informatietechnologie en de te hanteren kwaliteitsnormen.

Normen en standaarden zijn het onderwerp van dit themanummer van Compact, maar wat zijn dat eigenlijk, en wat zijn de eventuele verschillen? Omdat hierover in het vakgebied EDP-auditing geen eenheid van opvatting lijkt te bestaan, heeft de redactie in deze bijdrage enige beschouwingen aan deze vraagstelling gewijd. Hiertoe heeft zij de nieuwe editie van de Winkler Prins-encyclopedie en het Nederlands Normalisatie-instituut geraadpleegd.

De Winkler Prins (WP) geeft als definitie van norm (in de metrologie) 'een door een normalisatiecommissie opgestelde richtlijn (aanbeveling) tot uniformering op een bepaald gebied (bijvoorbeeld afmetingen en/of uitvoeringswijze van onderdelen, meeteenheden en/of meetmethoden, toe te laten grenswaarden, nomenclatuur)'.
In de sociale wetenschappen is een norm een gedragsregel in het intermenselijk verkeer, aldus de WP. Deze betekenis van norm lijkt niet direct van belang voor het vakgebied EDP-auditing, maar is dat mogelijk toch wel.

Een standaard (in de metrologie) definieert de WP als 'een tot norm gekozen waarde, dienend voor het definiëren van andere waarden'. Dit houdt in dat een *waarde* – de WP noemt als voorbeeld een kilogram – door keuze een norm kan worden, en daarmee (per definitie) een standaard (in het voorbeeld: standaardkilogram).

Het verschil tussen norm en standaard volgens de WP-definities lijkt te zijn dat een norm van alles kan zijn (waaronder een grenswaarde), maar dat een standaard uitsluitend een norm*waarde* is, een deelverzameling derhalve van norm. In het licht van de vele IT-'standaarden', al dan niet 'de jure' of 'de facto', lijkt de WP-definitie van standaard onvoldoende empirische basis te hebben, althans op het gebied van informatietechnologie.

Het Nederlands Normalisatie-instituut (NNI) hanteert de volgende definitie van norm: 'een document, opgesteld met consensus en goedgekeurd door een erkende instelling, dat voor gemeenschappelijk en herhaald gebruik regels, richtlijnen of kenmerken bevat met het doel zoveel mogelijk orde te bereiken in een bepaalde context'. 'Normen zijn gebaseerd op de gezamenlijke resultaten van wetenschap en praktijk', zo voegt het NNI er nog aan toe.

Een definitie van standaard geeft het NNI niet. Wel bevat NEN 5050, die gaat over ontraden/foute termen en aanbevolen termen, een toelichting op de begrippen standaardisatie en normalisatie:
'Standaardisatie is het brengen van uniformiteit in produkten, produktiemiddelen en diensten bij een bedrijf of groep van bedrijven (...).
Normalisatie is het in gezamenlijk overleg van alle belanghebbende groeperingen opstellen van regels voor de eigenschappen van produkten en diensten ter bevordering van het economisch verkeer.'

Deze toelichting kan aldus worden geïnterpreteerd dat standaardisatie een leveranciersaangelegenheid is (gelet op: 'produktiemiddelen' en 'bedrijf of groep van bedrijven'), terwijl bij normalisatie tevens de afnemers betrokken zijn (geen vermelding van produktiemiddelen, 'alle belanghebbende groeperingen'). Volgens deze gedachtengang ontstaan er eerst (leveranciers)standaarden, die door een erkende instelling eventueel tot norm kunnen worden verheven.
Als bezwaren tegen de toelichting van het NNI kunnen naar voren worden gebracht dat niet duidelijk wordt gemaakt wat het verschil is tussen 'het brengen van uniformiteit' en 'het opstellen van regels voor eigenschappen', en dat bij standaardisatie een doelstelling ontbreekt ('bevordering van het economisch verkeer' wellicht?).

Nuanceverschillen tussen de definities van de WP en die van het NNI zijn ten eerste dat de WP uniformering als een doelstelling van een norm ziet, terwijl het NNI uniformiteit juist kenmerkend acht voor standaardisatie. Een tweede mogelijk verschil is dat bij de WP een norm(waarde) vooraf lijkt te gaan aan een standaard, wat bij het NNI precies andersom is.

De belangrijkste taak van het NNI is inmiddels verschoven van het uitbrengen van Nederlandse normen naar het hebben van een inbreng bij instituten die internationale normen uitbrengen. Het NNI is hiertoe lid van het Comité Européen de Normalisation (CEN) en van de International Organization for Standardization (ISO). Hierbij valt op dat in de Angelsaksische wereld wordt gesproken van standaardisatie, terwijl op het continent van Europa voor hetzelfde proces de term normalisatie wordt gehanteerd.

De redactie houdt het erop dat norm en standaard, en normalisatie en standaardisatie, in de meeste situaties als synoniem kunnen worden beschouwd. Een mogelijke nuancering hierbij is dat standaarden primair ontstaan vanuit de industrie (aanbodzijde), terwijl bij normen de vraagzijde 'per definitie' een inbreng heeft (via de 'normalisatie-

commissie' van de WP of de 'erkende instelling' van het NNI). Deze nuancering gaat waarschijnlijk niet op voor de Angelsaksische situatie.

Een complicatie bij dit alles is dat in het vakgebied EDP-auditing norm in een andere betekenis wordt gebruikt dan in de gangbare betekenissen van de WP en het NNI, die beide een essentiële rol toekennen aan een erkende instelling bij het opstellen van een norm. Normen die bij EDP-audits worden toegepast, zijn meestal situatie-afhankelijke, niet zelden enigszins subjectieve, in algemene bewoordingen geformuleerde aanbevelingen of eisen, bij de totstandkoming waarvan geen normalisatiecommissie te pas is gekomen. Voor norm in deze betekenis wordt in de Angelsaksische auditpraktijk meestal de term 'objective' (doelstelling) gehanteerd, die zowel betrekking kan hebben op het auditobject ('control objective') als op de audit ('audit objective').
De conclusie hiervan kan zijn dat EDP-auditing een eigen definitie van norm moet ontwikkelen – en hieraan bekendheid moet geven – of moet uitzien naar een andere term.

De reden voor deze lange en academische inleiding is de ervaring van de redactie dat het onderwerp van normen en standaarden ernstige meningsverschillen kan uitlokken, waarbij soms emoties de overhand krijgen. Dit heeft misschien te maken met de sociaal-wetenschappelijke betekenis van norm: een gedragsregel in het intermenselijk verkeer (een fatsoensnorm).

Met deze overwegingen wil de redactie u tot steun zijn bij het lezen van de artikelen in dit nummer en bij het nuanceren van de inhoud. Vooral het openingsartikel, met als titel Normbesef, bevat een aantal uitspraken die als provocerend kunnen worden ervaren. Dit te meer daar de titel appelleert aan de betekenis van norm als fatsoensnorm.

Terwijl het openingsartikel een theoretische invalshoek heeft, gaan de overige artikelen vooral in op de praktische bruikbaarheid van bestaande normen of standaarden voor de EDP-auditor. Behandeld worden de ISO 9000-normen, de managementprocessen zoals beschreven in de IT Infrastructure Library (ITIL) en de beveiligingsrichtlijnen van de Code voor Informatiebeveiliging.

De redactie wenst u veel leesplezier en ontvangt gaarne – in het algemeen, maar in het bijzonder met betrekking tot dit toch wat controversiële onderwerp van normen en standaarden – uw reacties.

Drs. P. Veltman RE RA

Toekenning mr. dr. J.H.R. Sinninghe Damsté-prijs 1995

Tijdens de ledenvergadering van het Nederlands Instituut van Registeraccountants van 14 december jl. is de mr.dr. J.H.R. Sinninghe Damsté-prijs 1995 uitgereikt aan R.A. Jonker RA wegens bekroning van zijn publikatie 'Geautomatiseerde gegevensbewerking en jaarrekeningcontrole' in het winternummer 1994 van Compact.
De redactie wenst de auteur van harte geluk met de toekenning van deze prijs.

Normbesef

L. Annokkée RE en
B. Sebregts RE

Het kernprobleem bij het uitvoeren van een EDP-auditopdracht is het vaststellen van het stelsel van kwaliteitsnormen dat in de specifieke situatie de toetssteen vormt. Vanuit dit vertrekpunt geven de auteurs hun visie op het begrip norm, waarbij zij ingaan op de mogelijke bronnen van normen, de classificatie-mogelijkheden en de toepasselijke metanormen.

INLEIDING

In het vakgebied EDP-auditing maakt men onderscheid tussen uitvoerings- en kwaliteitsnormen. Uitvoeringsnormen zijn normen die beogen een systematische en achteraf verifieerbare uitvoering van de EDP-auditopdracht te waarborgen. Kwaliteitsnormen zijn normen op basis waarvan de oordeelsvorming met betrekking tot één of meer kwaliteitseigenschappen van een bepaald auditobject tot stand komt. In dit artikel komen alleen de kwaliteitsnormen aan bod. Dit houdt ook in dat we voorbij gaan aan de zogenaamde forensische audits, waarbij niet zozeer de kwaliteit, maar de waarheidsvinding centraal staat.

Het resultaat van een EDP-auditopdracht moet een oordeel zijn over de mate waarin het object van audit aan een vooraf vastgesteld stelsel van kwaliteitsnormen voldoet, eventueel (indien gewenst en van toepassing) aangevuld met adviezen om de aangetroffen situatie te verbeteren. Het kernprobleem daarbij is het vaststellen van het stelsel van kwaliteitsnormen (normconcretisering) dat bij een specifieke EDP-auditopdracht de toetssteen is. Omdat er (nog) geen sprake is van op specifieke auditopdrachten gerichte normenstelsels, neemt de EDP-auditor meestal zijn toevlucht tot het in gezamenlijk overleg met de opdrachtgever vaststellen van het te hanteren normenstelsel. Meestal is voor de opdrachtgever de wezenlijke betekenis van dat normenstelsel, in termen van risicobeheersing, onvoldoende duidelijk. Misschien geldt dit ook wel, zij het in mindere mate, voor de EDP-auditor.

In het vervolg van dit artikel komen eerst de normen zelf aan de orde, waarbij we achtereenvolgens aandacht besteden aan de bronnen waaraan normen ontleend kunnen worden en hoe normen naar verschillende gezichtspunten zijn te classificeren. De in dit verband aan de orde komende indelingen, begrippen en begripsomschrijvingen berusten op persoonlijke inzichten, die mede gevormd zijn door geraadpleegde literatuur.
Vervolgens is ingegaan op de zogenoemde metanormen, dat wil zeggen normen waaraan 'normen' op het vakgebied van de EDP-auditing moeten voldoen. Daarna is, in algemene zin, aandacht besteed aan de bruikbaarheid van bekende standaarden, omdat de opdrachtgever daarmee meestal een zekere affiniteit heeft. Over de metanormen en de bruikbaarheid van bekende standaarden is volgens ons tot op heden weinig gepubliceerd, en voor zover dat wel het geval is blijken er verschillen van inzicht te bestaan. Dit artikel tracht een impuls te geven aan de meningsvorming over deze twee thema's, met als doel de verdere ontwikkeling van het vakgebied te bevorderen. Ook voor deze twee thema's geldt, en zelfs in een sterkere mate, dat onze persoonlijke inzichten zijn weergegeven.
Vervolgens zijn enige woorden gewijd aan de lopende activiteiten op dit gebied en de huidige stand van zaken. Het artikel wordt afgesloten met een conclusie die betrekking heeft op de invloed die de theoretische ontwikkeling van het vakgebied kan hebben op de beroepsbeleving van de EDP-auditor.

NORMEN

Beoordelen impliceert het toetsen aan een norm. De begrippen normen en standaarden blijken zowel in de praktijk als in de literatuur veel verwarring te zaaien omdat men deze begrippen vaak door elkaar gebruikt. In deze context verstaan wij onder een norm 'een richtwaarde waaraan een specifiek onderdeel van het auditobject moet voldoen'. In die zin is een norm te beschouwen als de meest gepreciseerde eenheid van toetsing. Op een auditobject zijn doorgaans meerdere normen van toepassing. Voor het samenstel van deze normen hanteren wij het begrip normenstelsel. Als een normenstelsel een bepaalde status krijgt omdat bepaalde gezaghebbende instanties het betrokken normenstelsel onderschrijven, dan spreken wij van standaarden.

Herkomst van normen

Normen kan men onder andere aan de volgende bronnen ontlenen:

- het vakgebied administratieve organisatie, bijvoorbeeld controletechnische functiescheidingen, de informatiebehoeften;
- het vakgebied bedrijfseconomie, bijvoorbeeld de wijze waarop investeringen moeten worden beoordeeld;
- het vakgebied informatica, bijvoorbeeld systeemontwikkeling, het gebruik en beheer van informatiesystemen;
- wettelijke voorschriften, bijvoorbeeld de Wet op de jaarrekening, de Wet persoonsregistraties, de Wet computercriminaliteit, Europese aanbestedingsregels;
- publikaties van normalisatie-instituten, bijvoorbeeld NNI, ISO/IEC, ANSI/IEEE, CEN/CENELEC;
- standaardisatie- en overige organisaties, bijvoorbeeld ECMA, EWOS, EC, UN, CCITT;
- brancheverenigingen, bijvoorbeeld COSSO en VIFKA, waartoe wij ook de zogenoemde standaardcontracten Binnenlandse Zaken rekenen die de Rijksoverheid hanteert, omdat die in overleg met de COSSO en VIFKA zijn opgesteld;
- organisaties die zich bezighouden met het verzamelen, systematisch vastleggen en verwerken van gegevens die op het toepassen van informatietechnologie betrekking hebben, zoals Nolan Norton, Gartner group, Compass (benchmarking);
- organisaties die (mede) een toezichthoudende taak hebben, zoals De Nederlandsche Bank die een memorandum heeft uitgebracht ([DNB88]);
- publikaties van gezaghebbende organisaties en commissies die werkzaam zijn op aanverwante gebieden, zoals het Koninklijk NIVRA, het Committee of Sponsoring Organizations of the Treadway Commission ([COSO92]);
- normen die door het hoogste management zijn vastgelegd in het informatiebeleid en de nadere uitwerking daarvan in bijvoorbeeld het informatiebeveiligingsbeleid.

Classificatie van normen

Men kan normen naar verschillende invalshoeken classificeren, zoals naar: objectiviteit, naar formulering, naar schaalbaarheid, naar geldigheidsgebied, naar precisering, naar gezaghebbendheid, naar kwaliteitseigenschappen en dergelijke. De meeste van deze classificaties hebben betekenis als het gaat om het beantwoorden van de vraag in hoeverre een norm op een gezonde basis berust (deugdelijke grondslag) en concreet is.

Een norm is een richtwaarde waaraan een specifiek onderdeel van het auditobject moet voldoen.

Objectiviteit
Voor de invalshoek 'objectiviteit' is de volgende aan [Moon91] ontleende classificatie denkbaar:

- *Objectief*, hetgeen in deze context wil zeggen dat de norm vrij is van persoonlijke beïnvloeding, dat is bijvoorbeeld het geval als de norm gebaseerd is op principes uit de leer van de organisatiekunde, de administratieve organisatie, de leer van de accountantscontrole, de bedrijfseconomie, etc. Toch kan ook hier sprake zijn van persoonlijke beïnvloeding omdat deze principes in het algemeen nogal wat ruimte laten voor interpretatie.

- *Subjectief*, hetgeen in deze context wil zeggen dat er bij het vaststellen van de norm sprake is geweest van persoonlijke beïnvloeding (professional judgement). In een dergelijke situatie kan men trachten de norm voor die specifieke audit te objectiveren door daarover overeenstemming te bereiken met iedereen die belang heeft bij die audit. In een dergelijke situatie zou men ook kunnen spreken van geobjectiveerde normen.

- *Opgelegd*, hetgeen in deze context wil zeggen dat men onderworpen is aan normen die door de wetgever of door gezaghebbende instanties zijn bepaald. Daarbij kan gedacht worden aan de Wet persoonsregistraties, de Wet computercriminaliteit, het Memorandum van De Nederlandsche Bank ([DNB88]). Opgelegde normen kunnen ook als objectieve normen worden opgevat.

De mate waarin een norm objectief is, bepaalt mede de stelligheid van het oordeel waarin een EDP-audit uitmondt (deugdelijke grondslag). In die zin is objectiviteit een belangrijk aspect.

Formulering
Normen kan men op verschillende manieren formuleren. Op basis daarvan is de volgende classificatie denkbaar:

- *doelstelling:* bijvoorbeeld, er wordt naar gestreefd dat de beschikbaarheid van het netwerk 99 procent is bij een maximale uitvaltijd van vier uur;

- *eisen:* voorwaarden waaraan in elk geval voldaan moet worden (randvoorwaarden), bijvoorbeeld maximaal toelaatbare/geaccepteerde responstijden om bijvoorbeeld irritaties bij de gebruikers van informatiesystemen te voorkomen;
- *referentiepunten:* door bijvoorbeeld de kosten van de informatievoorziening in verhouding tot de omzet te vergelijken met het gemiddelde overeenkomstige cijfer bij soortgelijke bedrijven (benchmarking). Vanuit een oogpunt van concurrentieverhoudingen kan dit van groot belang zijn;
- *richtlijnen:* uitgangspunten waarvan alleen gemotiveerd mag worden afgeweken, bijvoorbeeld: de richtlijn is als systeemontwikkelingsmethode SDM-2 te gebruiken, maar daarvan mag worden afgeweken als in een specifieke situatie het gebruik van een andere methode de voorkeur verdient.

De mate waarin een norm objectief is, bepaalt mede de stelligheid van het oordeel waarin een EDP-audit uitmondt.

Het punt van de formulering lijkt niet echt belangrijk. Toch is het goed zich te realiseren dat men vaak met de opdrachtgever over de normstelling moet overleggen en dus de manier van formuleren van invloed is op het communicatieproces.

Schaalbaarheid
Een norm is te beschouwen als een beoogde of vereiste 'meetwaarde'. De betekenis van deze waarde wordt slechts duidelijk als men deze waarde op een zogenoemde meetschaal kan projecteren. Op normen kunnen verschillende meetschalen van toepassing zijn, op grond waarvan zij geclassificeerd kunnen worden. In [SERC92] komt de volgende classificatie van meetschalen voor:
- *kwalitatieve meetschalen,* die men verder, naar toenemende graad van nuancering, onderverdeelt in een nominale meetschaal en een ordinale meetschaal;
- *kwantitatieve meetschalen,* die men verder, ook op grond van een grotere mate van nuancering, heeft onderverdeeld in een intervalschaal en een ratioschaal.

De meetschaal waarin een norm is uitgedrukt en waaraan de waargenomen werkelijkheid wordt getoetst, is bepalend voor de mate van concreetheid waarmee een EDP-auditor zijn oordeel kan uitspreken en zijn adviezen kan geven.

Domein
Door organisaties uitgebrachte standaarden kunnen grote en minder grote delen van het werkterrein van de EDP-auditor bestrijken. Op grond daarvan is een classificatie van normenstelsels mogelijk met als uitersten:
- *groot:* bijvoorbeeld NEN-ISO 9001 *(Kwaliteitssystemen. Model voor de kwaliteitsborging bij het ontwerpen/ontwikkelen, het vervaardigen, het installeren en de nazorg),* die een groot deel van het werkterrein van de EDP-auditor beslaat;
- *klein:* bijvoorbeeld ANSI/IEEE Std 1008-1987 *(Software Unit Testing),* die alleen op het unittesten betrekking heeft.

De betekenis van deze classificatie is vooral gelegen in het feit dat er een nauwe samenhang bestaat tussen het abstractieniveau waarmee normenstelsels geformuleerd zijn en het deel van het werkterrein (domein) dat deze stelsels bestrijken. Hoe groter het domein, hoe hoger het abstractieniveau, des te globaler (minder concreet) het oordeel en de advisering van de EDP-auditor zullen zijn.

Precisering
Precisering heeft betrekking op het in de vorige subparagraaf al aan de orde gestelde abstractieniveau waarop normenstelsels geformuleerd kunnen zijn. Bezien vanuit de invalshoek 'abstractieniveau' is een classificatie denkbaar met als uitersten:
- *globaal:* bijvoorbeeld er moet een procedure bestaan die waarborgt dat men elke voorgenomen programmawijziging vooraf beoordeelt;
- *gedetailleerd:* bijvoorbeeld er moet een procedure bestaan die waarborgt dat men elke voorgenomen programmawijziging vooraf beoordeelt op: de noodzaak of het nut, de consequenties voor de performance, de kosten, de accountantscontrole, etc.

Ook hier is het abstractieniveau bepalend voor de mate van concreetheid waarmee de EDP-auditor zijn oordeel kan vellen en zijn adviezen kan geven.

Gezaghebbendheid
Vanuit een oogpunt van 'gezaghebbendheid' is de volgende classificatie denkbaar:
- *mondiale instituten:* bijvoorbeeld ISO/IEC, CCITT, UN, IEEE;
- *Europese instituten:* bijvoorbeeld CEN/CENELEC, ETSI, ECMA, EWOS, EC;
- *nationale instituten:* bijvoorbeeld NNI/NEC, ANSI, FIPS, DoD, NCSC, NIST, NIVRA, NOREA.

'Gezaghebbendheid' is van invloed op het objectieve gehalte van een normenstelsel en is dus van betekenis voor de onderbouwing (deugdelijke grondslag) van het oordeel van de EDP-auditor.

Kwaliteitseigenschappen
Normenstelsels zijn ook naar kwaliteitseigenschappen te classificeren. Een classificatie naar kwaliteitseigenschappen is bijvoorbeeld gegeven in [NIVR89]. In dit geschrift zijn de volgende kwaliteitseigenschappen (het geschrift spreekt van 'criteria') genoemd en gedefinieerd:
- beschikbaarheid;
- exclusiviteit;
- integriteit;
- controleerbaarheid;

- doelmatigheid (efficiency);
- doeltreffendheid (effectiviteit);
- bescherming van waarden.

Deze classificatie heeft vooral betekenis voor de mate van concreetheid waarmee een EDP-auditor zijn oordeel kan vellen en zijn adviezen kan geven.

METANORMEN

De overheersende rol die normen in het auditproces vervullen, rechtvaardigt de vraag: 'Aan welke normen moeten normen(stelsels) op het vakgebied van de EDP-auditing voldoen?' We spreken dan over de zogenoemde metanormen. Over metanormen is in de literatuur nauwelijks iets te vinden. Dit is voor ons aanleiding geweest om mede op basis van [Sloe91] zelf een aanzet te geven tot de ontwikkeling van deze metanormen. De metanormen hebben betrekking op de objectiviteit, de eenduidigheid en de relevantie.

Objectiviteit

Onder objectiviteit verstaan we de mate waarin normen(stelsels) vrij zijn van persoonlijke beïnvloeding.

(Wettelijk) opgelegde normen lijken objectief van aard. Toch kan er ook bij deze (wettelijke) normen sprake zijn van subjectieve invloeden omdat de (wettelijke) bepalingen veelal ruimte laten voor verschillende interpretaties. Jurisprudentie heeft daarentegen een objectiverende invloed, zij het dat daarbij sprake is van een bijzondere situatie die vaak niet zonder meer veralgemeend kan worden.

In hoeverre 'algemeen aanvaarde normen' objectief zijn hangt af van het aanzien van andere wetenschaps-/vakgebieden en/of de gezaghebbendheid van de organisaties die zich achter deze normen scharen. Ook hier kan de objectiviteit (verder) onder druk komen te staan doordat er sprake kan zijn van uiteenlopende opvattingen.

Eenduidigheid

Onder eenduidigheid verstaan we de mate waarin normen(stelsels) concreet zijn.

Bepalend voor de eenduidigheid zijn:
- *de schaalbaarheid*, zijnde de mate waarin een norm kwantitatief is uit te drukken;
- *de nauwkeurigheid*, zijnde de mate van detail waarmee een norm is gedefinieerd en de eventuele speelruimte (tolerantie) die daarbij mag optreden;
- *de meetbaarheid*, zijnde de mate waarin en de eenvoud waarmee de 'werkelijkheid' kan worden opgemeten en herleid kan worden tot de eenheid waarin de norm is uitgedrukt. Anders is een zuivere vergelijking van norm en werkelijkheid niet mogelijk.

Relevantie

Onder relevantie verstaan we de mate waarin normen(stelsels) bruikbaar zijn voor bepaalde auditopdrachten.

Bepalend voor de relevantie zijn:
- *de toepasbaarheid*, zijnde de mate waarin een normenstelsel betrokken kan worden op een bepaalde auditopdracht;
- *de risicodekkingsgraad*, zijnde de mate waarin duidelijk is in hoeverre inbreuken op de kwaliteit van het auditobject zijn afgedekt als aan het normenstelsel voldaan wordt, of andersom geformuleerd: welke risico's zijn niet (volledig) afgedekt.

BRUIKBAARHEID BEKENDE STANDAARDEN

Gezien de praktijk om het bij een bepaalde EDP-auditopdracht te hanteren normenstelsel af te stemmen met de opdrachtgever, ligt het voor de hand om gebruik te maken van de normen die opgesloten liggen in bekende standaarden, omdat de kans dat de opdrachtgever daarmee een zekere affiniteit heeft het grootst is.

Zonder goede meetbaarheid is een zuivere vergelijking van norm en werkelijkheid niet mogelijk.

Daarbij komt de vraag op in hoeverre deze bekende standaarden bruikbaar zijn, ofwel meer aansluitend op de vorige paragraaf, in hoeverre deze standaarden aan de metanormen voldoen. Daarbij beperken wij ons tot die metanormen die betrekking hebben op de relevantie, namelijk de toepasbaarheid en de risicodekkingsgraad.

Toepasbaarheid

Het resultaat van een EDP-auditopdracht zal ten minste een oordeel moeten inhouden over de mate waarin een bepaald auditobject aan bepaalde kwaliteitseigenschappen voldoet. Toepasbaarheid heeft dus betrekking op twee dimensies, namelijk het auditobject en de kwaliteitseigenschappen daarvan.
Als de EDP-auditor bekende standaarden als uitgangspunt voor het samenstellen van een bij een bepaalde auditopdracht te hanteren normenstelsel wil gebruiken, dan zou idealiter duidelijk moeten zijn bij welke auditopdrachten welke normen uit welke standaarden (in combinatie met elkaar) het op een bepaalde opdracht toegesneden normenstelsel kunnen vormen. Vaak zijn de verbanden tussen standaarden en auditopdrachten onvoldoende duidelijk. Deze conclusie slaat zowel op de auditobjecten als op de te 'auditen' kwaliteitseigen-

schappen. Een uitzondering vormen auditopdrachten die nu net gericht zijn op het vaststellen of een organisatie aan een specifieke standaard, bijvoorbeeld ISO 9001 (Kwaliteitssystemen), voldoet.

Standaarden en auditobjecten
De verschillende standaarden bestrijken qua omvang sterk uiteenlopende en elkaar deels overlappende delen van het werkterrein van de EDP-auditor. Om inzichtelijk te maken welk gedeelte van het werkterrein de verschillende standaarden bestrijken is een vaste indeling (standaardindeling) van het werkterrein nodig. Bij de keuze van de standaardindeling spelen onder meer de volgende criteria een rol:

- de indeling behoort een bepaalde structuur te hebben die een verder gaande indeling mogelijk maakt zonder dat het overzicht daarbij verloren gaat;
- de indeling sluit overlappingen van bepaalde deelterreinen zoveel mogelijk uit;
- de indeling behoort aan te sluiten op de voor de EDP-auditing relevante onderdelen van andere vakgebieden;
- de indeling ondersteunt de afbakening van een EDP-auditopdracht.

In NOREA-verband houdt de Studiegroep 'Inhoud EDP-auditing' zich met de indeling van het werkterrein bezig.

In de EDP-auditwereld bestaat geen eenheid van opvatting over de te onderscheiden kwaliteitseigenschappen en de definiëring ervan.

Een complicerende factor is dat auditobjecten die men op een bepaald abstractieniveau hetzelfde kan benoemen, toch van elkaar kunnen verschillen. Deze verschillen zijn toe te schrijven aan verschillen in organisatorische infrastructuur, in technische infrastructuur, in systeemconcept en dergelijke. Anders gezegd: een zelfde auditobject kan zich, al naargelang de situatie, in verschillende gedaanten manifesteren.

Standaarden en kwaliteitseigenschappen
Voor zover er in standaarden kwaliteitseigenschappen genoemd en gedefinieerd worden, sluiten deze niet naadloos aan op de begrippen en de inhoud daarvan zoals de EDP-auditor die in zijn dagelijkse praktijk toepast. Daarbij valt nog op te merken dat er sprake is van een extra complicatie, omdat er in de EDP-auditwereld met betrekking tot de te onderscheiden kwaliteitseigenschappen en de definiëring daarvan geen eenheid van opvatting bestaat. Deze complicatie is onder meer ook aangeroerd in [Bruij93]. Vanuit een oogpunt van beroepsuitoefening is dit hoogst ongewenst omdat daardoor (potentiële) opdrachtgevers in verwarring kunnen raken. De EDP-auditor benoemt en definieert de kwaliteitseigenschappen meestal in relatie tot het auditobject 'informatie'. Een verklaring daarvoor is dat de EDP-auditdiscipline vanuit de accountancy is ontwikkeld, in welke discipline 'het getrouwe beeld' een centrale plaats inneemt.
Inmiddels groeit het besef dat voor een opdrachtgever een audit aan waarde wint als de auditor de kwaliteitseigenschappen in relatie tot het auditobject benoemt en definieert. Een voorbeeld van een mogelijke uitwerking daarvan is te vinden in [Moll91]. In dit voorbeeld is ook aandacht besteed aan de samenhang tussen de kwaliteitseigenschappen van de onderscheiden componenten en activiteiten (mogelijke auditobjecten) en de uiteindelijke invloed daarvan op de kwaliteit(seigenschappen) van de informatie. Een ander voorbeeld is te vinden in [SERC92]. Voor het auditobject 'applicatieprogrammatuur' heeft de stichting SERC (Software Engineering Research Centre) een fijnmazig stelsel van kwaliteitseigenschappen uitgewerkt, dat herkenbaar is voor de managers die bij de ontwikkeling van applicatiesoftware zijn betrokken. Daarbij zijn bij elke onderscheiden kwaliteitseigenschap veelal één of meer indicatoren genoemd met de wijze waarop men een 'meetwaarde' kan verkrijgen. In deze publikatie is tevens het verband aangegeven met de internationale standaard ISO/IEC 9126 (Information technology – Software product evaluation – Quality characteristics and guidelines for their use).

Los van de vraag of de hiervoor bedoelde uitwerkingen nu voor de EDP-auditor direct bruikbaar zijn, biedt de gevolgde systematiek aanknopingspunten voor het ontwikkelen van stelsels van kwaliteitseigenschappen die meer zijn toegesneden op de verschillende auditobjecten. Bij het benoemen en definiëren van de kwaliteitseigenschappen kan men voor zover mogelijk aansluiten bij bekende standaarden teneinde de communicatie met de opdrachtgever te vergemakkelijken.

Overigens is er met betrekking tot de kwaliteitseigenschappen nog minstens één complex probleem, namelijk de onderlinge weging van de te 'auditen' kwaliteitseigenschappen. Dit is vooral een probleem als er sprake is van één of meer elkaar tegengesteld beïnvloedende kwaliteitseigenschappen, zoals bijvoorbeeld performance en controleerbaarheid. De sleutel voor de oplossing van dit probleem ligt vermoedelijk in het samen met de opdrachtgever bepalen van het relatieve belang van de verschillende kwaliteitseigenschappen (afhankelijkheidsanalyse), in combinatie met het vaststellen van 'normmeetwaarden' die als limieten opgevat moeten worden.

Standaarden en normenstelsels
Het feit dat een zelfde auditobject zich in een grote verscheidenheid van gedaanten kan manifesteren (zie hiervoor onder de subparagraaf 'Standaarden en auditobjecten') heeft ook consequenties voor het ontwikkelen van normenstelsels op basis van bekende standaarden. Er zal voor de diverse auditopdrachten slechts een meer algemeen toepasbaar normenstelsel ontwikkeld kunnen worden, dat voor de EDP-auditor het vertrekpunt kan zijn voor

de ontwikkeling van een situatiespecifiek normenstelsel.

Risicodekkingsgraad

Meer dan eens is hiervoor aangegeven dat het resultaat van een EDP-audit ten minste een oordeel moet inhouden over de mate waarin een bepaald auditobject aan bepaalde kwaliteitseigenschappen, in casu een bepaald normenstelsel voldoet. Meestal is de wezenlijke betekenis van dat oordeel, in termen van risicobeheersing, onvoldoende duidelijk. Dit geldt ook als men als normenstelsel een bepaalde standaard, bijvoorbeeld ISO 9001 (Kwaliteitssystemen) hanteert. Deze onduidelijkheid is te verklaren uit het gebrek aan inzicht in de mate waarin normenstelsels de risico's op inbreuken op de kwaliteit afdekken. Zelfs een ISO 9000-certificaat blijkt in de praktijk niet garant te staan voor de beoogde kwaliteit van produkten ([Swin95]). Voor de opdrachtgever zou er een duidelijker situatie ontstaan als de EDP-auditor, gegeven een bij een bepaalde opdracht behorend normenstelsel, de niet-afgedekte risico's zou kunnen expliciteren. Men zou zelfs kunnen denken aan meerdere normenstelsels voor een zelfde auditobject die van elkaar verschillen in de mate van risicodekking.

Economisch perspectief
Aan het reduceren van risico's zit ook een economische kant. De met een auditobject samenhangende risico's reduceert men door het treffen van een daarop toegesneden stelsel van maatregelen en die brengen kosten met zich mee. Meestal zijn er verschillende mogelijkheden, in casu alternatieve stelsels van maatregelen die (vrijwel) dezelfde risicoreductie realiseren, maar die alternatieven variëren qua hoogte van de kosten. Ideaal zou zijn als de EDP-auditor ook in staat zou zijn om het meest efficiënte stelsel van maatregelen te bepalen. Vandaaruit zou de EDP-auditor, als de auditbevindingen daartoe aanleiding geven, theoretisch gefundeerd kunnen adviseren over het aanpassen van het in de audit betrokken stelsel van maatregelen. Tot nu toe blijkt echter de economische kant van het in een bepaalde situatie te treffen stelsel van maatregelen, op zijn zachtst gezegd, niet de meest ontwikkelde kant van het vakgebied te zijn.

HUIDIGE ACTIVITEITEN EN STAND VAN ZAKEN

Momenteel buigt een tweetal groepen zich over de problematiek van de normen(stelsels), namelijk in NIVRA-verband de werkgroep Standaarden en Normen en in NOREA-verband de Studiegroep Standaarden.

De NIVRA-werkgroep beoogt te komen tot een algemeen geaccepteerd referentiekader waar het gaat om de inpassing van de automatisering in de jaarrekeningcontrole.
De Studiegroep Standaarden van de NOREA onderzoekt de mogelijke bruikbaarheid van een aantal internationaal bekende standaarden voor het bepalen van bij gebruikelijke auditopdrachten te hanteren normenstelsels. De beide auteurs van dit artikel maken deel uit van deze studiegroep.

CONCLUSIE

Een voorzichtige, tussentijdse conclusie is, dat we nog ver verwijderd zijn van het theoretische ideaalbeeld dat, gegeven een bij een bepaalde auditopdracht behorend normenstelsel, de mate van risicoreductie en het daarbij passende economisch meest verantwoorde stelsel van maatregelen bekend zijn. Dit theoretische ideaalbeeld zou ook wel eens het schrikbeeld voor de praktische beroepsuitoefening door de EDP-auditor kunnen blijken te zijn. Het uitvoeren van een EDP-auditopdracht zou dan een meer mechanische bezigheid worden, waarbij er minder ruimte is voor het zogenoemde professional judgement. Niettemin is het goed zich te realiseren dat de mate waarin de EDP-auditor zich op het professional judgement beroept, tegelijkertijd ook de mate van theoretische onvolwassenheid van het vakgebied EDP-auditing aangeeft.

LITERATUUR

[Bruij93] A.J.M. de Bruijn, *EDP-auditing, wat is het?*, De EDP-Auditor, april 1993.

[COSO92] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control – Integrated Framework*, 1992.

[DNB88] De Nederlandsche Bank, *Memorandum omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking in het bankwezen*, Amsterdam 1988.

[Moll91] K.IJ. Mollema, *Zichtbaarheid van informatiekwaliteit*, Samsom BedrijfsInformatie, Alphen aan den Rijn/Deurne 1991.

[Moon91] H.B. Moonen, *Kwaliteitsnormen bij EDP-auditing: een kritische beschouwing*, KUB, Tilburg 1991.

[NIVR89] Nederlands Instituut van Registeraccountants (NIVRA), *Automatisering en controle Deel VII, Kwaliteitsoordelen over informatievoorziening*, NIVRA-geschrift nummer 53, Kluwer Bedrijfswetenschappen, Deventer 1989.

[SERC92] Stichting Software Engineering Research Centre (SERC), *Het specificeren van software-kwaliteit*, Kluwer Bedrijfswetenschappen, Deventer 1992.

[Sloe91] L.H.J.M. Sloesen, *Lesbrief Auditing*, Erasmus Universiteit Rotterdam, 1991.

[Swin95] G.J.P. Swinkels, J.G. Verrijdt en G.J. van der Pijl, *Kwaliteitszorg, kwaliteitssysteem en certificering*, Maandblad voor Bedrijfsadministratie, april 1995.

L. Annokkée RE
Is werkzaam als medewerker Vaktechniek bij de Accountantsdienst van het Ministerie van Volksgezondheid, Welzijn en Sport. In 1994 heeft hij de opleiding tot Register EDP-auditor bij het TIAS afgerond.

B. Sebregts RE
Is werkzaam als senior consultant bij PTT Telecom BV binnen het werkveld van IT Control. Hieraan voorafgaand heeft hij de functie van senior EDP-auditor vervuld. In dat verband heeft hij in 1994 de opleiding tot Register EDP-auditor bij het TIAS afgerond.

ISO 9000 EN EDP-AUDITING

Mr. W.R. Nanninga RE en
ltkol J.M.W. van de Garde RE

ISO 9000 en EDP-auditing richten zich beide op de verbetering van de beheersing van het bedrijfsproces. De combinatie van de sterke kanten van de ISO 9000-benadering, zoals de algemene geldigheid en de brede acceptatie, met de sterke kanten van EDP-auditing, zoals de nadruk op de operationele uitvoerbaarheid, levert een model op dat het beste van beide werelden verenigt. Voor de EDP-auditor heeft het model als voordeel dat een bredere visie op het bedrijfsproces wordt geboden.

INLEIDING

Reeds kort na de tweede wereldoorlog werd met name in Japan het belang onderkend van kwaliteit en kwaliteitsverbetering. Pas in het laatste decennium is ook bij ons het kwaliteitsdenken definitief doorgebroken. Met name de introductie van de ISO 9000-normserie lijkt hierbij de rol van katalysator te hebben gespeeld. Omdat de in ISO beschreven normen en richtlijnen voor kwaliteitssystemen een zeer breed toepassingsgebied hebben en in principe dus ook op sterk geautomatiseerde bedrijfsprocessen van toepassing kunnen zijn, is het slechts een kwestie van tijd voordat ook de EDP-auditor met dit relatief nieuwe fenomeen in aanraking zal komen.

In dit artikel zijn de overeenkomsten en verschillen onderzocht tussen de door de EDP-auditor gehanteerde criteria en de normen zoals die beschreven zijn in de ISO 9000-serie. Omdat de kwaliteitszorg voor een belangrijk deel gericht is op de interne beheersing van processen, is ook nadrukkelijk gelet op het door de EDP-auditor gehanteerde instrument van de administratieve organisatie. Om de mogelijke verwevenheid van EDP-auditing met kwaliteitszorg nader te accentueren, is getracht om met behulp van elementen uit beide werelden een concreet en evenwichtig beheerssysteem te bouwen. Het resultaat hiervan zal in de vorm van een model gepresenteerd worden.

Het te beschrijven model is opgebouwd uit drie lagen, waarbij het buitenste kader wordt gevormd door de bedrijfsprocessen (1e laag) systeemontwikkeling, systeemonderhoud en detachering. In een verdere analyse zijn daarbinnen de beheerselementen (2e laag) en vervolgens de beheersaspecten (3e laag) nader onderscheiden en uitgewerkt. Van de laatste stap, het onderkennen van de verschillende beheersmaatregelen (4e laag), is – gezien de te verwachten omvang – vooralsnog afgezien.

Met het uiteindelijke model en de beschrijving van de totstandkoming daarvan wordt beoogd een brug te slaan tussen EDP-auditing en de wereld van de kwaliteitszorg. Door gelijksoortige begrippen in één model te integreren ontstaat een – uniform – platform voor communicatie en in het verlengde daarvan een beter inzicht in de wederzijdse activiteiten en doelstelling. Aldus wordt de mogelijkheid geopend om van elkaars inzichten en verworvenheden te profiteren en op termijn misschien tot een vorm van samenwerking te komen.

KWALITEIT EN EDP-AUDITING

De invloed van het kwaliteitsdenken en het daarbij veel genoemde ISO 9000 neemt nog steeds toe. Als gevolg hiervan besluit een toenemend aantal bedrijven tot het invoeren van een kwaliteitssysteem. Het is slechts een kwestie van tijd voordat ook de EDP-auditor met dit relatief nieuwe fenomeen geconfronteerd zal worden.

In dit artikel zal aan de hand van enkele veel voorkomende IT-processen bezien worden wat het gevolg van de wisselwerking tussen ISO-kwaliteitszorg en EDP-auditing zou kunnen zijn. Getracht zal worden om een aantal concrete EDP-auditing- en ISO-kwaliteitsbegrippen met elkaar te verbinden. Dit met de bedoeling om in eerste instantie tot een betere communicatie en op termijn tot een – ongetwijfeld positieve – samenwerking tussen beide vakgebieden te komen.

Allereerst zal kort worden ingegaan op wat nu precies onder kwaliteit wordt verstaan en hoe zich dit verhoudt met ISO 9000. Vervolgens zal aan de hand van een belangrijk instrument voor de EDP-auditor, de principes van de Administratieve Organisatie (kortweg AO), gekomen worden tot een integratie van beide ([Nieu95], [Kame95]).
In het tweede deel van dit artikel zal in de vorm van een globaal model het resultaat van deze integratie geschetst worden. Daarbij is ernaar gestreefd om op een zo duidelijk mogelijke wijze zowel de belangrijkste ISO-normen als EDP-auditingcriteria een plaats te geven.

Kwaliteit

Het kwaliteitsdenken dat ook aan ISO 9000 ten grondslag ligt, is in essentie gebaseerd op twee uitgangspunten[1] ([Swin95]).

– Centraal staat de vertrouwensrelatie tussen de klant en leverancier. Deze relatie kan alleen goed functioneren als er sprake is van een effectieve *communicatie* tussen beide partijen. De aard en wijze van deze communicatie zal deels bepaald worden door het te leveren produkt. Bij een massaprodukt bijvoorbeeld zal de relatie tussen klant en leverancier veel beperkter zijn dan bij de totstandkoming van een maatwerkprodukt. Echter, in beide gevallen zal de leverancier zich ten doel moeten stellen zoveel mogelijk tegemoet te komen aan de verwachtingen van de klant inzake het te leveren produkt.

– Behalve dat de leverancier de wensen van de klant onderkent, zal hij er ook voor moeten zorgen dat deze ook daadwerkelijk worden gerealiseerd. Dit leidt ertoe dat binnen de organisatie van de leverancier een voor dit doel ingericht *stuur- en beheersmechanisme* aanwezig moet zijn. Als dit mechanisme specifiek gericht is op het bevorderen van de kwaliteit, is er sprake van een kwaliteitssysteem.

Het streven naar kwaliteit zal erin moeten resulteren dat de leverancier niet alleen bekend is met de wensen en verwachtingen van zijn klant, maar ook dat het produktieproces zodanig kan worden gestuurd en beheerst dat ook daadwerkelijk aan de klantwensen zal kunnen worden voldaan. Aldus dient er een optimale interactie tussen de externe communicatie en de interne beheersing te ontstaan.

ISO-norm

Op nationaal en internationaal niveau bestaat er een hecht samenwerkingsverband van standaardisatie-instituten. Het bestaan hiervan wordt niet alleen actief ondersteund door bedrijven die daarmee hun concurrentiepositie trachten te beschermen of verbeteren, maar bijvoorbeeld ook door een internationale organisatie als de EU die hiermee één van haar oprichtingsdoelstellingen wil bevorderen, de – verdere – harmonisatie van de Europese markt.

Er dient een optimale interactie tussen de externe communicatie en de interne beheersing te ontstaan.

Binnen de standaardisatie-instellingen vindt overleg plaats tussen de meest betrokken partijen (concurrerende producenten, afnemers, etc.), in het verlengde waarvan besloten kan worden tot de vaststelling van een nieuwe norm. Daarbij moet ervoor worden gezorgd dat de besluitvorming eerlijk en evenredig verloopt. Als aan alle vormvereisten is voldaan, is er sprake van een normalisatieproces met als uitkomst een formele norm. In andere gevallen waarbij bijvoorbeeld een aantal – concurrerende – fabrikanten onderling een afspraak maken, wordt gesproken van een standaardisatieproces met als uiteindelijk resultaat een (industrie)standaard. Het is niet ongebruikelijk dat gezaghebbende en veel gebruikte standaarden – na een proces van normalisatie – tot norm verheven worden.

In Nederland vindt de formele aansturing van het normalisatieproces plaats door het Nederlands Normalisatie-instituut (NNI). Ook internationaal vindt er normalisatie plaats. Op Europees niveau wordt dit verzorgd door de Europese Commissie voor Normalisatie (CEN) welke de EN-normen opstelt. Op mondiaal niveau is dit de International Organization for Standardization (ISO), waar de ISO-normen tot stand komen.

De opstellers van de ISO 9000-normen hebben ernaar gestreefd deze een zo breed mogelijke werking te geven. Dit heeft erin geresulteerd dat de in de normbladen opgenomen definities ([ISO89a]) en beschrijvingen ([ISO88], [ISO89c]) slechts in zeer algemene bewoordingen zijn geformuleerd. Na verloop van tijd is in aanvulling hierop een aantal meer specifieke uitwerkingen opgesteld, de zogenaamde Guidelines of Richtlijnen ([ISO91], [ISO92]).

1. Behalve ISO zijn er – uiteraard – ook andere uitgangspunten en methodieken die bij de inrichting en ontwikkeling van een systeem voor kwaliteitszorg gehanteerd kunnen worden, zoals het Capability Maturity Model (CMM).

Voor zover in dit artikel gesproken wordt van ISO 9000 zal met name de ISO 9001-norm bedoeld worden. Deze heeft van de bestaande ISO-normen de breedste werking omdat hierin alle stadia van het bedrijfsproces worden bestreken.

Administratieve organisatie

Aan de ontwikkeling van de administratieve organisatie heeft met name het vakgebied van de accountancy sterk bijgedragen. Het is dan ook niet verwonderlijk dat de administratieve organisatie oorspronkelijk vooral werd gezien als instrument ter beoordeling en verbetering van de betrouwbaarheid van financiële processen alsmede de verantwoording die daarover moet worden afgelegd. Deze op interne controle gerichte administratieve organisatie (AO/IC) bevat alle bekende elementen als functiescheidingen, aansluiten van de geld-goederenbeweging, inventarisaties, voor- en nacalculatie, etc.

Naast een aantal belangrijke overeenkomsten zijn er ook significante verschillen tussen ISO-kwaliteitszorg en het aandachtsgebied van EDP-auditing.

Het inzicht dat met behulp van AO/IC kan worden verkregen, is ook bruikbaar voor het beheersen van andere dan alleen financiële stromen en processen. Een meer moderne zienswijze op administratieve organisatie heeft ertoe geleid dat in principe *alle* informatiestromen in beschouwing worden genomen. Om deze bredere visie op administratieve organisatie tot uitdrukking te brengen wordt ook wel gesproken van bestuurlijke informatievoorziening, kortweg BIV. Voor wat betreft het begrip administratieve organisatie zal in dit model – tenzij dit uitdrukkelijk anders wordt gesteld – steeds administratieve organisatie in brede zin (AO/BIV) bedoeld worden.
Naast de accountant maakt ook de EDP-auditor gebruik van de administratieve organisatie als instrument om een oordeel te vormen over de wijze waarop bedrijfsprocessen aangestuurd en beheerst worden. Aangezien het werkterrein van de EDP-auditor niet beperkt is tot financiële – verantwoordings – processen, maar zich uitstrekt over het gehele gebied van de geautomatiseerde informatievoorziening, kan dan ook gesproken worden van administratieve organisatie in brede zin.

Integratie

Het kwaliteitssysteem zoals dit door ISO wordt beschreven, lijkt – zeker als er sprake is van een sterk geautomatiseerd bedrijfsproces – voor een belangrijk deel te overlappen met het aandachtsgebied van de EDP-auditor. In beide gevallen wordt immers de nadruk gelegd op de beheersing van het bedrijfsproces. Een nadere beschouwing leert echter dat er naast een aantal belangrijke overeenkomsten ook een aantal significante verschillen bestaan. Onderstaand een viertal constateringen.

– Allereerst dient erop te worden gewezen dat er binnen het vakgebied van de EDP-auditing veelvuldig over kwaliteit gesproken wordt. Het betreft daarbij echter uitsluitend de 'kwaliteit van de geautomatiseerde gegevensverwerking' ([NIVR89]), waarmee vanuit een zestal expliciet omschreven invalshoeken naar het intern functioneren van geautomatiseerde systemen en de bijbehorende systeemomgevingen gekeken wordt. Deze zes 'kwaliteitsaspecten' zijn: beschikbaarheid, exclusiviteit, integriteit, controleerbaarheid, effectiviteit en efficiency.
Het kwaliteitsbegrip in ISO is veel minder gespecificeerd en is behalve op interne ook op externe aspecten gericht. Zo wordt er sterke nadruk gelegd op de communicatie met de klant, waarbij pas in tweede instantie wordt gekeken naar de gevolgen voor de interne beheersing van het voortbrengingsproces.
Daar waar EDP-auditing vooral de eigenschappen van een geautomatiseerd systeem beziet, richt ISO zich veel meer op de wijze waarop het geautomatiseerde systeem bijdraagt aan de beheersing van – en de communicatie rond – het gehele proces.
Tussen beide kwaliteitsbegrippen bestaan, naar aard en omvang, dan ook aanzienlijke verschillen. Mede gezien de veel ruimere werkingssfeer van het ISO-kwaliteitsbegrip, zal dit als uitgangspunt gehanteerd worden.

– Een tweede belangrijke constatering is dat alleen in een geautomatiseerde omgeving sprake kan zijn van een samenloop tussen ISO-kwaliteitszorg en EDP-auditing. Daar waar ISO in principe van toepassing is op alle mogelijke bedrijfsprocessen, richt EDP-auditing zich uitsluitend op 'een omgeving waarin sprake is van informatietechnologie' ([Brui93]). Door de auteurs is er dan ook voor gekozen om uitsluitend aandacht te besteden aan bedrijfsprocessen die primair gericht zijn op het ontwikkelen en onderhouden van geautomatiseerde systemen. Ook detachering, dat gezien wordt als bijzondere vorm van IT-dienstverlening, zal hieronder worden begrepen.

– Het kwaliteitshandboek waarin de structuur van het kwaliteitssysteem is vastgelegd, vormt een belangrijk en tastbaar resultaat van elk kwaliteitsproject. Behalve dat het handboek aan de minimale eisen van duidelijkheid moet voldoen, is de verdere opzet en indeling vormvrij. Door het vooralsnog ontbreken van een specifieke modelleringsmethode voor kwaliteitssystemen wordt veelvuldig gebruik gemaakt van op administratieve organisatie gelijkende schematechnieken en tekenconventies. Een voorbeeld hiervan is het pakket SDW-9000. Met name bij organisaties waar reeds in het verleden een uitvoerige inventarisatie en vastlegging van de AO-maatregelen en -procedures heeft plaatsgevonden, bestaat het gevaar van redundantie. Binnen de Rijksoverheid is onder invloed van de Operatie Comptabel Bestel gekozen voor het gebruik van SDW-AO, dat grote gelijkenis vertoont

met het bovengenoemde pakket. Zowel bij het opstellen als bij het onderhouden van het kwaliteitshandboek zal dus steeds op een goede afstemming met het AO-beheer en AO-handboek gelet moeten worden.

– Ook op een aantal andere gebieden is er tussen ISO-kwaliteitszorg en EDP-auditing eerder sprake van onderlinge aanvulling dan van een tegenstelling. Deze wisselwerking leidt ertoe dat de nogal sterk intern gerichte AO-maatregelen in het bredere verband van de externe communicatie geplaatst kunnen worden. Aan de andere kant zullen de veel gedetailleerder en verder ontwikkelde methoden en technieken van de administratieve organisatie een zeer welkome aanvulling – en concrete invulling – kunnen betekenen voor de nogal globale maar wel eenduidige en breed geaccepteerde ISO-normen.

Het bovenstaande heeft geleid tot het idee dat er – binnen bepaalde randvoorwaarden – sprake kan zijn van een zinvolle integratie tussen ISO 9000 en administratieve organisatie als instrument van de EDP-auditor. Dit heeft geresulteerd in het opstellen van een lijst van gecombineerde normen en maatregelen, welke enerzijds voor de beheerder of ontwikkelaar van een ISO-kwaliteitssysteem kan dienen als een volledig overzicht van alle mogelijke beheersmaatregelen en anderzijds aan de adviserende of controlerende EDP-auditor een opsomming presenteert van een groot aantal – meer of minder – noodzakelijke AO-maatregelen.

AANZET TOT EEN MODEL

De lijst van gecombineerde normen en maatregelen is samengebracht in één model, dat gezien zou kunnen worden als een bijdrage aan een betere communicatie en samenwerking tussen de EDP-auditor en de kwaliteitsbeheerder.

Randvoorwaarden en uitgangspunten van het model

Bij het opstellen van het model is uitgegaan van een drietal veel voorkomende IT-processen. Voor zowel het bedrijfsproces ontwikkeling als onderhoud als detachering is vervolgens met behulp van ISO 9001 een eerste indeling gemaakt van de te stellen normen en eisen. Deze ISO-norm bevat een twintigtal artikelen ter verbetering van de beheersing van processen. Omdat in ISO 9001 nauwelijks aandacht wordt besteed aan het element financieel beheer is dit onderdeel toegevoegd.
Voor wat betreft systeemontwikkeling en -onderhoud is tevens gebruik gemaakt van de Guidelines in ISO 9000-3. Bij detachering is aanvullend gekeken naar de Richtlijnen voor diensten ([ISO92]).

Ter bevordering van de overzichtelijkheid en de algemene geldigheid is de diepgang van het model bewust beperkt gehouden. Zo worden er geen normen en maatregelen gesteld aan de individuele projecten. Hiervoor bestaan voldoende, goed gedocumenteerde, methoden en technieken van projectbeheersing. Het model gaat dan ook niet verder dan te verlangen dat zo snel mogelijk – liefst in de offertefase – een methode van projectbeheersing wordt gekozen welke vervolgens in het projectplan verder uitgewerkt wordt. Ook op activiteiten die sterk situationeel afhankelijk zijn, zal in het model niet – inhoudelijk – worden ingegaan.
Wellicht ten overvloede wordt nog opgemerkt dat het de gebruiker van het model natuurlijk vrij staat om, afhankelijk van de individuele situatie, bepaalde punten verder uit te werken of misschien juist te beperken.

De ISO 9000-normen bevatten slechts een opsomming van een aantal van de belangrijkste kwaliteitsbegippen.

De ISO 9000-normen bevatten slechts een opsomming van een aantal van de belangrijkste kwaliteitsbegrippen. Een ISO-kwaliteitssysteem kan (en moet zelfs) door de gebruiker ervan verder worden aangevuld en verbeterd. Bij het opstellen van het model is in aanvulling van de expliciet in ISO 9000 genoemde elementen bijvoorbeeld ook gebruik gemaakt van een aantal onderdelen van de Kaizen-filosofie ([Masa90]).

Mondige klanten
Reeds eerder is gewezen op het belang van de externe communicatie. Het contact met de klanten zal door het gehele proces heen gewaarborgd moeten zijn. Daartoe zal allereerst een organisatorische structuur met vaste aanspreekpunten en vaste overlegmomenten ingericht moeten worden. Het overleg met de klant zal vervolgens tot daadwerkelijke interne verbeteringsactiviteiten moeten leiden. In ieder geval zal elk project door middel van een eindevaluatie met de klant moeten worden afgesloten.
Buiten de reguliere communicatie zal ook ruimte moeten zijn voor incidentele informatie-uitwisseling, bijvoorbeeld een klachtenprocedure. Gezien het feit dat de reguliere communicatie blijkbaar niet voldoende heeft gewerkt en het kwaliteitssysteem mogelijk heeft gefaald, zal de klachtenprocedure met extra waarborgen omgeven moeten worden.

Tevreden medewerkers
Het is belangrijk dat ook de medewerkers regelmatig in de gelegenheid worden gesteld hun ideeën en opmerkingen over het functioneren van de organisatie alsmede hun eigen functioneren te bespreken. Met name als personeelsleden buiten de organisatie te werk zijn gesteld, zal dit proces nadrukkelijk bewaakt moeten worden. Daarnaast zal ook de opleiding en ontwikkeling van de deskundigheid van de desbetreffende medewerkers aan de orde gesteld moeten worden.

Meten is weten
De registratie van gegevens speelt in de kwaliteitszorg een belangrijke rol. Zo zal aan het begin van

een kwaliteitsverbeteringstraject eerst een selectie van de meest significante kengetallen van het te verbeteren proces worden gemaakt. Uitgaande van de actuele waarde wordt vervolgens de na te streven norm opgesteld. Tijdens het kwaliteitsverbeteringstraject zal de – positieve – ontwikkeling van deze kengetallen een belangrijke succesindicator zijn.

Door het vastleggen van beheersgegevens en het evalueren van afwijkingen zal zich een instrument voor planning en sturing ontwikkelen.

Een lerende organisatie
Binnen de organisatie vinden er op verschillende momenten en op verschillende niveaus plannings-, bewakings-, terugkoppelings- en evaluatiehandelingen plaats. Deze dienen op een eenduidige manier met elkaar te worden verbonden, zodat effectieve plannings- en controlecycli ontstaan. Door het steeds opnieuw vastleggen van de meest essentiële beheersgegevens en het evalueren van geconstateerde afwijkingen zal zich op termijn een steeds betrouwbaarder instrument voor planning en sturing ontwikkelen.

De optimale benutting van de urencapaciteit
Bij elk van de genoemde bedrijfsprocessen is sprake van kennisintensieve processen. Door op het juiste moment over de vereiste deskundigheid te beschikken zal de kwaliteit van het te leveren eindprodukt positief worden beïnvloed. Bij dienstverlenende organisaties zullen daarnaast de personeelskosten een belangrijk beslag leggen op de financiën van de organisatie. Het efficiënt aanwenden en effectief benutten van deze urencapaciteit zal dan ook in sterke mate bijdragen aan het succes van de organisatie.

De financiële verantwoording
Uitgangspunt van het financieel beheer is een betrouwbaar en controleerbaar stelsel van vastleggingen en verantwoordingen. Behalve in de noodzakelijke functiescheidingen en controle- en beveiligingsmaatregelen zal dit resulteren in een groot aantal specifieke maatregelen. Daarnaast zal erop moeten worden toegezien dat de verschillende maatregelen ook daadwerkelijk worden nageleefd.

STRUCTUUR VAN HET MODEL

Het model dat hier gepresenteerd wordt, bestaat uit drie lagen.
Allereerst worden drie veel voorkomende IT-processen onderscheiden welke het buitenste kader van het model vormen. Deze bedrijfsprocessen zijn: de ontwikkeling van maatwerkprogrammatuur, het onderhoud van applicatiesoftware en de detachering van IT-deskundigen. Voor andere primaire processen binnen het veld van informatietechnologie heeft het model in eerste instantie geen geldigheid. Door echter gebruik te maken van dezelfde methodiek en door een selectie van de voorbeelden in het model moet het niet al te moeilijk zijn om het model – naar behoefte – met andere bedrijfsprocessen uit te breiden.
De tweede laag wordt gevormd door binnen elk van de bedrijfsprocessen de belangrijkste beheerselementen te onderscheiden. Hierbij spelen de twintig artikelen uit de ISO 9001-norm een doorslaggevende rol. Voor wat betreft de indeling van de beheerselementen wordt aansluiting gezocht bij de elementaire onderdelen van transformatieprocessen.
In de derde laag ten slotte worden de beheerselementen verder ingevuld met behulp van concrete beheersaspecten. Hierin wordt behalve naar de bepalingen van de ISO 9001-norm ook gekeken naar de ISO-richtlijnen, de eisen en maatregelen die voortvloeien uit de administratieve organisatie, alsook de 'kwaliteits'-criteria van EDP-auditing.

EERSTE LAAG, BEDRIJFSPROCESSEN

Uitgangspunt van dit model is steeds geweest om een beschrijving te geven van het beheersmechanismen binnen het systeemontwikkelings-, het systeemonderhouds- en het detacheringsproces. Een nadere beschouwing van deze processen laat zien dat er naast een groot aantal verschillen ook enkele overlappingen zijn. Het betreft dan met name de op ondersteuning gerichte activiteiten zoals het structureren van het proces, het verzorgen van de benodigde produktiemiddelen, de communicatie met de klant en de markt en het toezicht op de uitvoering. Ter voorkoming van redundanties bij de behandeling van de verschillende processen zijn deze elementen in een aparte groep, onder de noemer 'Algemeen', bijeengebracht.

Dit resulteert erin dat op het hoogste niveau in het model onderscheid wordt gemaakt in de volgende bedrijfsprocessen:
- Algemeen;
- Ontwikkeling;
- Onderhoud;
- Detachering.

Deze indeling in bedrijfsprocessen vormt de basis voor de verdere behandeling van het model.

TWEEDE LAAG, BEHEERSELEMENTEN

De tweede laag van het model bestaat uit beheerselementen, die kunnen worden onderverdeeld in elementaire proceselementen, elementen van het ondersteunende proces, elementen van het primaire proces en beheerselementen.

Elementaire proceselementen

De voor het model gekozen bedrijfsprocessen zijn transformatieprocessen. Om van een volwaardig transformatieproces – en dus ook een bedrijfsproces – te kunnen spreken moet minimaal een vijftal

elementaire proceselementen aanwezig zijn ([Veld88]). Deze elementaire proceselementen zijn:

– *Structuur*
Het proces op zich moet bestaan en daarmee een bepaalde structuur en systematiek van functioneren hebben. De transformatie die binnen het proces plaatsvindt zal op een geordende manier moeten verlopen.

– *Invoer*
Om een transformatieproces te kunnen laten functioneren is het noodzakelijk dat er input is. Dit vormt de grondstof voor de omzetting die na de invoer binnen het proces plaatsvindt.

– *Signaal*
Behalve de invoer zal er ook een signaal moeten zijn waarmee het proces gestart kan worden. In zijn meest elementaire vorm fungeert de invoer gelijk als trigger, waarna het proces doorloopt tot er geen input (brandstof) meer is. Bij een complexer proces staan de signalen los van de invoer en kunnen de signalen ook het functioneren beïnvloeden door het proces bijvoorbeeld te versnellen, te vertragen of te stoppen. Het signaal wordt een stuursignaal voor het omzettingsproces.

– *Activiteit*
Binnen het proces zal een reeks van activiteiten moeten plaatsvinden die te zamen de transformatie bewerkstelligen. Het proces zal dus moeten 'werken'. Dit is de kern van het proces waarvan de andere procesonderdelen afhankelijk zijn.

– *Uitvoer*
Ten slotte leidt elk omzettingsproces tot uitvoer, het eindprodukt van het proces. De mate waarin de uitkomst van het proces voorspeld kan worden, is met name afhankelijk van de structuur en de aanwezige sturingsmogelijkheden.

Elk van de genoemde elementaire proceselementen zal dus in de verschillende bedrijfsprocessen een plaats moeten krijgen. Hierbij dient echter aangetekend te worden dat in een eerder stadium een aantal 'overlappende' proceselementen uit de primaire processen is gehaald en in het bedrijfsproces Algemeen is ondergebracht. Om te spreken van een volwaardig proces dient elk van de elementaire proceselementen of in het primaire proces of in het ondersteunende proces voor te komen. Allereerst zal het ondersteunend proces – Algemeen – bekeken worden.

Elementen van het ondersteunende proces

Binnen het ondersteunende proces vinden zowel de structurerende elementen als de input van de voor het proces noodzakelijke middelen een plaats.

De structurerende elementen kunnen worden onderverdeeld in meer eenmalige en langdurige zaken zoals de opzet van de organisatie en het te voeren (meerjaren)beleid en meer dynamische en kortlopende zaken zoals procedures en werkafspraken. Het is belangrijk dat deze structuur ook behouden blijft. Er zal moeten worden gecontroleerd dat alle deelnemers zich wel aan de gemaakte – korte- en lange-termijn- – afspraken houden.

Kunnen in de vrije natuur processen voorkomen die – schijnbaar – geen doel hebben, aan een bedrijfsproces worden stringentere eisen gesteld. Een bedrijfsproces ontleent zijn bestaan in principe slechts aan een bepaalde vraag uit de markt. De output van het proces zal dus steeds zodanig moeten zijn dat aan deze vraag wordt beantwoord. Zeker als er meer gelijksoortige aanbieders zijn – in geval van concurrentie – zal het eigen voortbrengingsproces zodanig moeten worden ingericht en gestuurd dat het eindprodukt – beter dan dat van de concurrent – aansluit bij de behoefte van de klant. Het belang van een goede communicatie met de klant en daarmee van een belangrijk onderdeel van het kwaliteitsdenken wordt nogmaals benadrukt.
Omdat produkten verouderen en markten veranderen is het belangrijk om niet alleen op de bestaande maar ook op de toekomstige vraag in te spelen. Naast marketing zal ook aan innovatie gedaan moeten worden.

Naast de structurerende en de marketingelementen bevinden zich ook de voor het transformatieproces noodzakelijke middelen in het ondersteunende proces. Dit zijn de bekende produktiemiddelen Financiën, Personeel en (overige) Middelen. De managementvaardigheden van de bedrijfsleiding die ook vaak als produktiemiddel worden genoemd, zijn hier niet verbijzonderd. De kundigheid van het management zal moeten blijken uit de wijze waarop het bedrijfsproces is gestructureerd en wordt bestuurd, en de wijze waarop het middelenbeheer wordt gevoerd. In feite is dit produktiemiddel over alle proceselementen gedistribueerd.

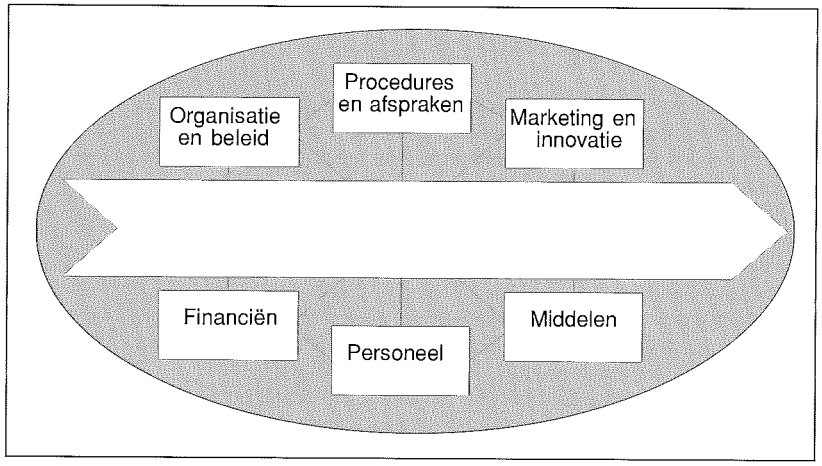
Voor wat betreft het gebruik van middelen is het essentieel dat er hiervan steeds voldoende aanwezig zijn om het primaire proces ongestoord te laten verlopen. Omdat hoge voorraden en een omvangrijke personele bezetting aanzienlijke kosten met zich meebrengen, zal er dus een balans moeten worden gezocht tussen voorraad en gebruik. De input van middelen zal beheerst moeten worden.

Kort samengevat kunnen in het ondersteunende proces (Algemeen) de volgende proceselementen worden onderscheiden:
- Organisatie en beleid;
- Procedures en afspraken;
- Marketing en innovatie;
- Financiën;
- Personeel;
- Middelen.

In figuur 1 is een schematisch overzicht gegeven van het algemene ondersteunende proces en de daarin voorkomende proceselementen.

Elementen van het primaire proces

Ter voorkoming van hinderlijke redundanties zullen de drie verschillende primaire processen op dit niveau van het model nog zoveel mogelijk gezamenlijk worden behandeld. Er zal -vooralsnog –



Figuur 1. Ondersteunend proces: algemeen.

dan ook gesproken worden van 'het primaire proces'. Uitgaande van de elementaire proceselementen resteren er voor het primaire proces nog de elementen: signaal, activiteit en uitvoer.

Het externe signaal of de trigger start het transformatieproces. Daarnaast is er ook tijdens het transformatieproces nog invloed van externe of interne signalen mogelijk. Om de mogelijkheid van een conflict tussen externe signalen en de interne besturing bij de uitvoering van het proces te vermijden, bestaat er een mechanisme waarbij steeds één van beide signalen prioriteit heeft. Op bepaalde momenten tijdens het transformatieproces stopt de interne besturing en wacht deze op een extern signaal.
In een regulier bedrijfsproces zal de meerderheid van de signalen afkomstig zijn van interne besturing. Om ook ruimte te geven aan externe signalen zal in de structuur van het proces vastgelegd moeten worden op welke momenten en onder welke voorwaarden externe signalen de besturing – tijdelijk – overnemen.

Het mag duidelijk zijn dat elk bedrijfsproces begint met een opdracht van de klant, de trigger. Daarbij zal allereerst gekeken moeten worden of de opdracht van de klant binnen het bedrijfsproces kan worden uitgevoerd. Er zullen tussen de opdrachtgever en de – procesverantwoordelijke – leverancier verkennende besprekingen moeten plaatsvinden.

Als uitvoering in principe mogelijk is, zal vervolgens voorkomen moeten worden dat gedurende de uitvoering van het proces een groot aantal wijzigingen en bijsturingen plaatsvinden die de voortgang mogelijk kunnen verstoren. De opdracht, de wijze van uitvoering en het eindresultaat zullen vooraf duidelijk moeten zijn. Beide partijen bevestigen deze door middel van een afspraak.

De daadwerkelijke transformatie komt tot stand door de uitvoering van activiteiten welke daarmee de kern van het proces is. Voorafgaand aan de uitvoering van een bedrijfsproces zal er dus duidelijkheid moeten zijn over de structuur van werken, de aansturing en de beschikbaarheid van produktiemiddelen. Van de gekozen bedrijfsprocessen wordt zowel bij Ontwikkeling als bij Onderhoud een planmatige werkwijze gevolgd. Bij Detachering is dit minder het geval omdat de uitvoeringsactiviteit in sterke mate wordt bepaald door een – moeilijk voorspelbare – externe vraag. In de verdere uitwerking van de bedrijfsprocessen zal op deze verschillen nog nader worden ingegaan; vooralsnog kan echter gesteld worden dat de procesactiviteiten steeds een duidelijke voorbereiding vereisen.

Het eindprodukt is de uitvoer van het transformatieproces en daarmee de resultante van het – goede – functioneren van alle andere proceselementen. Het eindprodukt is voor het bedrijfsproces van essentieel belang omdat daarmee een plaats in de markt en zodoende het bestaan van het proces zelf kan worden gelegitimeerd. Een produkt zal dus niet alleen in een bepaalde vraag moeten voorzien maar, wil er sprake zijn van kwaliteit, ook zo dicht mogelijk moeten aansluiten op de verwachting van de klant. Daarom wordt nogmaals gewezen op het belang van goede afspraken vooraf en een goede communicatie tijdens de uitvoering.

Mocht er desondanks met het eindprodukt na oplevering toch iets mis gaan, dan zal de leverancier dit door middel van zijn nazorg moeten oplossen. Een goede nazorg draagt bij aan de positieve communicatie met de klant en kan op termijn weer tot nieuwe opdrachten leiden.

Periodiek zal gekeken moeten worden of de tot stand gebrachte eindprodukten niet alleen in voldoende mate aan de eisen van de klant, maar ook aan de verwachtingen van de procesverantwoordelijke zelf hebben voldaan. Omdat het eindprodukt een resultante is van alle procesonderdelen zal een dergelijke evaluatie zich ook over het gehele bedrijfsproces moeten uitstrekken. Niet alleen voor het voortbestaan van het proces maar ook voor de kwaliteit van het eindprodukt is een dergelijke evaluatie van essentieel belang.

Kort samengevat worden in het primaire proces (Ontwikkeling, Onderhoud en Detachering) de volgende proceselementen onderscheiden:
- Verkenning;
- Afspraak;
- Voorbereiding en uitvoering;
- Nazorg en evaluatie.

Ter verduidelijking van het primaire proces en de daarin voorkomende proceselementen is dit in figuur 2 schematisch weergegeven.

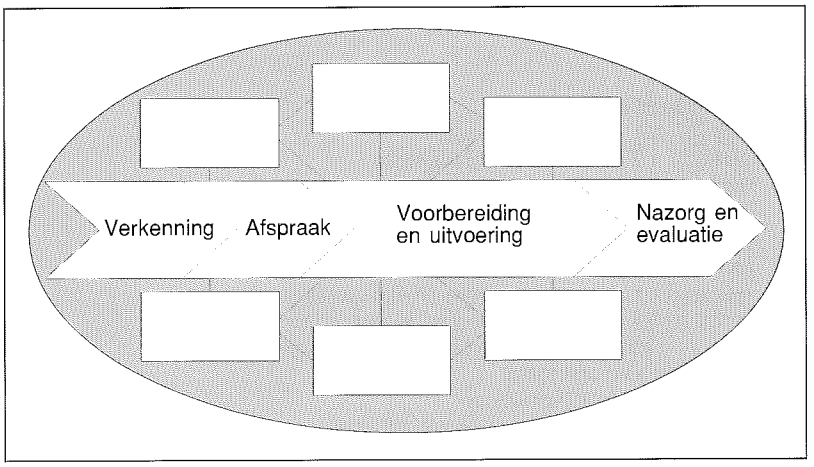
Beheerselementen

Een nadere beschouwing van zowel het ondersteunende als het primaire proces heeft laten zien dat deze zijn opgebouwd uit verschillende procesonderdelen. Met dit inzicht is het niet alleen mogelijk om processen te begrijpen, maar ook om deze beter te laten functioneren. Als de verschillende proceselementen beter beheerst worden, zal dit tot een beter eindprodukt leiden. In het vervolg van dit artikel zal dan ook van beheerselementen in plaats van proceselementen gesproken worden.
De beheerselementen te zamen zullen ervoor moeten zorgen dat het bedrijfsproces op een zodanige

wijze functioneert dat zowel de externe communicatie met de klant, als de interne beheersing van het ondersteunende en primaire proces, optimaal verloopt. Het resultaat van een dergelijk bedrijfsproces is een eindprodukt van hoge kwaliteit.

Resteert nog een overzicht waarin de beheerselementen van zowel het ondersteunende als het primaire proces bijeen zijn gebracht. Omdat de beheerselementen Voorbereiding en uitvoering en Nazorg en evaluatie sterk afhankelijk zijn van het primaire proces waarop deze betrekking hebben, zal hier volstaan worden met de vermelding van de naam van het bedrijfsproces.

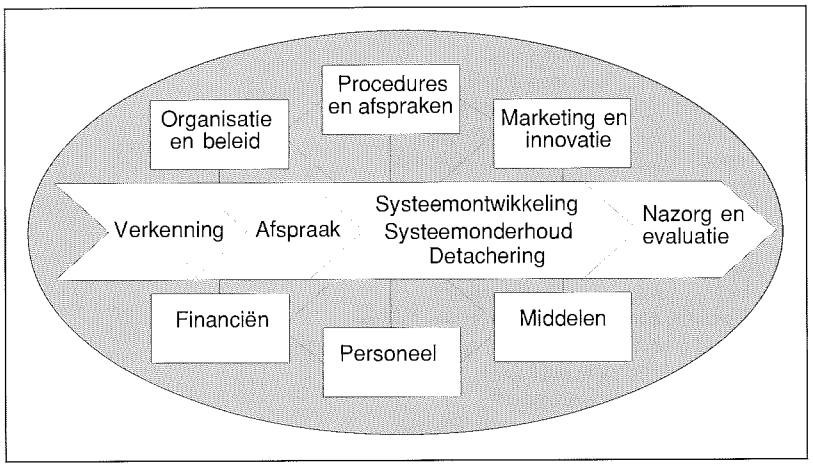
In figuur 3 worden de beheerselementen uit het ondersteunende en de verschillende primaire processen te zamen schematisch weergegeven.



Figuur 2. Primair proces: ontwikkeling, onderhoud en detachering.

DERDE LAAG, BEHEERSASPECTEN

De beheerselementen geven slechts een algemeen beeld van het proces. Voor de inzichtelijkheid van de procesbeheersing zal een nadere invulling van de proceselementen plaatsvinden met behulp van de zogenaamde beheersaspecten.
Hierbij dient in ogenschouw te worden genomen dat elk beheerselement ook weer een volledig proces representeert. De verschillende beheersaspecten te zamen zullen in principe dan ook weer alle elementaire proceselementen omvatten.



Figuur 3. Volledig bedrijfsproces: alle beheerselementen.

– *Structuur*
Een nadere structurering wordt op dit niveau niet nodig geacht. Reeds binnen twee andere deelprocessen – Organisatie en beleid alsmede Procedures en afspraken – heeft dit een plaats binnen de organisatie gevonden.

– *Invoer*
De invoer wordt eveneens al binnen andere proceselementen verzorgd. Verwezen wordt naar de beheerselementen Financiën, Personeel en Middelen. De invoer hoeft dan ook niet meer in andere beheerselementen te worden opgenomen.

– *Signaal*
Een trigger of signaal is ook voor processen op dit niveau nog wel steeds noodzakelijk. Niet alleen tijdens het starten van het proces, maar gedurende de gehele uitvoering wordt er voortdurend gecommuniceerd. In ieder geval zal er steeds sprake zijn van interne communicatie. Voor wat betreft de beheerselementen die deel uitmaken van het primaire proces vindt ook communicatie met de klant plaats.

– *Activiteit*
De uitvoering is eveneens een belangrijk onderdeel van elk van de beheerselementen. Er zullen dus steeds één of meer beheersaspecten zijn die een bepaalde activiteit inhouden.

– *Uitvoer*
Elk deelproces zal ook hier steeds tot een bepaalde uitvoer moeten leiden. Vaak zal binnen een beheerselement meer dan één activiteit plaatsvinden. Omdat de activiteiten en de daaruit voortvloeiende produkten vaak zeer dicht tegen elkaar liggen en meestal tussenprodukten zijn die in opvolgende processen weer verder bewerkt worden, zal alleen van activiteiten gesproken worden. Wel is getracht om het doel van het beheerselement – en daarmee de som van de tussenprodukten – duidelijk aan te geven.

Samengevat kan gesteld worden dat er binnen elk beheerselement sprake moet zijn van één of meer signalen en activiteiten alsmede van communicatie met andere beheerselementen of met de klant. Deze procesonderdelen moeten in elk van de verschillende beheersaspecten terug te vinden zijn.

Onderstaand zullen de beheersaspecten worden besproken waarbij gebruik gemaakt zal worden van de eerder gemaakte indeling in bedrijfsprocessen. De rangschikking van de beheersaspecten is zoveel mogelijk in overeenstemming met de normale volgorde van de operationele bedrijfsactiviteiten.

De beheersaspecten van het bedrijfsproces Algemeen

In het bedrijfsproces Algemeen wordt een nadere

ALGEMEEN

1.	**Organisatie en beleid**		
	(sign.)	1.1	lange-termijnbeleid
	(actv.)	1.2	invullen bedrijfsstructuur
	(actv.)	1.3	opstellen van financieel plan
	(actv.)	1.4	opstellen van personeelsplan
	(actv.)	1.5	opstellen van middelenplan
	(actv.)	1.6	opstellen overall-controleplan
	(comm.)	1.7	afstemmen plannen met betrokkenen
	(actv.)	1.8	nader uitwerken van de verschillende plannen
	(doel.)		randvoorwaarden scheppen voor de organisatie
2.	**Procedures en afspraken**		
	(sign.)	2.1	bedrijfsstructuur
	(actv.)	2.2	handboeken en werkinstructies
	(comm.)	2.3	afstemmen met betrokkenen
	(actv.)	2.4	gebruik van standaarden
	(actv.)	2.5	documentatie en beheer
	(doel.)		structuur aanbrengen binnen de organisatie
3.	**Financiën**		
	(sign.)	5.1	financieel plan
	(actv.)	5.2	financieel beleid
	(comm.)	5.3	afstemmen met betrokkenen
	(actv.)	5.4	financiële administratie
	(actv.)	5.5	debiteurenadministratie
	(actv.)	5.6	salarisadministratie
	(doel.)		beschikken over voldoende financiële middelen
4.	**Personeel**		
	(sign.)	4.1	personeelsplan
	(actv.)	4.2	personeelsbeleid
	(comm.)	4.3	afstemmen met betrokkenen
	(actv.)	4.4	werving, selectie en uitdiensttreding
	(actv.)	4.5	personeelsadministratie
	(actv.)	4.6	opleidingen
	(actv.)	4.7	functies en functioneren
	(actv.)	4.8	aanwezigheidsregistratie
	(doel.)		beschikken over voldoende deskundig personeel
5.	**Middelen**		
	(sign.)	5.1	plan voor middelenbeheer
	(actv.)	5.2	middelenbeleid
	(comm.)	5.3	afstemmen met betrokkenen
	(actv.)	5.4	inkoop
	(actv.)	5.5	configuratiemanagement
	(actv.)	5.6	onderhoud
	(actv.)	5.7	gebruikersondersteuning en systeembeheer
	(doel.)		beschikken over voldoende fysieke middelen
6.	**Verbijzonderde controle**		
	(sign.)	6.1	controleplan of eigen initiatief
	(actv.)	6.2	planning van de controle
	(comm.)	6.3	overleg met gecontroleerden
	(actv.)	6.4	onderzoek
	(comm.)	6.5	voorlopige conclusies
	(actv.)	6.6	rapport en aanbevelingen
	(doel.)		voldoende functioneren van de beheerssystemen
7.	**Marketing en innovatie**		
	(sign.)	7.1	periodiek, na een klacht of na beëindiging van een contract
	(actv.)	7.2	intern onderzoek
	(comm.)	7.3	evaluatie met de klant
	(comm.)	7.4	marktonderzoek
	(actv.)	7.5	verwerken resultaten
	(doel.)		blijvende aansluiting op de marktverwachtingen

Tabel 1. Algemeen bedrijfsproces.

uitwerking in beheersaspecten gegeven, waarbij uitgegaan wordt van de hierboven onderscheiden elementaire proceselementen.

– *Organisatie en beleid*

Allereerst zal er een structuur aan de organisatie gegeven moeten worden door het benoemen van afdelingen en functies.
Vervolgens zal hieraan invulling moeten worden gegeven door het ontwikkelen van een beleid voor de lange en middellange termijn. Op hoofdlijnen wordt een richtinggevend personeels-, financieel en middelenplan opgesteld. Uiteraard wordt daarbij gebruik gemaakt van de ervaring en deskundigheid uit de organisatie. De verdere uitwerking van de plannen gebeurt binnen de verschillende betrokken beheerselementen.
Ter bewaking van de structuur en de sturing van de activiteiten die binnen het proces een plaats vinden, wordt een controleplan opgesteld.
De beheersaspecten binnen dit beheerselement scheppen de randvoorwaarde voor een gestructureerde organisatie.

– *Procedures en afspraken*

Ook hier is sprake van structurering, maar dan veel meer gericht op de activiteiten en de binnen de organisatie te verrichten taken. Gedacht wordt aan het opstellen van documentatie, handboeken voor bijvoorbeeld administratieve organisatie en kwaliteit, alsmede het ontwikkelen van procedures in het algemeen. Ook het opstellen van werkinstructies wordt hieronder begrepen. Deze activiteiten zullen uiteindelijk moeten leiden tot een betere structuur en beheersing en daarmee tot een betere manier van werken binnen de organisatie.
Het doel van dit beheerselement is een nadere structuur aan te brengen in de activiteiten binnen de organisatie.

– *Financiën*

Het beheer van financiële middelen is voor de bedrijfsuitoefening van essentieel belang. Ondanks het feit dat ISO 9001 dit onderwerp uitdrukkelijk buiten beschouwing laat zal het hier toch worden behandeld. Het uitgangspunt van dit beheerselement is dat er steeds voldoende middelen aanwezig dienen te zijn om het primaire proces ongestoord te laten verlopen. De beheersaspecten die hieraan bijdragen zijn het opstellen van een financieel beleid en het voeren van verschillende administraties.

– *Personeel*

Het personeel vormt een belangrijk onderdeel van het kwaliteitssysteem. Behalve de bekende beheersaspecten die gericht zijn op een bepaalde structuur, een personeelsbeleid en -administratie, zal er ook aandacht besteed worden aan het welzijn van het personeel. Ontevreden medewerkers vormen nu eenmaal een ernstige bedreiging voor kwaliteit. Er zal dus veel aandacht besteed moeten worden aan het motiveren en begeleiden van personeel. Dit begint al met het werven van de juiste mensen voor de juiste functies en het bewaken van het functioneren en eventueel verder opleiden van de medewerkers. De beheersaspecten binnen dit beheerselement dienen te resulteren in een perso-

neelsbestand van een kwantitatief en kwalitatief voldoende niveau.

– *Middelen*
Gezien de eerdere keuze voor bedrijfsprocessen binnen de informatietechnologie, is het beheerselement Middelen voornamelijk gericht op het beheer van automatiseringsmiddelen en -technieken. Deze zullen op het moment dat dit nodig is binnen het primaire proces beschikbaar moeten zijn. Een belangrijk aspect van het middelenbeheer is het waarborgen van de betrouwbaarheid en continuïteit bij het gebruik van geautomatiseerde middelen. Dit vereist configuratiemanagement, systeembeheer en -onderhoud en gebruikersondersteuning (helpdesk) bij eventuele problemen.

– *Verbijzonderde controle*
Binnen de structuur van de organisatie dienen op de verschillende niveaus sturing en controle plaats te vinden.
Allereerst zal binnen de uitvoering van het proces zelf controle moeten plaatsvinden, bijvoorbeeld door zelf-, collegiale of lijncontrole. Eventuele fouten dienen zo spoedig mogelijk na hun ontstaan te worden gesignaleerd en vervolgens gecorrigeerd.
Daarnaast is er een apart boven het primaire proces fungerend sturings- en controlesysteem, waarmee de beheersing van het primaire proces wordt gerealiseerd en de kwaliteit ervan geborgd.
Als sluitstuk is er ten slotte een onafhankelijke controle, bijvoorbeeld de certificatie of de externe controle, die zekerheid zal moeten geven of de processen zelf, de sturing en beheersing van die processen, alsmede de controle op dit geheel naar behoren is verlopen. Dit valt buiten de beschreven bedrijfsprocessen en dus ook buiten het beheerselement Verbijzonderde controle.

– *Marketing en innovatie*
Periodiek zullen de structuur van de organisatie, het gevoerde beleid, de activiteiten en de resultaten daarvan moeten worden geëvalueerd. Belangrijk is dat gekeken wordt naar de ervaringen van klanten alsmede de positie van de eigen organisatie binnen de markt. Een dergelijke analyse kan leiden tot het verbeteren of wijzigen van de bestaande produkten en op termijn het ontwikkelen van nieuwe produkten. De beheersaspecten binnen deze beheerselementen zullen de optimale aansluiting op de marktbehoefte moeten bevorderen.

De beschrijving van het bedrijfsproces Algemeen, de beheerselementen en de daarbinnen onderscheiden beheersmaatregelen is in tabel 1 schematisch weergegeven.

De beheersaspecten van het bedrijfsproces Ontwikkeling

Uitgaande van de eerder onderscheiden beheerselementen zal voor het bedrijfsproces Ontwikkeling een nadere uitwerking van de aanwezige beheersaspecten worden gegeven. Wederom zal de eerder gemaakte indeling in elementaire procesonderdelen tot uitgangspunt dienen.

– *Verkenning*
Het eerste contact met de klant en de wijze waarop dit wordt ingevuld, is een belangrijke factor voor het verdere verloop van het primaire proces en de kwaliteit van het eindprodukt. Het zal voor beide partijen – op hoofdlijnen – duidelijk moeten zijn wat de wederzijdse wensen en eisen zijn ten aanzien van de opdracht. Onderzocht zal moeten worden of de leverancier in staat zal zijn het gevraagde produkt te leveren. Pas als beide partijen hiervan overtuigd zijn, wordt een offerte opgesteld.
Doel van dit beheerselement en de daarin opgenomen beheersaspecten is te komen tot een voor beide partijen acceptabele offerte.

– *Afspraak*
De tijdens de verkenning gemaakte afspraken worden in een overeenkomst geformaliseerd. Het voortbrengingsproces en het te verwachten eindresultaat alsmede de daarbij te hanteren toetsingsnormen dienen zo duidelijk mogelijk te worden vastgelegd. De afspraken met externe klanten krijgen tevens een juridische gelding, zodat ook juridische normen in de overeenkomst een plaats zullen moeten vinden.

– *Voorbereiding*
De gemaakte afspraken zullen in concrete activiteiten omgezet moeten worden. Daarvoor dient allereerst een gedetailleerd plan van aanpak te worden opgesteld, zullen de benodigde middelen definitief dienen te worden gereserveerd, etc. Dit zal uiteindelijk moeten resulteren in een door beide partijen geaccepteerd plan van aanpak voor de uitvoering van het project.
Het bijzondere en eenmalige karakter van systeemontwikkeling maakt deze bijzonder geschikt om projectmatig te werken. De voorbereiding en planning van het ontwikkelproject spelen dan ook een belangrijke rol. Bij het systeemonderhoud dat meer cyclisch van aard is speelt de voorbereiding een minder prominente rol. Detachering kent slechts een zeer korte planningsperiode, de voorbereiding zal daar vooral gelegen zijn in de opleiding en ervaring van de desbetreffende medewerker. Op deze verschillen zal nog nader worden teruggekomen.

– *Uitvoering*
In het model is bewust niet voor een specifieke methode van projectbeheersing gekozen. Afhankelijk van de specifieke omstandigheden zullen de klant en leverancier – in samenspraak – tot de meest geschikte methode moeten besluiten. Deze keuze zal in ieder geval in het projectplan, maar liefst al eerder, dienen te worden vastgelegd. Om te komen tot een voldoende aansluiting van de gekozen projectbeheersingsmethode met het beheerselement Uitvoering en de daarin aanwezige beheersaspecten, dient de gekozen methode minimaal te voorzien in een duidelijke projectstructuur en -uitvoering, voldoende tussentijdse test- en controlemomenten en een goede communicatie met de klant.

– *Oplevering*
De oplevering van het gereed produkt is een essentieel onderdeel van het systeemontwikkeltraject, omdat dit het opleveren van een deugdelijk en

ONTWIKKELING

1.	**Verkenning**		
	(sign.)	1.1	klantbehoefte
	(actv.)	1.2	eerste interpretatie
	(comm.)	1.3	verkennend overleg
	(actv.)	1.4	beoordelen haalbaarheid
	(actv.)	1.5	voorlopige offerte opstellen
	(comm.)	1.6	overleg met klant over voorlopige offerte
	(actv.)	1.7	opstellen definitieve offerte
	(doel.)		vastleggen van de klantwensen en de prestaties van de leverancier
2.	**Afspraak**		
	(sign.)	2.1	goedgekeurde offerte
	(actv.)	2.2	opstellen concept-contract
	(comm.)	2.3	overleg met klant over concept-contract
	(actv.)	2.4	opstellen definitief contract
	(doel.)		formaliseren van wederzijdse wensen en prestaties
3.	**Voorbereiding**		
	(sign.)	3.1	getekend contract
	(actv.)	3.2	opstellen van een concept-projectplan
	(comm.)	3.3	overleg met de klant over het concept-projectplan
	(actv.)	3.4	definitief projectplan
	(doel.)		duidelijke projectaanpak
4.	**Uitvoering**		
	(sign.)	4.1	definitief projectplan
	(actv.)	4.2	uitvoering van de projectfase
	(actv.)	4.3	modulaire test
	(comm.)	4.4	tussentijds afstemmen met de klant
	(actv.)	4.5	terugkoppelen uitkomsten
	(doel.)		deugdelijk deelprodukt
5.	**Oplevering**		
	(sign.)	5.1	gereed produkt
	(actv.)	5.2	integrale systeemtest
	(comm.)	5.3	gebruikersacceptatie
	(actv.)	5.4	overleg met de klant
	(comm.)	5.5	formele overdracht aan de klant
	(doel.)		opleveren van deugdelijk eindprodukt
6.	**Nazorg**		
	(sign.)	6.1	servicenoodzaak
	(actv.)	6.2	onderzoeken aansprakelijkheid
	(comm.)	6.3	maken afspraak
	(actv.)	6.4	verlenen van service
	(comm.)	6.5	verlenen decharge
	(doel.)		probleemloos functionerend systeem
7.	**Evaluatie**		
	(sign.)	7.1	projectbeëindiging
	(actv.)	7.2	onderzoek
	(comm.)	7.3	overleg met de betrokkenen
	(actv.)	7.4	verbeteringen implementeren
	(doel.)		aangepaste en slagvaardige organisatie

Tabel 2. Ontwikkeling.

door de klant gewenst eindprodukt tot doel heeft. Ondanks de verschillende modulaire tests die gedurende het voortbrengingsproces zijn uitgevoerd, zal de leverancier een afsluitende integrale systeemtest van het gehele produkt moeten uitvoeren, waarbij niet alleen aan de normaliter te stellen technische eisen, maar ook aan de – meest actuele – klantwensen getoetst zal moeten worden. Pas in tweede instantie vindt er een gebruikerstest plaats waarbij eventuele 'last minute'-fouten worden opgelost. Ten slotte volgt de gebruikersacceptatie en de formele overdracht van het gereed produkt aan de klant.

– *Nazorg*
De relatie met de klant zal ook na beëindiging van het voortbrengingsproces blijven voortduren. De in een eerdere fase overeengekomen garantieverplichtingen kunnen tot een hernieuwde activering van de relatie aanleiding geven. Dit beheersgebied is erop gericht om, ook na de formele kwijting, het opgeleverde systeem probleemloos te laten functioneren.

– *Evaluatie*
Na het beëindigen van een individueel project of na een vooraf vastgestelde tijdsperiode zal nagegaan moeten worden of de primaire en secundaire processen naar verwachting hebben gefunctioneerd. Daartoe zullen de gemaakte vastleggingen vergeleken moeten worden met eerder opgestelde prognoses alsmede met algemene ervaringsfeiten. Uiteindelijk zal dit kunnen resulteren in een bijstelling van de bestaande beheerselementen en uiteindelijk tot een slagvaardiger organisatie.

De beschrijving van het bedrijfsproces Ontwikkeling, alsmede de daarbij te onderscheiden beheerselementen en beheersaspecten is in tabel 2 schematisch weergegeven.

De beheersaspecten van het bedrijfsproces Onderhoud

Opnieuw, maar nu voor het bedrijfsproces Onderhoud, zal aan de hand van de eerder onderscheiden beheerselementen een overzicht van de aanwezige beheersaspecten worden gegeven. Omdat deze echter voor een belangrijk deel samenvallen met de beheerselementen en -aspecten die hiervoor reeds bij het bedrijfsproces Ontwikkeling zijn besproken, zal alleen naar de verschillen tussen beide worden gekeken.

Voor wat betreft het bedrijfsproces Onderhoud wordt er in dit model van uitgegaan dat de gebruikersapplicatie waarop het onderhoud wordt uitgevoerd, zich binnen het rekencentrum van de leverancier bevindt. De aanwezigheid en het functioneren van de verschillende beheerssystemen binnen dit rekencentrum (zoals toegangsbeveiliging, change management, produktiebesturing, etc.) worden gezien als een verantwoordelijkheid van de leverancier.

– *Verkenning*
In tegenstelling tot Ontwikkeling, waar de werkzaamheden in principe eenmalig en uniek zijn, zal er binnen het rekencentrum van de leverancier sprake zijn van een reeds bestaand beheersmechanisme voor de feitelijke beheersing van de aanwezige gebruikersapplicaties. De leverancier zal ernaar streven nieuwe klanten zoveel mogelijk binnen de reeds bestaande manier van werken in te passen. De klant en de leverancier zullen in overleg moeten uitmaken of, en zo ja in hoeverre, van deze interne rekencentrumstandaarden afgeweken kan worden.

– *Voorbereiding*
Alle periodieke en een deel van de incidentele onderhoudswerkzaamheden worden in een onder-

houdsplan vastgelegd. Voor de niet-voorspelbare onderhoudswerkzaamheden zal op de verschillende beheerssystemen binnen het rekencentrum vertrouwd moeten worden (helpdesk, problem en change management).
Hoewel hier alleen gesproken wordt over onderhoud, zal ook voor de reguliere exploitatie van de gebruikersapplicatie gebruik worden gemaakt van de beheersmechanismen binnen het rekencentrum.
In alle gevallen zal voorafgaand aan het onderhoud – in feite aan de exploitatie in het algemeen – een produktie-acceptatietest plaatsvinden, waarbij gekeken wordt hoe de gebruikersapplicatie het beste binnen de verschillende beheerssystemen van het rekencentrum geïmplementeerd kan worden. Na een positieve produktie-acceptatietest zal de nieuwe gebruikersapplicatie – voor wat betreft de onderhoudsverplichting – in ieder geval onder de specifieke beheersing van het helpdesk-, het change en het problem management-mechanisme gebracht moeten worden.

– *Uitvoering*
De voorzienbare onderhoudsactiviteiten worden in het systeem van change management ingevoerd, waarna vervolgens de voortgang van de uitvoering wordt bewaakt.
Het is aan de klant om te bepalen in welke mate er onderhoud moet worden gepleegd. Door middel van een prioriteitenmechanisme kan de leverancier erop toezien dat voor de klant onbelangrijke zaken (lage prioriteit) niet of in een later stadium worden uitgevoerd. Een dergelijk prioriteitenmechanisme kan ook op tijd (totale uren onderhoud) of op geld (totale kosten onderhoud) gestuurd worden.
Urgente problemen die bij de klant ontstaan worden afgehandeld via de helpdesk. Deze kan de problemen vervolgens zelf oplossen, of als dit onmogelijk is, doorgeven aan het problem management. In minder dringende gevallen worden de verzoeken omgezet in een change request. Interne produktieproblemen gaan, afhankelijk van de urgentie daarvan, direct of naar het problem of naar het change management.
Nadat de programmatuur is aangepast, zal deze intern getest dienen te worden. Vervolgens zal de herziene programmatuur aan de klant ter acceptatie worden aangeboden en na akkoord definitief worden geïmplementeerd.

– *Nazorg*
Onderhoud wordt niet beschouwd als een eenmalig, maar als een voortdurend proces. De nazorg van het onderhoud zit als het ware ingebouwd in de volgende onderhoudsronde en hoeft dan ook niet meer apart te worden gespecificeerd.

Ten slotte wordt nog opgemerkt dat bij de besproken onderhoudswerkzaamheden er steeds van uitgegaan wordt dat de noodzaak van het onderhoud vooral voortkomt uit een technische oorzaak en niet zozeer uit een – functionele – gebruikerswens. Voor dit laatste kan beter aansluiting worden gezocht bij het bedrijfsproces Ontwikkeling.

De beschrijving van het bedrijfsproces Onderhoud, alsmede de daarbij te onderscheiden beheerselementen en beheersaspecten is in tabel 3 schematisch weergegeven.

ONDERHOUD

1.	**Verkenning**		
	(sign.)	1.1	verzoek klant
	(actv.)	1.2	eerste inventarisatie
	(comm.)	1.3	verkennend overleg met de klant
	(actv.)	1.4	onderzoek van het systeem
	(actv.)	1.5	voorlopige offerte opstellen
	(comm.)	1.6	overleg met de klant
	(actv.)	1.7	opstellen definitieve offerte
	(doel.)		vaststellen klantbehoefte en eigen mogelijkheden
2.	**Afspraak**		
	(sign.)	2.1	goedgekeurde offerte
	(actv.)	2.2	opstellen contract
	(comm.)	2.3	overleg met de klant
	(actv.)	2.4	opstellen definitief contract
	(doel.)		formaliseren wederzijdse wensen en prestaties
3.	**Voorbereiding**		
	(sign.)	3.1	definitief contract
	(actv.)	3.2	opstellen onderhoudsplan
	(actv.)	3.3	opstellen draaiboek
	(comm.)	3.4	overleg met de klant
	(actv.)	3.5	aansluiten op bestaand beheersmechanisme
	(doel.)		duidelijke onderhoudsaanpak
4.	**Uitvoering**		
	(sign.)	4.1	onderhoudsplan
	(actv.)	4.2	change management
	(actv.)	4.3	prioriteitenmechanisme
	(comm.)	4.4	helpdesk en problem management
	(actv.)	4.5	uitvoeren werkzaamheden
	(actv.)	4.6	systeemtest
	(comm.)	4.7	acceptatie door de klant
	(actv.)	4.8	implementeren
	(doel.)		deugdelijke reparatie
5.	**Evaluatie**		
	(sign.)	5.1	periodiek
	(actv.)	5.2	onderzoek
	(comm.)	5.3	evaluatie met de klant
	(actv.)	5.4	terugkoppelen bevindingen
	(doel.)		deugdelijk systeem van onderhoud

Tabel 3. Onderhoud.

De beheersaspecten van het bedrijfsproces Detachering

De beheersaspecten binnen Detachering komen slechts voor een deel overeen met die van het bedrijfsproces Ontwikkeling. Zo is het onderdeel Verkenning vervangen door het beheersaspect Verzoek en zijn de onderdelen Voorbereiding, Uitvoering, Oplevering en Nazorg samengevat in het beheersaspect Volgen op afstand. De beheersaspecten Afspraak en Evaluatie zijn in grote lijnen gelijk met hetgeen bij het bedrijfsproces Ontwikkeling is beschreven en zullen dan ook niet nogmaals behandeld worden.

– *Verzoek*
De inzet van gedetacheerd personeel is een zeer flexibel proces, dat in sterke mate door de markt wordt bepaald. Door deze onzekere factoren is een goede kennis van de markt, en daarmee een betrouwbare voorspelling van de te verwachten marktontwikkeling, onontbeerlijk.

DETACHERING

1.	**Verzoek**	
(sign.)	1.1	verzoek klant
(actv.)	1.2	beschikbaarheid
(comm.)	1.3	kennismaking
(actv.)	1.4	opstellen definitieve offerte
(doel.)		vaststellen klantbehoefte en eigen mogelijkheden
2.	**Afspraak**	
(sign.)	2.1	goedgekeurde offerte
(actv.)	2.2	opstellen contract
(comm.)	2.3	overleg met de klant
(actv.)	2.4	opstellen definitief contract
(doel.)		formaliseren wederzijdse wensen en prestaties
3.	**Volgen op afstand**	
(sign.)	3.1	periodiek
(actv.)	3.2	bijhouden tewerkstellingen
(actv.)	3.3	begeleiden gedetacheerden
(actv.)	3.4	urenbriefjes
(comm.)	3.5	overleg met de klant
(actv.)	3.6	terugkoppelen bevindingen
(doel.)		goed functionerende medewerker en tevreden klant
4.	**Evaluatie**	
(sign.)	4.1	einde opdracht
(actv.)	4.2	onderzoek
(actv.)	4.3	evaluatie met gedetacheerde
(comm.)	4.4	evaluatie met de klant
(actv.)	4.5	terugkoppelen bevindingen
(doel.)		tevreden klant en medewerker

Tabel 4. Detachering.

Wat geldt voor het personeelsbeheer in elk bedrijfsproces, geldt voor detachering in versterkte mate: de juiste man op de juiste plaats. Binnen de detacheringsorganisatie zal er dus een actueel en betrouwbaar inzicht moeten zijn in de beschikbaarheid en kwalificaties van de medewerkers. Aan de andere kant zullen de klantwensen duidelijk moeten zijn, zowel wat betreft de deskundigheid alsook de persoonlijkheidskenmerken van de gedetacheerde. Het is dan ook van belang dat de gedetacheerde altijd aan de klant wordt voorgesteld.

– *Volgen op afstand*
Detachering heeft als bijzondere eigenschap dat het uitvoerende werk niet bij de leverancier maar bij de klant plaatsvindt. Door de leverancier zal er alleen op moeten worden toegezien dat het contact tussen de klant en de gedetacheerde optimaal verloopt waarna dit proces verder op afstand gevolgd kan worden. Vervolgens kan periodiek worden bezien of er misschien nog verbeteringen mogelijk zijn.

De beschrijving van het bedrijfsproces Detachering, alsmede de daarbij aan de orde zijnde beheerselementen en beheersaspecten is schematisch weergegeven in tabel 4.

BEHEERSMAATREGELEN

In het bovenstaande globale model is weliswaar op hoofdlijnen een aantal belangrijke onderwerpen behandeld, maar daarbij is nog niet tot op het niveau van specifieke – beheers – maatregelen gedifferentieerd. In het kader van dit artikel zou het echter te ver voeren om het gepresenteerde model nog verder uit te diepen.
Volstaan wordt met de opmerking dat een dergelijke volledige uitwerking van het model – tot op het niveau van de beheersmaatregelen – wel heeft plaatsgevonden. Daarbij is met name gebruik gemaakt van AO-maatregelen en de gedetailleerde uitwerking van EDP-auditingcriteria. Door de geïnteresseerde kan een dergelijke detailuitwerking van het model bij de auteurs besteld worden.

BEHEERSMAATREGELEN BINNEN ONTWIKKELING

1. Verkenning
1.1 klantbehoefte
1.2 eerste interpretatie
- verzoek van klant geregistreerd
- strikte voortgangsbewaking
- eerste screening van de klant
- is het juiste produkt in huis

1.3 verkennend overleg
- door deskundige personen
- duidelijke afspraken

1.4 beoordelen haalbaarheid
- eerste uitwerking, belangrijkste functionaliteiten
- kan produkt gemaakt worden
- is er reeds ervaring met soortgelijk produkt
- is er voldoende capaciteit

1.5 voorlopige offerte opstellen
- schriftelijk
- activiteiten op hoofdlijnen
- de kritieke succesfactoren bepalen
- inventariseren functiepunten
- methode van projectbeheersing
- deelprodukten
- globale functiepuntanalyse
- globale doorlooptijd
- globale voorcalculatie
- wijze van financieren
- voorlopige reserveringen

1.6 overleg met klant over voorlopige offerte
- door deskundige personen
- opstellen globale acceptatiecriteria
- duidelijke afspraken

1.7 opstellen definitieve offerte
- bevoegde functionaris
- vastlegging in register
- voortgang bewaken

Tabel 5, Beheersmaatregelen.

Bij wijze van illustratie is in tabel 5 een voorbeeld van de detailuitwerking tot op maatregelniveau van het beheerselement Verkenning van het bedrijfsproces Ontwikkeling bijgevoegd.

TOT BESLUIT

Onderstaand één waarschuwing, twee conclusies en een uitnodiging.

Allereerst is het belangrijk te beseffen dat er verschillende betekenissen aan het woord kwaliteit gehecht kunnen worden. Een zinvolle communicatie zal dan ook vooraf gegaan moeten worden door een eenduidige keuze van het kwaliteitsbegrip, waarbij het brede en duidelijk gedefinieerde ISO-kwaliteitsbegrip de voorkeur verdient. Een belangrijk voordeel daarbij is dat de EDP-auditor een bredere visie op het bedrijfsproces wordt geboden.

Vervolgens kan worden geconcludeerd dat er een belangrijke overlap bestaat tussen EDP-auditing en de ISO-kwaliteitszorg. Beide richten zich op de verbetering van de beheersing van het bedrijfsproces. Alleen de wijze waarop en de mate waarin dit gebeurt zijn verschillend.

In het verlengde hiervan is vastgesteld dat waar sprake is van een samenloop tussen EDP-auditing en ISO-kwaliteitszorg, verrassenderwijs steeds sprake is van een duidelijke onderlinge aanvulling en zelfs een wederzijdse versterking. Zo blijft een groot voordeel van ISO, namelijk het gebruik van een duidelijk en breed geaccepteerd normenstelsel, bestaan. Aan de andere kant wordt een nadeel van ISO, namelijk dat deze normen nogal algemeen en formeel zijn uitgewerkt, door de introductie van AO- en EDP-auditmaatregelen gecompenseerd. Er vindt als het ware een – noodzakelijke – onderbouwing van het ISO-kwaliteitssysteem plaats.
In aanvulling op de ISO-kwaliteitszorg kan de functie- en maatregelgerichte benadering die aan administratieve organisatie en EDP-auditing ten grondslag ligt, de bouwstenen en de dwarsverbanden leveren binnen het denken in processen.

In het gepresenteerde model is uitwerking gegeven aan de gedachte dat een ISO-kwaliteitssysteem met behulp van AO- en EDP-auditmaatregelen nader aangevuld en ingevuld zou kunnen worden. Daarbij is onder meer gebleken dat op het hoogste niveau vooral de invloed van ISO 9000 aanzienlijk is, terwijl op de onderliggende niveaus de betekenis van de administratieve organisatie en EDP-auditing sterk in betekenis toeneemt. Een oordeel over het nut en de bruikbaarheid van het model is echter aan de lezer.

LITERATUUR

[Bruij93] A.J.M. de Bruijn, *EDP-auditing, wat is het?*, De EDP-Auditor, april 1993.

[ISO88a] *ISO 9000, Kwaliteitszorg en normen voor kwaliteitsborging, Richtlijnen voor de keuze en toepassing*, Nederlands Normalisatie-instituut, september 1988.

[ISO88b] *ISO 9001, Kwaliteitssystemen, Model voor de kwaliteitsborging bij het ontwerpen/ontwikkelen, het vervaardigen, het installeren en de nazorg*, Nederlands Normalisatie-instituut, september 1988.

[ISO88c] *ISO 9002, Kwaliteitssystemen, Model voor de kwaliteitsborging bij het vervaardigen en het installeren*, Nederlands Normalisatie-instituut, september 1988.

[ISO88d] *ISO 9003, Kwaliteitssystemen, Model voor de kwaliteitsborging bij de eindkeuring en de beproeving*, Nederlands Normalisatie-instituut, september 1988.

[ISO89a] *ISO 8402, Kwaliteit, Termen en definities*, Nederlands Normalisatie-instituut, juli 1989.

[ISO89b] *ISO 9004, Kwaliteitszorg en de elementen van een kwaliteitssysteem, Richtlijnen*, Nederlands Normalisatie-instituut, september 1989.

[ISO91] *ISO 9000-3, Quality management and quality assurance standards. Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software*, International Organization for Standardization, 1991-06-01.

[ISO92] *ISO 9004-2, Kwaliteitszorg en elementen van een kwaliteitssysteem. Deel 2: Richtlijnen voor diensten*, Nederlands Normalisatie-instituut, maart 1992.

[Kame95] M.C. Kamermans en P.G. Noordam, *Certificering bij gegevens-verwerkingsorganisaties*, De Accountant, september 1995.

[Masa90] Masaaki Imai, *Kaizen de sleutel van Japans succesvolle concurrentie*, Kluwer 1990.

[Nieu95] R. Nieuwenhuizen, *Voorkom dubbel werk*, Controllers Magazine, april/mei 1995.

[NIVR89] NIVRA, *Automatisering en controle, Deel VII: Kwaliteitsoordelen over informatievoorziening*, NIVRA-geschrift 53, Kluwer 1989.

[Swin95] G.J.P. Swinkels, J.G. Verrijdt en G.J. van der Pijl, *Kwaliteitszorg, kwaliteitssysteem en certificering*, MAB, april 1995.

[Veld88] J. in 't Veld, *Analyse van organisatieproblemen, een toepassing van denken in systemen en processen*, Stenfert Kroese BV, 1988.

Omtrent dit artikel

Dit artikel is voor een belangrijk deel gebaseerd op de resultaten van een onderzoek dat is uitgevoerd door de Controle Sector EDP-Auditing van de Defensie Accountantsdienst. Daarbij is mede gebruik gemaakt van de expertise van KPMG EDP Auditors en KPMG Management Consulting. Met name de inbreng van ir. C.P.J. Plompen heeft in belangrijke mate bijgedragen aan het uiteindelijke resultaat van het voornoemde onderzoek.

De volledige tekst, bestaande uit zowel het globale als de detailuitwerking in beheersmaatregelen, kan worden verkregen door een verzoek hiertoe te richten aan één van de auteurs, per adres de Defensie Accountantsdienst, Controle Sector EDP-Auditing, Postbus 20701, 2500 ES 's-Gravenhage.

Mr. W.R. Nanninga RE
Is werkzaam bij de Controle Sector EDP-Auditing van de Defensie Accountantsdienst. Naast de auditing van rekencentra vormt de beheersing van geautomatiseerde gegevensverwerkende processen een belangrijk aandachtsgebied binnen zijn werkzaamheden. Daarnaast is hij docent SDW-AO en participant in verschillende werkgroepen op het gebied van de kwaliteitszorg.

Ltkol J.M.W. van de Garde RE
Is luitenant-kolonel bij de Koninklijke Luchtmacht en als EDP-auditor werkzaam bij de Controle Sector EDP-Auditing van de Defensie Accountantsdienst.

ITIL als inrichtings- en beoordelingsinstrument

Drs. F.J. Hut

Steeds meer organisaties adopteren ITIL als het beheerinstrument voor hun IT-omgeving, maar wat is ITIL eigenlijk en wat kunnen EDP-auditors ermee?
De auteur, die zich als gecertificeerd ITIL Service Manager bezighoudt met het inrichten van ITIL-processen, behandelt vanuit zijn praktijkervaringen de belangrijkste ITIL-processen, en de bruikbaarheid ervan als norm bij de uitvoering van EDP-audits.

INLEIDING

Bij het beheren van automatiseringsomgevingen geldt ITIL tegenwoordig als de standaard. Dat is een goede reden om ITIL eens nader onder de loep te nemen. Waar komt het vandaan, wat is het en waar staat het voor? En voor EDP-auditors: wat heb je eraan en welke normen zijn hieraan te ontlenen?
In dit artikel wordt op deze onderwerpen ingegaan, waarbij de auteur zijn persoonlijke visie geeft.

ITIL staat voor IT Infrastructure Library en is opgezet door de CCTA, een orgaan van de Britse overheid. ITIL bestaat uit een serie van ruim veertig boeken, waarin allerlei onderwerpen zijn beschreven, variërend van kabels en infrastructuur tot het kwaliteitsmanagement. Het doel van de serie boekjes is bij te dragen aan het verbeteren van de efficiency en effectiviteit van de IT-dienstverlening en het managen van de IT-infrastructuur in een willekeurige omgeving.[1]
In ieder boek is een afzonderlijk onderwerp nader uitgewerkt. De inhoud van ieder boek geeft weer wat – op moment van schrijven – de zogenoemde 'best business practice' was. Dit betekent dat omgevingen die volgens ITIL werken relatief goed scoren ten opzichte van andere omgevingen. Alleen daarom al is kennisneming van ITIL de moeite waard.

Ieder boek heeft een vaste indeling, wat de toegankelijkheid van de serie ten goede komt. In afzonderlijke hoofdstukken wordt beschreven welke voorbereidingen getroffen moeten worden, hoe invoering zou kunnen gebeuren, en hoe het resultaat van de invoering naderhand kan worden gecontroleerd. Deze controle achteraf is vooral operationeel van aard ('werkt het proces goed'). Een speciaal hoofdstuk in ieder deel beschrijft de kosten, baten en mogelijke problemen. Met name dit hoofdstuk is interessant voor EDP-auditors, omdat het een blik gunt op de echte problemen die kunnen optreden bij het inrichten van een bepaald proces. Deze beschrijvingen kunnen de EDP-auditor van dienst zijn als instrument bij het uitvoeren van risico-analyses en audits.
Een belangrijk pluspunt van de ITIL-reeks is verder dat alle onderwerpen onderling consistent worden beschreven, en dat de terminologie ook consistent wordt gehanteerd.

ITIL SERVICE MANAGEMENT

Sprekend over 'ITIL' wordt vaak 'ITIL Service Management' bedoeld. ITIL Service Management bestaat uit de volgende setjes boeken:
- de Service Support set, bestaand uit vijf delen die met name gaan over het stabiliseren en beheersen van de dagelijkse IT-dienstverlening;
- de Service Delivery set, bestaand uit vijf delen die met name gaan over het bedrijfsmatig exploiteren en aanbieden van IT-diensten;
- de Managers' set, bestaand uit zes delen die met name gaan over het managen van de verwerkingsorganisatie en van de relaties met klanten en leveranciers.

Dit artikel beperkt zich tot Service Support en Service Delivery. Beide gebieden samen worden aangeduid als Service Management.

SERVICE SUPPORT

Service Support houdt zich bezig met iets heel basaals, namelijk het zorgen voor de dagelijkse beschikbaarheid van de service. Iedere automatiseringsomgeving – groot, klein, intern en extern – ontleent hieraan het nut voor haar gebruikers, en iedere omgeving doet ook in meerdere of mindere mate aan Service Support.

Service Support is ver uitgekristalliseerd, vooral ook omdat het zo dicht staat bij de dagelijkse operationele problemen. In Nederland wordt ITIL Service Support veel toegepast, en is het een de facto standaard geworden voor het operationeel beheer van automatiseringsomgevingen.

Service Support bestaat uit de volgende processen:
- Configuration Management;
- Help Desk;
- Problem Management;
- Change Management;
- Software Control and Distribution.

Het is belangrijk te onderkennen dat ITIL *processen* beschrijft in plaats van afdelingen. Het is vervolgens aan de gebruiker van ITIL om de processen af te beelden op afdelingen.

Service Support-jargon
ITIL Service Support kent een eigen jargon, waarvan hieronder enkele begrippen worden gegeven.

Een *Incident* is een afwijking van de normale operationele gang van zaken. Dit hoeft niet te betekenen dat een systeem plat ligt of dat gebruikers niet kunnen werken; iedere afwijking van normaal is een incident.

Indien een incident vaak voorkomt, of onacceptabel ernstig negatieve gevolgen heeft, dan kan een *Problem* gedefinieerd worden. Het belangrijkste aan zo'n problem is dat de oorzaak ervan nog onbekend is.

Nadat de oorzaak van een problem is achterhaald, is het niet langer een problem maar wordt het een (Known) *Error*.

Om vervolgens de situatie structureel te verbeteren wordt een *Request For Change (RFC)* ingediend, waarna een *Change* wordt uitgevoerd.

De route incident – problem – error – change is niet verplicht. Ook zonder incidenten kan een problem worden gedefinieerd, en ook zonder problem kunnen changes worden aangevraagd.

Configuration Management

Het proces Configuration Management is het fundament voor Service Support. Het proces is gericht op het vastleggen, beheren en beheersen van componenten en hun onderlinge relaties, die worden vastgelegd in de Configuration Management Database (CMDB). Twee belangrijke vragen bij Configuration Management zijn de volgende:
- Welke zaken worden opgenomen?
- Welke mate van detail wordt hierbij aangehouden?

Het zal sterk van de organisatie afhangen welke keuzen worden gemaakt. Om enige voorbeelden te noemen:

Handleidingen en procedures horen bij een produkt. Een foute handleiding kan een bijzonder hardnekkige oorzaak van onbegrepen incidenten zijn. Het kan daarom een keus zijn om handleidingen en procedures onder het regime van Configuration Management te plaatsen.
Heeft iedereen een standaardwerkplek, dan is het registreren van het nummer van de werkplek voldoende. Zijn er daarentegen vier soorten PC's met verschillende componenten in gebruik, dan moet heel wat meer worden bijgehouden, zoals het merk PC, CPU, geheugen, ingebouwde kaarten, etc.
Als iedere gebruiker een diskettestation in de PC heeft, dan kan het veel werk zijn om softwarecomponenten te beheersen. Zonder diskettes is het Configuration Management veel eenvoudiger.

Configuration Management is, zeker bij hardwarecomponenten, een fysiek proces met labels, kabels, insteekkaarten, netwerkadressen, etc. Naarmate meer mensen zich met fysieke hardware bezighouden wordt het lastiger om de configuratie te blijven beheersen. Als organisaties groter worden en geografisch verspreid zijn, wordt Configuration Management nog weer lastiger, en als decentrale onderdelen zelfstandig hardware en software kunnen selecteren en aanschaffen, wordt Configuration Management zelfs een vrijwel onmogelijke opgave. Kortom, Configuration Management is geen dankbare taak, en een configuration manager zal een vasthoudende taakopvatting moeten hebben.
Om toch het hoofd boven water te houden is een zekere standaardisatie onontbeerlijk, en daarnaast zal het Configuration Management-proces op een zodanige manier moeten worden opgesplitst dat lokale wijzigingen ook lokaal worden geadministreerd.

1. The IT Infrastructure Library, An Introduction, CCTA. De ITIL-reeks wordt uitgegeven door HMSO, die boekhandel Kooyker in Leiden opgeeft als Nederlandse 'HMSO stockist and distributor'.

Help Desk

Het proces Help Desk heeft als doel na een incident de dienstverlening aan eindgebruikers zo snel mogelijk te hervatten. Daarnaast is het de vraagbaak voor alle gebruikersvragen. In principe is de Help Desk voor eindgebruikers het enige contact met de automatiseringsorganisatie.
Bij het inrichten van het proces Help Desk moeten eveneens verschillende keuzen worden gemaakt:

Het mag niet de automatiseerder zijn die bepaalt wanneer de service niet beschikbaar is.

- Wordt het een minimale Help Desk die de telefoon aanneemt en doorschakelt naar een specialist, of maken specialisten deel uit van de Help Desk?
- In hoeverre wordt de Help Desk centraal bemand en in hoeverre decentraal?
- Op welke manier wordt de samenwerking met andere afdelingen geregeld?

Problem Management

Het proces Problem Management heeft vooral een pro-actieve taak. De opdracht voor dit proces is om de oorzaken van problemen te achterhalen, en het optreden van incidenten zoveel mogelijk te voorkomen.

Problem Management heeft een nauwe relatie met het proces Help Desk. Enerzijds moet dat proces natuurlijk goed lopen, maar interessanter is het om de geregistreerde incidenten kritisch te beoordelen om de ernstige en/of structurele problemen vast te stellen. Nadat een problem is gedefinieerd volgt het achterhalen van de onderliggende oorzaken en het voorbereiden van de RFC, waarmee het stokje wordt doorgegeven aan Change Management.

Ook Problem Management kan weer op verschillende manieren worden vorm gegeven. Een vaste afdeling zou het werk kunnen uitvoeren, maar met name in grote en complexe omgevingen zijn zoveel specialismen nodig dat een vaste centrale groep niet praktisch is. Handiger is het in dat geval om problemen aan de relevante specialistische afdelingen toe te wijzen, en vervolgens de voortgang van de afhandeling te bewaken.

Change Management

Change Management heeft als missie om veranderingen en daaraan verbonden risico's te beheersen. De procesgang behelst een aanvraag (RFC), een toetsing van de risico's – waarvoor Configuration Management onontbeerlijk is – autorisatie, en controle achteraf.

Om te voorkomen dat dit proces een bottleneck vormt, kunnen verschillende routes worden gevolgd:
- standaardwijzigingen worden geregistreerd en minimaal getoetst;
- ingrijpende wijzigingen worden binnen het proces uitgebreid behandeld;
- urgente wijzigingen worden snel door het proces geloodst zonder stappen over te slaan.

Het doorvoeren van een wijziging kan voor sommige gebruikersgroepen lastig zijn, bijvoorbeeld bij een conversie waarvoor een systeem enige dagen uit de lucht moet. Toch zijn dergelijke ingrepen soms nodig, maar het mag niet de automatiseerder zijn die bepaalt wanneer de service niet beschikbaar is. Het Change Management-proces wordt binnen ITIL daarom in de organisatie verankerd door de Change Advisory Board (CAB), een soort stuurgroep. Bij voorkeur is ook de gebruikersorganisatie in deze groep vertegenwoordigd.
De CAB moet voldoende mandaat hebben om beslissingen te nemen en prioriteiten te stellen bij ingrijpende wijzigingen die consequenties hebben voor meer partijen.

Software Control and Distribution

Software Control and Distribution is een mix van Configuration Management en Change Management. In feite wordt software vaak reeds in Configuration Management meegenomen.

SERVICE DELIVERY

Service Delivery bestaat uit de volgende processen:
- Availability Management;
- Contingency Planning;
- Cost Management;
- Capacity Management;
- Service Level Management.

De Service Delivery-processen zijn geen de facto standaard, en staan ook relatief los van de ondersteuning van de dagelijkse exploitatie. Service Level Management was ten tijde van het verschijnen (1989) het neusje van de zalm, maar is onderhand een gedateerd werk. Toch zijn de onderliggende gedachten goed, en is het zeker nuttig om de onderscheidene processen eens afzonderlijk te belichten.

Availability Management

Availability Management heeft betrekking op de beschikbaarheid. Het proces doorloopt een cyclus van risico's analyseren, beschikbaarheid afspreken, meten en rapporteren. Lastig bij Availability Management is dat niemand goed kan omschrijven wat beschikbaarheid precies is, maar dit altijd uitdrukt in niet-onbeschikbaar zijn. Ter illustratie: Is een geldautomaat beschikbaar als het geld na tien seconden komt? En als het na één minuut komt? En na vijf minuten?
In feite is er maar één goede maat voor beschik-

baarheid, en dat is of de eindgebruiker goed heeft kunnen werken. Dit is lastig te meten.

Qua kosten en baten is Availability Management verder moeilijk te onderbouwen. Een goede invalshoek kan zijn om Problem Management in het kader van de pro-actieve taak ook beschikbaarheid te laten bewaken.

Contingency Planning

Contingency Planning is een concreet proces, dat zich richt op de continuïteit van de automatiseringsomgeving. Dit proces zou kunnen worden gezien als een zijstap van Availability Management, maar is sterker verweven met de feitelijke operatie.

Automatisering is natuurlijk maar één aspect uit vele, en om een bedrijf echt operationeel te houden moet veel meer geregeld zijn. Sinds kort heeft ITIL daarom ook een boek over Business Continuity Management, dat breder van opzet is en zich richt op de continuïteit van het gehele bedrijf.

Cost Management

De processen Cost Management, Capacity Management en Service Level Management vormen, mits goed ingevuld, een drieluik met allerlei dwarsverbanden. De samenhang kan als volgt worden gezien: Service Level Management regelt de afspraken, Capacity Management is het technisch geweten van de gemaakte afspraken, en Cost Management is het financieel geweten.

Cost Management houdt zich dus bezig met kosten. ITIL maakt hierbij duidelijk onderscheid tussen:
- de kosten die in rekening worden gebracht;
- de kosten die zelf worden gemaakt.

Voor rekencentra is doorbelasten een bekend fenomeen. Meestal echter is de doorbelasting gebaseerd op technische zaken zoals I/O's, gigabytes opslagruimte en CPU-seconden. Een klant kan daar niets mee, want die verkoopt polissen, bestelt onderdelen of voert een ander onderdeel van een primair proces uit. Het is de klant dan vaak ook volkomen onduidelijk wat hij eraan kan doen om kosten te beheersen.

Dergelijke doorbelasting op technische basis kan ook leiden tot ongewenste effecten, zoals blijkt uit het volgende voorbeeld:
CPU-seconden zijn de basis voor doorbelasting. De belangrijkste applicatie kan met een beperkte investering worden geoptimaliseerd, waarbij het CPU-gebruik met tachtig procent kan worden teruggedrongen. De automatiseringsorganisatie heeft er geen belang bij deze optimalisatie uit te voeren, omdat dit allereerst geld kost, en vervolgens de opbrengsten van de doorbelasting doet verminderen. De automatiseringsorganisatie besluit daarom de optimalisatie niet uit te voeren.

Doorbelasten zal dus moeten gebeuren op basis van het bedrijfsproces van de klant. In feite is dit niets anders dan Activity Based Costing, maar dan voor automatisering. Invoering hiervan zal geruime tijd kosten, onder andere omdat de meetpunten hiervoor vaak nog binnen applicaties moeten worden aangebracht.

Bij het introduceren van Cost Management is het van groot belang dat de automatiseringsorganisatie in kwestie ook ruimte heeft om zelf te ondernemen. Om een voorbeeld te noemen: electronic mail mag per bericht niet meer kosten dan de postzegel die betaald zou zijn voor briefpost. Bij introductie van zo'n dienst moet dan misschien eerst een jaar verlies gemaakt kunnen worden, en de ruimte hiervoor moet dan wel aanwezig zijn.

Verder heeft Cost Management een raakvlak met Capacity Management: als nieuwe technologie goedkoper is, kan Cost Management initiatief nemen om deze technologie aan te gaan wenden. Een en ander zal in nauw overleg met Capacity Management worden voorbereid.

Capacity Management

Capacity Management zorgt dat voldoende capaciteit voorhanden is. Bovendien moet de aanwezige capaciteit optimaal worden benut.

Capacity Management kent enerzijds technisch getinte taken:

- Er moet voldoende hardware beschikbaar zijn, en de beschikbare hardware moet optimaal worden benut. Hiervoor is het nodig om in het besturingssysteem metingen te verrichten, om daarna gebaseerd op onder andere technisch inzicht een systeem uit te breiden of systeeminstellingen te wijzigen.

- Applicaties moeten goed worden gebouwd, geconfigureerd en vooraf op performance-aspecten worden doorgemeten. Uitgaand van het verwachte gebruik van een applicatie kan vervolgens worden berekend hoeveel verwerkingscapaciteit voor deze applicatie nodig is.

Naast de technische kant heeft Capacity Management ook een sterk organisatorische component. Om over een jaar de goede capaciteit te leveren, is het namelijk nodig om te weten hoe de wereld er dan uit zal zien. Hoeveel personeel is waarmee bezig? Wat zijn de verwachte verkoopvolumes? Worden verwerking in Europa en Azië geïntegreerd? Om dit soort zaken te kunnen weten moet Capacity Management stevig geworteld zijn in de planningscycli op hoog niveau.

Service Level Management

Als bekroning van Service Management is er het proces Service Level Management. De doelstelling ervan is eenvoudigweg dat klant en automatisering tot wederzijds voordeel zakelijk met elkaar omgaan.

Dit zakelijk met elkaar omgaan houdt in dat in ieder geval duidelijk moet vastliggen welke diensten worden geleverd en met welke kwaliteit (de rekencentrumkant), maar tegelijk ook hoe het werk wordt aangeleverd, en om welke hoeveelheden dat dan zal gaan (de kant van de klant). In een steeds veranderende wereld zullen ook eenmaal gemaakte afspraken moeten worden bijgesteld. Het resultaat van Service Level Management bestaat daarom enerzijds uit de gemaakte afspraken (Service Level Agreement of SLA), en daarnaast uit een continu proces waarbij beide partijen doorlopend blijven afspreken, meten, rapporteren en bijstellen.

Invullen van Service Level Management is voor een belangrijk deel ook een zaak van cultuur. Het rekencentrum moet eraan wennen – en dat is op zich al moeilijk genoeg – maar daarnaast moet ook de klant erin willen meegaan. Waar vroeger werd gerend als de klant ineens iets onmogelijks vroeg, komt nu een Service Level Manager op bezoek die doorspreekt wat gebeuren moet, die mogelijke negatieve consequenties aangeeft, en die ook nog aangeeft welke extra kosten met de extra wensen zijn gemoeid. Zowel klant als automatiseerder zal aan zo'n nieuwe aanpak moeten wennen, en zeker in het begin geneigd zijn de formele route over te slaan.

Om Service Management adequaat te kunnen invullen, zijn alle voorgaande Service Support-processen nodig.

STELLINGEN OVER ITIL

Onderstaand zijn enige stellingen over ITIL opgenomen. De stellingen zijn prikkelend geformuleerd, maar tegelijk serieus bedoeld.

Stelling 1: *Iedere organisatie met een behoorlijke automatisering is al tachtig procent ITIL.*
ITIL is gewoon gezond verstand. Dat gezonde verstand is niet alleen voorbehouden aan de CCTA, maar is ook in Nederland voorhanden. Ook zonder ITIL zijn helpdesks ontstaan, worden componenten vastgelegd en beheerd, wordt een formeel traject voor wijzigingen afgesproken, etc. De opbrengsten van ITIL kunnen dan ook wel eens behoorlijk tegenvallen, omdat ITIL feitelijk niet zoveel verschilt met de bestaande situatie.

Stelling 2: *ITIL Service Management heeft weinig te maken met automatisering.*
Service Management kan zonder ingrijpende aanpassingen ook worden toegepast in een koekjesfabriek. De processen beschrijven vooral de vorm waarin moet worden gewerkt. De feitelijke werkzaamheden en de vakkundigheid waarmee deze werkzaamheden worden uitgevoerd, vallen buiten ITIL.

Stelling 3: *Heel veel ITIL bestond al lang voor ITIL.*
Nutsbedrijven weten al jaren welke componenten in de grond liggen, weten wanneer ze vervangen moeten worden, kunnen risico's van onderhoud inschatten, maken afspraken over de afname, meten beschikbaarheid, bereiden uitvalscenario's voor, etc. Wat is er eigenlijk nieuw aan ITIL?

Stelling 4: *ITIL is geen methode.*
ITIL is een verzameling boekjes waarin waardevolle gedachten zijn neergelegd. De lezer van de boekjes moet zich deze gedachten eigen maken, en er vervolgens uit selecteren wat hij kan gebruiken. ITIL kent geen voorgeschreven route of fasering, en geen nauwkeurig beschreven eindresultaat.

Stelling 5: *ITIL ademt de sfeer van een centrale verwerkingsomgeving.*
De problematiek van grootschalige decentrale verwerking, de logistiek van wijzigingen en de moeilijk te beheersen veelvormigheid van al deze decentrale systemen komen in ITIL niet tot uiting. Met wat creativiteit is hieraan echter best iets te doen.

Stelling 6: *Er zijn goede argumenten nodig om **niet** aan ITIL te doen.*
ITIL is een heel bruikbaar kader om ondersteunende processen in te richten. Zelf het wiel weer uitvinden is niet efficiënt.

DE INVOERING VAN ITIL

Het professionaliseren van automatisering kent vaak een heel simpele start: de klant vindt geleverde diensten te duur en van onvoldoende kwaliteit. Vanaf twee kanten kan daaraan dan worden gewerkt:
- automatisering probeert professioneler te werken, en adopteert ITIL Service Support;
- de klant krijgt (eist!) een Service Level Agreement (SLA).

Om een SLA te kunnen waarmaken zijn alle andere ondersteunende processen nodig. Met name de laatste jaren hoort een SLA er gewoon bij, en wordt automatisering vaak gedwongen een SLA af te geven voordat de ondersteunende processen zijn ingericht. Dat wordt dan een oncomfortabel jaar, maar het goede nieuws is wel dat de klant nog steeds met zijn leverancier in gesprek is. Deze relatie met de klant is van groot belang, want uiteindelijk bepaalt de subjectieve beleving van de klant of hij zaken wil blijven doen of niet.

Ook zonder dwang van de zijde van de klant is het verstandig om van twee kanten te werken. Het inrichten van ondersteunende processen kost geruime tijd, en in die periode is de automatisering eigenlijk niet geëquipeerd om een SLA waar te maken. De dialoog met de klant, het wennen aan SLA's en het omgaan met de overlegstructuren hebben echter ook ruim de tijd nodig, zodat het verstandig is om Service Support en Service Delivery niet volgtijdelijk maar parallel in te richten.

Zoals eerder gesteld zijn alle processen nodig om een SLA echt te kunnen waarmaken. Inclusief cultuuromslag zal daar minimaal een jaar of enige jaren doorlooptijd mee gemoeid zijn. Het is niet verstandig om zo lang bezig te zijn zonder tussentijds succes, zodat al eerder een ITIL-deelproces

moet zijn ingericht. Een hanteerbare volgorde is de volgende:

Fase 1: Vlug scoren: Help Desk en Problem Management.

Fase 2a: Noodzakelijk voor stabiliteit: Configuration Management en Change Management.

Fase 2b: Vooral de klant niet vergeten: eerste fase Service Level Management.

Fase 3: Afmaken: Contingency Planning, met daarna de rest van Service Delivery.

In kleinschaliger omgevingen is het invoeren van ITIL lastiger. De schaalgrootte ontbreekt om processen op een voor de hand liggende manier op te splitsen, en het is onvermijdelijk dat medewerkers meer rollen in meer processen zullen gaan vervullen. Speciaal voor dit soort omgevingen is onlangs een lezenswaardig boekje uitgekomen.[2]

ITIL BIJ GROOTSCHALIGE DECENTRALE VERWERKING

Beheren en beheersen van centrale mainframe-omgevingen gelden in het algemeen niet meer als groot probleem voor het management. De omgeving is bekend, er zijn voldoende beheerhulpmiddelen, en procedures zijn onderhand ingeslepen. Met wat gezond verstand (en dus ongeweten misschien wel tachtig procent ITIL) rolt die kar wel door.

Beheren en beheersen van grootschalige decentrale omgevingen blijken echter lang niet zo eenvoudig te zijn. Uitgaande van honderd decentrale omgevingen betekent het aanbrengen van een simpele wijziging dat deze honderd maal moet worden uitgevoerd en gecontroleerd. Overal aanbrengen van een ingrijpende wijziging betekent naast de logistiek ook nog eens dat op de avond van 'uitrol' op honderd plaatsen iemand fysiek aanwezig moet zijn. Uitrollen van een onvoldoend geteste versie betekent dat op honderd plaatsen herstelacties moeten worden uitgevoerd, die per omgeving verschillend kunnen zijn.

Als de praktische problemen in deze omgevingen in al hun omvang zichtbaar worden, komt vaak iemand op het idee van ITIL, en kijkt iedereen reikhalzend uit naar de oplossing van alle problemen. Bij het invoeren zal dan blijken dat beheerhulpmiddelen nog lang niet zo ver ontwikkeld zijn als in de mainframe-omgeving, en verder dat ITIL volgens het boekje te weinig aandacht schenkt aan het eigene van grootschalig decentraal verwerken.

Om ook in deze omgevingen een goed gereedschap te zijn, moet ITIL worden aangevuld en aangepast. Hieronder is uitgewerkt welke aanpassingen er naar de mening van de schrijver nodig zijn.

Capacity Management bij Service Support

Gebrek aan voldoende capaciteit is zonder ingericht Capacity Management-proces een frequente oorzaak van incidenten. Om een stabiele dienst aan te bieden, en dat is de taak van Service Support, moet Capacity Management adequaat zijn ingevuld. Voor decentrale omgevingen moet Capacity Management daarom niet bij Service Delivery maar bij Service Support zijn ingedeeld.

Service Support uitbreiden met Testen

In produktie brengen van foute componenten of programma's levert op iedere locatie herstelwerk op. Bij honderd locaties is dat honderd maal herstelwerk, en dit herstelwerk vraagt zoveel capaciteit dat de dagelijkse ondersteuning in het gedrang komt. Deze ondersteuning moet altijd doorgaan, en Service Support zou daarom moeten worden uitgebreid met een proces Testen om uitrol van foute componenten zoveel mogelijk te voorkomen. Voor een deel is voor het testen al een handreiking te vinden in de Software Support set.[3]

Met het echt kunnen waarmaken van een SLA is minimaal een jaar doorlooptijd gemoeid.

Logistieke appendix toevoegen aan Change Management

Change Management bestaat uit twee delen: het aanbrengen van wijzigingen en het besturen van het wijzigingsproces. Bij het aanbrengen van een zelfde wijziging op honderd locaties is het mogelijk hiervoor een change te definiëren met daaraan verbonden honderd uit te voeren acties. Een alternatief kan zijn om honderd aparte changes te definiëren.

Als de wijziging ingrijpend is, zal deze zoveel mogelijk worden gecombineerd met andere wijzigingstrajecten. Bijvoorbeeld: bij dertig sites wordt de wijziging meegenomen bij het installeren van nieuwe schijven, bij vijfentwintig sites met de uitrol van nieuwe database-software, en bij vijfenveertig moet de wijziging speciaal worden gebracht.

Het verschil tussen een change met honderd acties en honderd aparte changes komt naar voren als er halverwege problemen ontstaan. Statusinformatie per site is alleen makkelijk te krijgen als iedere locatie afzonderlijk kenbaar is. Honderd aparte changes zijn in dat geval verre te prevaleren boven een enkelvoudige change met honderd acties. Change Management zou daarom moeten worden uitgebreid met een logistieke appendix, waarin dit soort overwegingen verder wordt uitgewerkt.

Organisatieblauwdrukken

Verder bestaat in de grootschalige decentrale verwerkingsomgeving een groot palet van mogelijkheden de organisatie in te richten. Hierbij is te denken aan centrale, regionale en lokale invullingen. Afgeleid van de verantwoordelijkheden en van de mogelijkheden en beperkingen die de beheertechniek biedt, kunnen dan de ondersteunende proces-

2. *IT Infrastructure Library practices in small IT units, CCTA.*
3. *Testing an IT Service for Operational Use, CCTA.*

sen worden ingevuld. Het aantal mogelijkheden is echter zo groot dat gebruikers van ITIL baat zouden hebben bij enige karakteristieke organisatieblauwdrukken.

DE BRUIKBAARHEID VAN ITIL VOOR DE EDP-AUDITOR

Voor een EDP-auditor biedt ITIL een goed handvat bij de uitvoering van werkzaamheden. Concrete voordelen van ITIL zijn:

Begrip
De beschrijvingen van de ITIL-processen bieden een goed startpunt om inzicht te krijgen in een bepaald ondersteunend proces.

Terminologie
De binnen ITIL gehanteerde terminologie is eenduidig en consistent. Een incident, problem, error of change betekent altijd hetzelfde en wordt door alle ITIL Service Managers ook op ongeveer dezelfde wijze gebruikt. Met het stijgende aantal organisaties dat ITIL hanteert, wordt de ITIL-terminologie de gemeenschappelijke taal van de verwerkingsorganisaties. De EDP-auditor behoort deze taal te begrijpen, en bij voorkeur ook te spreken.

De EDP-auditor hoort de ITIL-taal te begrijpen en te spreken.

Kader voor normen
De ITIL-processchema's geven globaal de te volgen procedures weer. De processchema's zijn vrij globaal, maar iedere stap heeft vaak een praktische reden. Het is een goede oefening om een ITIL-procedure eens te doorlopen, en bij iedere stap de volgende vragen te stellen:
- Gebeurt dit hier ook?
- Zo nee, wordt deze controle, deze stap op een andere wijze uitgevoerd?
- Zo nee, welke risico's loopt het verwerkingsproces hierdoor?

Als resultaat ontstaat op deze manier een soort risico-analyse, waaruit op deelaspecten normen voor de verwerkingsomgeving kunnen worden afgeleid.

Samenhang
Alle processen zijn beschreven in hun onderlinge samenhang. Het wordt hierdoor mogelijk om zicht te krijgen op de totale ondersteuning, maar ook worden de onderlinge aansluiting en de afhankelijkheden van de verschillende processen duidelijk. Zo is het nauwelijks zinvol om Configuration Management in te voeren zonder tegelijkertijd Change Management in te richten. Geïsoleerde processen – hoe perfect ook volgens het boekje geïmplementeerd – zullen geen problemen oplossen, en moeten als onvoldoende worden beoordeeld.

Kwaliteit
In verschillende bijlagen van boekjes worden rapporten voorgesteld waarmee inzicht kan worden verkregen in de efficiency en effectiviteit van de desbetreffende processen. Dergelijke informatie kan een goede start zijn om inzicht te krijgen in de kwaliteit van zo'n ondersteunend proces.
Hierbij is een waarschuwing op zijn plaats. In de praktijk blijkt het nauwelijks mogelijk om een algemeen geldend rapportageraamwerk op te stellen. Iedere omgeving moet dit zelf inrichten.

Als voorbeeld: Incidenten moeten snel en liefst structureel worden verholpen. Het is een slecht teken als incidentmeldingen lange tijd open blijven, of als het aantal openstaande incidentmeldingen toeneemt. In de meeste gevallen is een incidentmelding die drie maanden blijft openstaan een teken van tekortkomingen in het proces. Soms echter ook niet, want als een systeem slechts eens per drie maanden wordt opgestart, dan is pas na drie maanden bij de volgende start duidelijk dat de snelle fix inderdaad het probleem heeft opgelost. Vervolgens wordt de incidentmelding gesloten, nadat zij zonder enig probleem drie maanden heeft opengestaan.

Implementatie
De ITIL-boekjes bieden een raamwerk voor implementatie van het beschreven proces. Deze informatie kan door een projectmanager worden gebruikt om een implementatie snel te starten, maar de EDP-auditor kan hetzelfde hoofdstuk gebruiken om te verifiëren dat geen voor de hand liggende zaken worden vergeten.

Aandachtsgebieden
Hoofdstuk 6 van ieder Service Management-boekje heeft als titel 'Benefits, Costs and Possible Problems'. Voor een EDP-auditor is dit een verplicht hoofdstuk, omdat het een snelle ingang biedt naar gangbare problemen die kunnen optreden rond een bepaald proces. Het hoofdstuk kan worden gebruikt als leidraad bij een risico-analyse van het proces, waarmee zowel een projectleider bij het inrichten als een EDP-auditor bij het beoordelen zijn voordeel kan doen.

Afbakening
ITIL-processen zijn duidelijk afgebakend, en steeds meer organisaties volgen ITIL. Niet overal echter worden afdelingen begrensd door het kaft van het desbetreffende ITIL-boekje. Aan de hand van ITIL-processen is echter vaak snel vast te stellen welke taken een afdeling uitvoert. De reikwijdte van een onderzoek is daarmee ook snel aan te geven.

DE BRUIKBAARHEID VAN ITIL ALS NORM

Is ITIL door de EDP-auditor te gebruiken als norm? Op deze vraag is niet direct een duidelijk ja of nee te geven. In de volgende alinea's wordt hierop nader ingegaan.

Beperkt
Uitgangspunten bij ITIL zijn efficiency en effectiviteit. Het aspect vertrouwelijkheid en maatregelen zoals functiescheiding zijn geen expliciet aandachtspunt. Het aandachtsgbied Security Management ontbreekt binnen Service Management vooralsnog geheel.
Al met al is ITIL Service Management daarmee te arm om in alle aspecten zelfstandig als norm te kunnen dienen. Indien ITIL echter wordt gecombineerd met bijvoorbeeld 'Control Objectives' van EDPAA/EDPAF, dan ontstaat daarmee een bruikbare combinatie.

Alleen processen
ITIL Service Management beschrijft processen, zonder voor te schrijven op welke wijze deze processen op de organisatie moeten worden afgebeeld. Iedere implementatie van ITIL wordt alleen daardoor al een creatief proces. Onderling verschillende implementaties kunnen nog steeds 'perfect ITIL' zijn. De bruikbaarheid van ITIL als toetssteen voor implementaties neemt daarmee af.

Organisatie-afhankelijk
Bij ieder proces moet de organisatie zelf de diepgang, de reikwijdte en de organisatorische inbedding van het proces vaststellen. Het is essentieel dat ITIL op de organisatie wordt toegesneden, want afhankelijk van allerlei factoren kunnen identieke implementaties in de ene organisatie perfect werken, en in de andere organisatie een fiasco zijn. Als norm wordt ITIL hierdoor vaag.

Een voorbeeld van het bovenstaande is de mate van detaillering bij Configuration Management. In een organisatie met standaardwerkplekken zonder diskettes, afgeschermde infrastructuur en strakke controle van de inkoop kan het prima werken om alleen het registratienummer van een werkplek vast te leggen, en alle andere details buiten de Configuration Management-registratie te houden. Dezelfde aanpak is tot mislukken gedoemd als meer soorten PC's worden gebruikt, elke PC diskettes kan gebruiken, de infrastructuur door gebruikers kan worden beïnvloed en de inkoop minder wordt gecontroleerd.

Generiek
ITIL Service Management beschrijft alleen *hoe* bepaalde zaken geregeld kunnen worden. De feitelijke uitvoering en de vakkundigheid van de betrokken medewerkers onttrekken zich aan het zicht van Service Management. Service Support heeft dan ook weinig specifiek met automatisering te maken, en kan evengoed worden toegepast om andere procesgangen te bewaken. Service Management is slechts losjes gekoppeld aan de automatisering. Hiervan afgeleide normen voor de automatisering zullen daarom alleen globaal kunnen zijn.

Centraal
ITIL Service Management is vooral geënt op centrale omgevingen. Voor gebruik in grootschalige decentrale omgevingen moet ITIL, zoals ook eerder is aangegeven, nog worden aangepast. Hierdoor is ITIL minder goed bruikbaar in andere dan (grootschalige) centrale omgevingen.

CONCLUSIES

Voor EDP-auditors met een taak in een verwerkingsomgeving is ITIL Service Support verplichte kost. Deze processen zijn ondertussen een de facto standaard, en bewegen zich op een gebied waar basale auditrisico's bestaan.

ITIL Service Delivery is geen de facto standaard, maar is wel een nuttig referentiekader bij specifieke onderzoeken naar continuïteit, efficiency en effectiviteit.

Voor grootschalige decentrale omgevingen is ITIL een goed startpunt. Het vergt echter creativiteit en praktijkkennis om de ondersteunende processen voor deze omgevingen met behulp van ITIL in te richten en te beoordelen.

Als norm is ITIL Service Management niet zonder meer toepasbaar. Het is globaal en generiek en het vergt, vooral in decentrale omgevingen, nog veel creativiteit. Op een hoger niveau is wel een norm te stellen, namelijk dat ieder proces aandacht moet hebben gekregen, en op de een of andere manier moet zijn ingevuld.

Als laatste is nog een waarschuwing op zijn plaats. ITIL heeft een hoog consultancy-gehalte, waarmee wordt bedoeld dat er weinig of geen absolute waarheden zijn, en het antwoord op eigenlijk iedere vraag zal beginnen met: 'Dat hangt ervan af, ...'. Het toepassen van ITIL, bij invoering maar ook bij beoordelingen, is daarom alleen verantwoord in combinatie met een dosis praktijkervaring.

Drs. F.J. Hut
Is onafhankelijk adviseur op het gebied van beheer en exploitatie van automatiseringsomgevingen. Hij heeft enige jaren als EDP-auditor gewerkt bij één van de grote accountantskantoren, en daarnaast heeft hij ervaring opgedaan met het inrichten en uitvoeren van verschillende Service Management-processen conform ITIL. Hij is gecertificeerd ITIL Service Manager, en houdt zich tegenwoordig vooral bezig met de inrichting van organisatie en processen in een grootschalige decentrale verwerkingsomgeving.

De Code voor Informatiebeveiliging

Dr. ir. P.L. Overbeek

Uit onderzoek blijkt dat in het Midden- en Kleinbedrijf (MKB) de meeste schade ontstaat als gevolg van een gebrekkige beveiliging. Beveiligingsmaatregelen hebben niet alleen betrekking op technische beveiliging; het gaat om een evenwicht tussen de maatregelen, ingebed in een passende organisatie. Om evenwicht tussen de maatregelen te realiseren is de Code voor Informatiebeveiliging ontwikkeld; een hulpmiddel dat ook toepasbaar is in het MKB. De basis is een verzameling van tien basisprincipes om een bodem te leggen voor beveiliging in uw organisatie.

INLEIDING

Informatiebeveiliging heeft nog immer een hoge attractiviteit voor de media. De incidenten die daarin breed worden uitgemeten, zijn echter niet representatief voor de huidige stand van de beveiliging. Uit verschillende onderzoeken, ook in Europees verband, blijkt namelijk dat het vooral het Midden- en Kleinbedrijf (MKB) is waar de meeste schade ontstaat door gebrekkige beveiliging. In de publiciteit is er vaak kritiek op de gebrekkige technische beveiliging. Ook deze kritiek is maar ten dele terecht. Het gaat immers altijd om het evenwicht tussen de beveiligingsmaatregelen: fysieke afscherming, technische hulpmiddelen, ondersteunende procedures, en dat geheel ingebed in een passende organisatie.
Juist met het oog op het evenwicht tussen maatregelen is de Code voor Informatiebeveiliging ontwikkeld: als een leidraad voor praktische informatiebeveiliging dat ook toepasbaar is in het MKB.

De Code is ontwikkeld in antwoord op de vraag naar praktische hulpmiddelen voor beveiliging van informatie in computers en netwerken. Hij biedt een gemeenschappelijke basis voor bedrijven om beveiligingsbeleid te ontwikkelen, de nodige plannen op te stellen, en zo tot 'beveiliging op maat' te komen.
De Code voor Informatiebeveiliging biedt een basis voor de bescherming van informatie. Deze basis wordt gegeven als een verzameling van tien basisprincipes voor informatiebeveiliging. In de eerste plaats is het de bedoeling van de Code om in eigen huis orde op zaken te stellen. Bovendien is de Code bedoeld als referentiekader tussen (elektronische) zakenpartners. In zaken moet men op elkaar kunnen vertrouwen. Dat geldt zeker als de organisatie afhankelijk wordt van (de beveiliging bij) partners waarmee elektronisch zaken worden gedaan, bijvoorbeeld als EDI of elektronische post wordt gebruikt.
De Code voor Informatiebeveiliging is ontstaan in Engeland. De Nederlandse introductie van de Code wordt onder andere gestimuleerd door het Ministerie van Economische Zaken, dat hiermee het belang van informatiebeveiliging voor het Nederlandse bedrijfsleven onderschrijft. Ook organisaties als FENIT, RCO en RIT ondersteunen het gebruik van de Code.

BEVEILIGINGSEISEN: EERST PRIORITEITEN STELLEN

Eerst moet duidelijk zijn welke doelstellingen de organisatie nastreeft voor wat betreft de te bereiken beveiliging. Een uitgebreide risico-analyse is niet altijd noodzakelijk. Veelal is het voldoende om een prioriteitenstelling te maken voor de meest urgente beveiligingseisen en -wensen. De eerste bron daarvoor is een inschatting van de grootste beveiligingsrisico's (bedreigingen en zwakke plekken) voor de informatie in de computers en netwerken; dit in het licht van het bedrijfsbelang. De tweede bron is een externe conformiteitsanalyse: wat schrijven wetten en contracten voor; en wat is goed gebruik in de branche. De derde bron is een interne toetsing: uitgaande van de bedrijfsdoelstellingen worden de implicaties bepaald voor de informatievoorziening en wordt de vraag beantwoord hoe de informatiebeveiliging daarop moet anticiperen. Afstemming met andere vormen van beleid, zoals het informatiebeleid en het algemene beveiligingsbeleid, is daarbij noodzakelijk.
De Code gaat uitgebreid in op de eerste bron met een beschrijving van risico's en mogelijke maatregelen. Voor de tweede en derde bron wordt een raamwerk gegeven.

Beveiligingscategorieën	Toelichting
Beleid	Doelstellingen; beschrijving te bereiken of na te streven situatie in termen van de bedrijfsbelangen.
Organisatie	Beveiligingsfuncties, taken en verantwoordelijkheden, samenhang en rapportagelijnen.
Classificatie en beheer	Rubriceringsschema's vormen het verband tussen de waarde, bijvoorbeeld van informatie, en de daarbij behorende beveiligingsmaatregelen. Voorbeelden: 'Geheim', 'Medisch', 'Privé' of 'Niet uitzetten'.
Personeel	Training, security awareness, veilig gedrag op de werkvloer, aannemingsbeleid en functioneringsbeoordeling.
Fysieke beveiliging & omgeving	Beveiliging van en in de infrastructuur, ook zaken als stroomvoorziening, datacommunicatielijnen, koeling, enz.
Computer- en netwerkbeheer	Beheer van de technische beveiliging; incidentrapportages; veilige systemen veilig *houden*.
Toegangsbeveiliging	Toegangsbeheersing en -autorisatie.
Bouw & onderhoud systemen	Aandacht voor de nodige beveiligingsfunctionaliteit en veilige ontwikkel- en onderhoudsmethoden leiden 'zeker' tot veilige systemen, die ook veilig blijven.
Calamiteit & continuïteit	Rampenplannen, uitwijk.
Toezicht	EDP-audit, interne controle.

Tabel 1. De tien categorieën voor beveiliging.

DE CODE NADER TOEGELICHT

Onderstaand worden de in de Code onderscheiden beveiligingscategorieën en de beveiligingsaanpak kort aangeduid.

Aandachtsgebieden voor informatiebeveiliging

In de Code zijn tien categorieën vastgesteld als aandachtsgebieden voor beveiliging (zie tabel 1). Iedere categorie is op dezelfde wijze opgebouwd: er zijn doelstellingen, en er is een basisset aan beveiligingsmaatregelen om een doelstelling te bereiken.

Voorbeeld: categorie 2, de organisatie van de beveiliging. De *doelstelling* is om een managementkader op poten te zetten voor informatiebeveiliging. Als *maatregelen* zijn ten minste vereist: het toekennen van verantwoordelijkheden, coördinatie tussen verantwoordelijken en duidelijke rapportagelijnen. *Activiteiten* zijn bijvoorbeeld: herziening van beleid, toezicht op veranderende risico's, opstellen van uitwijkplannen, reageren op incidenten, organiseren van externe onafhankelijke beoordeling van de beveiliging.

Alle categorieën worden zo behandeld: de doelstellingen, mogelijke beveiligingsmaatregelen (althans: de ondergrens), de bijbehorende activiteiten voor de selectie van maatregelen of, indien van toepassing, de concretisering in de vorm van een plan.

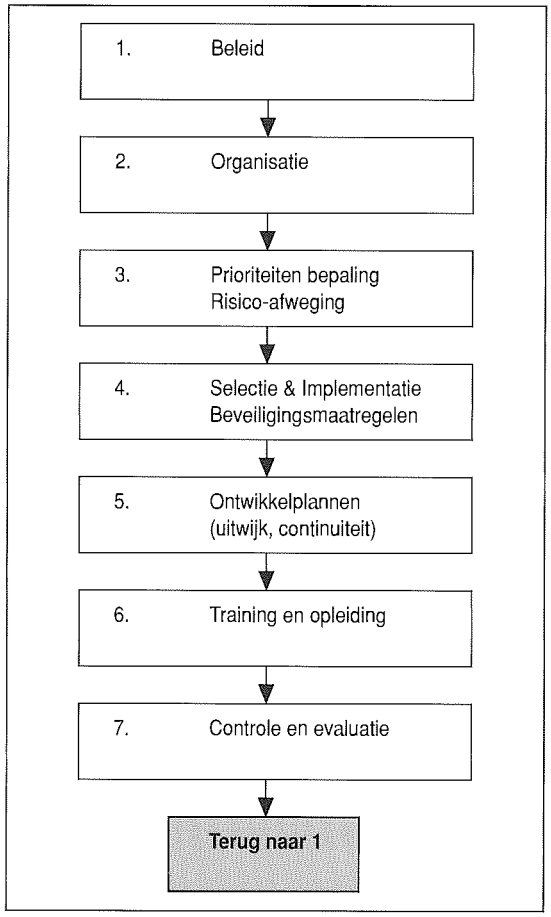
De belangrijkste maatregelen: het vertrekpunt

Om de drempel zo laag mogelijk te maken is een top 10 opgesteld van beveiligingsmaatregelen (zie tabel 2). Het uitgangspunt van de Code is dat deze maatregelen, althans initieel, boven aan het prioriteitenlijstje moeten staan.

Tabel 2. De top 10 voor beveiliging.

Belangrijkste maatregelen
• Doelstellingen voor beveiliging
• Verantwoordelijkheden
• Training en opleiding
• Rapportage van incidenten
• Viruscontrole
• Reageren op calamiteiten
• Import/export (o.a. programmatuur, informatie)
• Veiligstellen informatie (backup)
• Voldoen aan wet/regelgeving (o.a. privacy-wetgeving)
• Interne controle

Dr. ir. P.L. Overbeek
Is als EDP Audit Manager werkzaam bij KPMG EDP Auditors. Na zijn promotie op het onderwerp 'Secure Open Systems' heeft hij zich verder gespecialiseerd in informatiebeveiliging, beveiligingsstandaardisatie en evaluatiecriteria.



Figuur 1. Stappenplan voor het opzetten van een beveiligingsorganisatie.

Actieplan

Er is tevens een ondersteunend stappenplan beschikbaar als een 'vliegende start' voor het operationaliseren van een beveiligingsorganisatie (zie figuur 1).
Natuurlijk is beveiliging geen eenmalige exercitie maar een continu proces. Is de beveiliging eenmaal op orde, dan is het misschien de moeite waard om nogmaals naar de externe afhankelijkheden te kijken: voldoet de beveiliging bij zakenpartners aan de doelstellingen die de organisatie nastreeft voor wat betreft de te bereiken beveiliging?

TOT SLOT

De Code voor Informatiebeveiliging is een middel voor het leggen van een bodem, het noodzakelijke draagvlak, voor beveiliging in de organisatie. Met de Code kan ten minste een algemeen geldend minimumniveau voor beveiliging worden bereikt. Voor specifieke toepassingen zijn aanvullende maatregelen noodzakelijk, zoals overigens ook in de Code wordt aangegeven. Voorbeelden waarin extra maatregelen nodig zijn: de systemen waarmee bijzonder strategische of gevoelige gegevens worden verwerkt, de systemen waarvan de bedrijfsvoering direct afhankelijk is (mission critical systems) en de systemen die mogelijk schade aan de belangen van derden kunnen veroorzaken (safety critical systems, privacy critical systems). In dit soort gevallen zijn aanvullende maatregelen mogelijk en noodzakelijk.

Met het gebruik van de Code kan het algehele beveiligingsniveau verbeteren; in Nederland maar ook daarbuiten: de Code is een internationale standaard. Ook het MKB zal hier voordeel bij hebben. Tevens kan de Code gebruikt worden tussen zakenpartners, zodat op een verantwoorde manier gebruik kan worden gemaakt van de nieuwe technologische mogelijkheden in de industrie. Dat is goed voor het Nederlandse bedrijfsleven.

Meer weten

De Code voor Informatiebeveiliging is te bestellen bij het Nederlands Normalisatie-instituut in Delft (015 - 2690390). Tevens is er een gratis helpdesk voor het gebruik van de Code ingericht door de Raad voor de Informatietechnologie in Den Haag (070 - 3819444).

De Code voor Informatiebeveiliging als norm voor de EDP-auditor

W.S.C. Krol RE en
drs. M.M. Smits

De Code voor Informatiebeveiliging biedt een leidraad aan managers en werknemers voor het opzetten, implementeren en onderhouden van informatiebeveiliging. De Code is tot stand gekomen op grond van praktijkervaring van gerenommeerde bedrijven. Aan de hand van drie criteria wordt in dit artikel beoordeeld of de Code kan dienen als norm voor de EDP-auditor bij het uitvoeren van EDP-audits. Tot slot geven de auteurs aanbevelingen omtrent de bruikbaarheid van de Code als norm voor de EDP-auditor.

INLEIDING

In het najaar van 1994 is de Code voor Informatiebeveiliging geïntroduceerd in Nederland. De Code heeft als ondertitel 'Een leidraad voor beleid en implementatie' en richt zich op managers en werknemers die verantwoordelijk zijn voor het opzetten, implementeren en onderhouden van informatiebeveiliging in hun organisatie. Hij is gebaseerd op praktijkervaring van een aantal toonaangevende internationale bedrijven. De Code heeft tot doel het verschaffen van een gemeenschappelijke basis voor informatiebeveiliging en het bevorderen van het vertrouwen in het handelsverkeer tussen bedrijven. Thans heeft de Code de status van richtlijn. Verheffing van de Code tot (ISO-)norm zal mede worden bepaald door het draagvlak.
Tot op heden ontbeert het vakgebied EDP-auditing normen en standaarden die gehanteerd kunnen worden bij het uitvoeren van EDP-audits. In dit artikel wordt beoordeeld of de Code door de EDP-auditor gehanteerd kan worden en daarmee de gesignaleerde leemte kan opvullen.
Beoordeling van de Code gebeurt aan de hand van een drietal criteria. Allereerst wordt nagegaan of de Code het gehele gebied van informatiebeveiliging bestrijkt. Vervolgens wordt vastgesteld of de Code in voldoende mate rekening houdt met de door organisaties geformuleerde beveiligingsdoelstellingen. Ten slotte wordt beoordeeld of de formulering van de Code een eenduidige interpretatie waarborgt. Op grond van de conclusies omtrent de bruikbaarheid van de Code als norm voor de EDP-auditor wordt een aantal aanbevelingen gedaan.

DEKKING VAN HET GEBIED VAN INFORMATIEBEVEILIGING

De waarde van de Code als norm bij de beoordeling van de informatiebeveiliging van een organisatie wordt mede bepaald door de mate waarin de Code het gebied van informatiebeveiliging bestrijkt. Indien belangrijke beveiligingsitems ontbreken of onderbelicht worden, kan dit leiden tot een onjuist of onvolledig oordeel omtrent het niveau van beveiliging van een organisatie. De grenzen van het begrip informatiebeveiliging zijn niet eenduidig vast te stellen. Het gebied van informatiebeveiliging kan vanuit verschillende invalshoeken worden benaderd. Elke invalshoek kent een nadere onderverdeling. Figuur 1 geeft een overzicht van mogelijke invalshoeken en de daaraan gekoppelde onderverdeling.

Alle in de figuur genoemde aspecten worden door de Code in beschouwing genomen. In tabel 1, die aan het eind van dit artikel is opgenomen, wordt dit aan de hand van voorbeelden aangetoond. Er kan gesteld worden dat de Code het gehele gebied van informatiebeveiliging afdekt, overigens met inachtneming van de volgende kanttekeningen:

- Er is niet systematisch onderzocht of alle aspecten in de Code volledig zijn uitgewerkt. De Code geeft overigens zelf al aan dat het afhankelijk van de omstandigheden nodig kan zijn meer (striktere) maatregelen te treffen, die niet in de Code zijn opgenomen.

- Bij een globale beoordeling van de volledigheid van de Code blijken de volgende maatregelen te ontbreken, zonder dat daarvoor goede alternatieven worden genoemd:
  - verzekeringen;
  - softwaredeponerings-overeenkomsten (escrow);
  - voorkoming van het ontstaan van kritieke functies en maatregelen om de vervanging van functionarissen op een kritische positie te waarborgen;
  - goede naamgevingsconventies voor bestanden en programmatuur.

- De diepgang waarmee de verschillende aspecten worden behandeld, varieert van zeer globaal tot zeer gedetailleerd. Maatregelen met betrekking tot computer- en netwerkbeheer (hoofdstuk 6 en 7) worden bijvoorbeeld globaal beschreven. Daarentegen worden maatregelen met betrekking tot logische toegangsbeveiliging gedetailleerd uitgewerkt.

Figuur 1. Verschillende invalshoeken van informatiebeveiliging.

Invalshoek	Onderverdeling
Beveiligingsdoelstellingen	integriteit, vertrouwelijkheid, beschikbaarheid
Objecten	computer-, netwerk- en randapparatuur, programmatuur, gegevens, mensen, procedures, documentatie
Processen	ontwikkeling, installatie en onderhoud, beheer en gebruik, buitengebruikstelling en verwijdering
Aard van de organisatie	gebruikers-, verwerkers-, netwerk- en systeem-ontwikkelingsorganisatie
Soorten bedreigingen	onopzettelijk: menselijk falen, technisch falen en natuurrampen opzettelijk: kwade wil
Aard van de maatregelen	organisatorisch (incl. procedureel), fysiek, logisch (geprogrammeerd) en juridisch (contractueel)
Managementniveaus	strategisch, tactisch en operationeel
Fasen van de managementcyclus	beleidsbepaling, implementatie, uitvoering en evaluatie

RELATIE MAATREGELEN MET BEVEILIGINGSDOELSTELLINGEN

Het treffen van beveiligingsmaatregelen is doorgaans geen doel op zichzelf. Maatregelen worden getroffen om beveiligingsdoelstellingen te realiseren. Integriteit, vertrouwelijkheid en beschikbaarheid worden algemeen beschouwd als hoofddoelstellingen van informatiebeveiliging. De hoofddoelstellingen kunnen nader worden geconcretiseerd in de vorm van subdoelstellingen. De te realiseren beveiligingsdoelstellingen zijn doorgaans afgeleid van het beleid van de organisatie alsmede de van toepassing zijnde wettelijke en contractuele verplichtingen. Daarmee zijn beveiligingsdoelstellingen en dus ook de te treffen maatregelen om deze doelstellingen te realiseren niet voor alle organisaties gelijk. Beveiligingsmaatregelen dienen daarom gerelateerd te worden aan beveiligingsdoelstellingen. Het loskoppelen van maatregelen en doelstellingen kan eenvoudig leiden tot een te laag (ondoeltreffend) of een te hoog (ondoelmatig) beveiligingsniveau.

In de Code wordt een groep maatregelen voorafgegaan door een korte toelichting op de doelstelling en de reikwijdte van de bijbehorende maatregelen. De doelstellingen in de Code refereren in de meeste gevallen (soms impliciet) aan de beveiligingsdoelstellingen integriteit, vertrouwelijkheid en beschikbaarheid. Deze drie hoofddoelstellingen en een daarvan afgeleid stelsel van subdoelstellingen zijn echter niet als uitgangspunt genomen voor de structuur van de Code. De structuur van de Code is gebaseerd op tien categorieën van maatregelen die algemeen worden gebruikt bij bedrijven die betrokken zijn geweest bij het opstellen van de Code. Er wordt in alle hoofdstukken van de Code gerefereerd aan de drie hoofddoelstellingen van beveiliging. Ten aanzien van de hoofddoelstellingen overlappen de hoofdstukken in de Code elkaar. Dit leidt ertoe dat ten behoeve van een hoofddoelstelling van beveiliging (of een daarvan afgeleide doelstelling) op meerdere plaatsen in de Code maatregelen zijn opgenomen (zie voorbeeld 1). De Code geeft geen handreiking voor het samenvoegen van maatregelen die, vanuit de invalshoek

'hoofddoelstelling van beveiliging' gezien, logisch bij elkaar horen.
Bovendien is als gevolg van de gekozen structuur in de Code niet zonder meer vast te stellen of de doelstellingen en de daarvan afgeleide maatregelen een sluitend geheel vormen.

5.1 Beveiligde ruimten

DOELSTELLING: Het voorkomen van onbevoegde toegang tot, schade aan of hinderlijke storing van IT-diensten.

6.4 Huisregels

DOELSTELLING: Het handhaven van de integriteit en de beschikbaarheid van IT-diensten.

De twee doelstellingen hebben beide betrekking op de beveiligingsdoelstellingen integriteit en beschikbaarheid van IT-diensten. Als een gebruiker van de Code geïnteresseerd is in bijvoorbeeld maatregelen met betrekking tot de beschikbaarheid van IT-diensten, is er voor hem geen ingang waaruit blijkt dat hij zowel in 5.1 als in 6.4 (en wellicht elders) maatregelen aantreft.

Voorbeeld 1. De structuur van de Code.

Op grond van het voorgaande kan gesteld worden dat de Code een checklist van maatregelen vormt, zonder expliciete verwijzing naar beveiligingsdoelstellingen. Dit heeft een aantal consequenties bij hantering van de Code als norm bij de beoordeling van de informatiebeveiliging:

– Beveiligingsdoelstellingen zijn situationeel bepaald. Zo zijn de hoofddoelstellingen van beveiliging en daarvan afgeleide subdoelstellingen niet voor iedere organisatie even belangrijk. In een technisch georiënteerde omgeving kan de nadruk bijvoorbeeld liggen op beschikbaarheid, terwijl in een administratieve omgeving de nadruk kan liggen op integriteit. Bij hantering van de Code als norm komen dergelijke verschillen onvoldoende tot uitdrukking.

– Doordat maatregelen in de Code niet geordend zijn naar beveiligingsdoelstellingen, is niet zonder meer vast te stellen wat de consequentie is van het ontbreken van maatregelen. Als een aantal maatregelen gericht op een gelijkluidende doelstelling ontbreekt, is het cumulatief effect hiervan niet direct zichtbaar.

– Veel organisaties hebben inmiddels beveiligingsmaatregelen getroffen. Dit hoeven niet noodzakelijkerwijs maatregelen te zijn die in de Code zijn opgenomen. Door het ontbreken van de koppeling van maatregelen aan doelstellingen, blijkt niet zonder meer dat bepaalde maatregelen uit de Code kunnen vervallen omdat inmiddels alternatieven zijn getroffen.

EENDUIDIGHEID VAN DE CODE

Om de Code als norm te kunnen hanteren dient gewaarborgd te zijn dat de Code op de juiste wijze wordt geïnterpreteerd. De Code bevat een groot aantal generieke maatregelen waaraan in een specifieke situatie veelal nader invulling gegeven dient te worden. Op een aantal punten zou de Code daarbij onjuist kunnen worden geïnterpreteerd, hetgeen achtereenvolgens betrekking kan hebben op:
a. de gehanteerde terminologie;
b. de wijze waarop uitwerking van maatregelen in een specifieke situatie dient plaats te vinden;
c. de inschatting van het belang om maatregelen in een specifieke situatie al dan niet te treffen.

Ad a. Terminologie

In de Code wordt een groot aantal termen gehanteerd die (in ieder geval in EDP-auditland) niet al te gangbaar zijn (zie voorbeeld 2). Wellicht vloeit dit voort uit de vertaling uit het Engels. De betekenis is niet altijd direct duidelijk. Soms moet uit de context worden opgemaakt wat wordt bedoeld. Een verklarende woordenlijst ontbreekt. Aangezien een eenduidige terminologie in het vakgebied van informatiebeveiliging en auditing van wezenlijk belang is, kan dit aangemerkt worden als een belangrijke tekortkoming.

8.3.1 Het bijwerken van operationele programmabibliotheken dient uitsluitend te worden uitgevoerd door de aangewezen bibliotheekbeheerder na autorisatie van de IT-ondersteuningsmanager van de betreffende toepassing.

Niet duidelijk is wat moet worden verstaan onder een IT-ondersteuningsmanager. Elders in de Code wordt duidelijk dat hiermee de applicatiebeheerder wordt bedoeld.

8.4 Beveiliging van ontwikkel- en ondersteunende afdelingen.

Niet duidelijk is wat bedoeld wordt met ondersteunende afdelingen.

Tevens worden termen gebruikt als IT-bedrijfsmiddelen (3.1.1), informatiebedrijfsmiddelen (3.2), IT-voorzieningen (5.1), IT-systemen (3.2.2), IT-apparatuur (5.2.1), computersystemen (6.2.2), systemen (6.2.2). Niet steeds is direct duidelijk of het gaat om apparatuur, programmatuur, media, een samenstel van apparatuur en programmatuur, etc.

Voorbeeld 2. Het gebruiken van terminologie in de Code.

Ook de term maatregel wordt in de Code niet consistent gebruikt. Veelal geeft de Code eerst aan dat er iets moet gebeuren (de eis), vaak gevolgd door hoe dit dient te gebeuren (de maatregel). In beide gevallen spreekt de Code over maatregelen. Het onzorgvuldig gebruik van de term maatregel is verwarrend.

Ad b. Wijze waarop maatregelen uitgewerkt dienen te worden

De diepgang waarmee maatregelen in de Code zijn beschreven, varieert van zeer globaal tot redelijk gedetailleerd. De mate van detail verschilt per hoofdstuk, maar ook binnen de hoofdstukken zijn er variaties (zie voorbeeld 3). De Code stelt zelf overigens al dat in de praktijk nadere invulling gegeven zal moeten worden aan maatregelen. De invulling is mede afhankelijk van factoren zoals de soort omgeving en de techniek. De auditor zal zelf moeten bepalen op welke wijze dit zal moeten geschieden.

Verschillen tussen hoofdstukken:
Hoofdstuk 1, 6 en 9: vrij globaal uitgewerkt.
Hoofdstuk 4 en 7: bevatten zeer concrete maatregelen.

Verschillen binnen hoofdstukken:
6.1.1 Schriftelijke bedieningsprocedures

Bevat slechts globaal aanwijzingen voor de op te stellen procedures en nauwelijks aanwijzingen voor de inhoud van de procedures.

6.1.2 Procedures voor het behandelen van incidenten

Geeft gedetailleerd aan waarvoor procedures opgesteld dienen te worden en wat in de procedures geregeld dient te worden.

Voorbeeld 3. De detaillering van maatregelen in de Code.

Tevens gebruikt de Code geregeld woorden als 'etcetera'. Ook op deze punten geeft de Code aan dat nadere invulling in de praktijk mogelijk is (zie voorbeeld 4).

Ad c. Inschatting van het belang van de maatregelen

Niet alle maatregelen zijn in alle situaties van toepassing. In de Code wordt dan ook veelvuldig gebruik gemaakt van zinsneden als 'Het wordt aangeraden om ...', 'Overweeg of ...', 'Indien noodzakelijk ...'. Soms beveelt de Code aan de afweging te maken op basis van risico-analyse. In andere gevallen worden geen criteria aangereikt op basis waarvan de afweging gemaakt dient te worden. De auditor zal hieraan zelf een interpretatie moeten geven.

6.1.1 Schriftelijke bedieningsprocedures

Er dienen ook gedocumenteerde procedures te worden opgesteld voor huishoudelijke activiteiten met betrekking tot computer- en netwerkbeheer, zoals opstart- en afsluitprocedures, reservekopieën, onderhoud van apparatuur, beheer en beveiliging van computerruimten, etc.

Het betreft hier de dagelijkse gang van zaken in een rekencentrum. Interpretatieverschillen op dit punt kunnen derhalve grote consequenties hebben.

Voorbeeld 4. De beschrijving van maatregelen in de Code.

De Code blijft vaag omtrent het verplichtend karakter van de maatregelen (zie voorbeeld 5). Gesteld wordt dat maatregelen alleen getroffen dienen te worden als de `plaatselijke omstandigheden' dit rechtvaardigen. Vervolgens lijkt ten aanzien van de maatregelen een driedeling te worden aangebracht:
- 'aanbevolen als richtsnoer in alle situaties';
- 'te bepalen op basis van een risico-analyse';
- 'te bepalen op basis van gespecialiseerde beveiligingsadviezen'.

De tien maatregelen die worden aangemerkt als essentieel en fundamenteel zijn limitatief opgesomd. Van deze tien maatregelen wordt gesteld dat deze van toepassing zijn op elke organisatie en omgeving. In hoeverre 'essentieel en fundamenteel' als verplicht moet worden aangemerkt, wordt niet duidelijk. In de oorspronkelijke (Engelse) versie van de Code wordt essentieel overigens aangeduid als 'mandatory requirements', waaruit een dwingender karakter spreekt.

Het onderscheid tussen de 'aanbevolen' en 'nader te bepalen' maatregelen is niet strikt aangegeven in de Code. De EDP-auditor zal dit onderscheid uit de tekst bij de maatregelen moeten opmaken. Tevens zal de EDP-auditor zelf moeten vaststellen of de 'aanbevolen' en de 'nader te bepalen' maatregelen in een specifieke situatie getroffen dienen te worden.

6.1.4 Het is wenselijk de voorzieningen voor produktie en ontwikkeling te scheiden ...
5.2.2 Er zou nagedacht dienen te worden over de noodzaak van een reserve-voedingseenheid.

Kader 5. Inschatting van het belang van maatregelen.

Samenvattend kan gesteld worden dat de Code op veel punten niet eenduidig is. In een specifieke situatie is aanvullende informatie en vakkennis nodig om inzicht te verkrijgen in de wijze waarop de maatregelen in de Code moeten worden geïnterpreteerd en uitgewerkt.

CONCLUSIES

De Code is in de eerste plaats een leidraad voor het opzetten van informatiebeveiliging in organisaties. Hij beoogt vooralsnog geen norm te zijn. Mede vanuit de behoefte van de EDP-auditors aan normen en standaarden voor het uitvoeren van EDP-audits is in het voorgaande kritisch beschouwd of de Code desalniettemin gehanteerd kan worden als toetsingsnorm voor de EDP-auditor. Op grond van deze kritische beschouwing kan geconcludeerd worden dat de Code in zijn huidige vorm niet geschikt is als toetsingsnorm voor de EDP-auditor.

In de eerste plaats laat de eenduidigheid van de Code veel te wensen over. Gebleken is dat veel maatregelen in de Code nader uitgewerkt moeten worden. De Code geeft niet aan hoe de uitwerking dient te geschieden. Er ontbreken richtlijnen om vast te kunnen stellen welke maatregelen in een specifieke omgeving van toepassing zijn. Tevens geeft de Code geen uitsluitsel omtrent het al dan niet verplicht zijn van maatregelen. Een begrippenlijst ten behoeve van een eenduidige uitleg van de gehanteerde terminologie is niet aanwezig. Als toetsingsnorm laat de Code de auditor veel ruimte voor interpretatie. De auditor zal op grond van zijn eigen vaktechnische kennis en ervaring een (subjectieve) inschatting moeten maken om vast te stellen of aan de Code is voldaan.
Ten tweede is geconstateerd dat de structuur van de Code gebaseerd is op de aard van de maatregelen. De Code biedt vervolgens onvoldoende aanknopingspunten om maatregelen (terug) te vertalen naar beveiligingsdoelstellingen. Indien toetsing plaatsvindt aan de Code kan derhalve slechts worden vastgesteld of een aantal maatregelen al dan niet is getroffen. Een uitspraak over het beveiligingsniveau, de mate waarin de beveiligingsdoelstellingen worden gerealiseerd, is niet zonder meer mogelijk.
Geconstateerd is ten slotte dat de Code het gebied van informatiebeveiliging in ruime mate bestrijkt. Hieruit mag weliswaar voorzichtig worden afgeleid dat indien alle maatregelen uit de Code zijn getroffen (en afgezien wordt van problemen met betrekking tot de interpretatie), sprake zal zijn van een redelijk hoog niveau van beveiliging. Het zonder meer treffen van alle maatregelen zal echter in veel situaties ondoelmatig blijken.

AANBEVELINGEN

In de vorige paragraaf is geconcludeerd dat de Code in zijn huidige vorm tekort schiet als norm voor de EDP-auditor. Desondanks dient de Code vooralsnog niet terzijde geschoven te worden. Uniek aan de Code is dat hij op basis van jarenlange praktijkervaring van gerenommeerde organisaties tot stand is gekomen. Vanwege zijn herkomst en de ondersteuning die hij thans geniet maakt de Code derhalve goede kans door bedrijfsleven en wellicht overheid algemeen geaccepteerd te worden als uitgangspunt voor informatiebeveiliging, temeer daar de introductie van de Code samenvalt met de groeiende vraag vanuit de samenleving om concreet invulling te geven aan een toenemend aantal (wettelijke) voorschriften (Wet persoonsregistraties, Wet computercriminaliteit, Voorschrift Informatiebeveiliging Rijksdienst, diverse Europese richtlijnen). Om als beroepsgroep aansluiting te houden bij de maatschappelijke ontwikkelingen dient de afwachtende houding plaats te maken voor een actief optreden waarin getracht wordt de geconstateerde tekortkomingen te ondervangen. Hierna wordt een aantal suggesties gegeven om hieraan concreet invulling te geven:

- De maatregelen in de Code laten veel ruimte voor interpretatie. Voor zover dit voortvloeit uit onzorgvuldig gehanteerde terminologie kan een duidelijk afgebakend begrippenkader helpen interpretatieverschillen te voorkomen.

- De ruimte voor interpretatie betreft tevens de wijze waarop in specifieke situaties nadere invulling aan de Code gegeven dient te worden. De invulling houdt mede verband met de soort omgeving. Interpretatierichtlijnen per soort omgeving kunnen bijdragen aan een eenduidiger uitleg van de Code. Bij de soorten omgevingen kan gedacht worden aan: IBM Mainframe, AS400, UNIX, DEC/VAX, PC Lan, systeemontwikkelingsorganisatie, etc.

- De te realiseren beveiligingsdoelstellingen vormen het uitgangspunt voor de beoordeling van de beveiliging van organisaties. De introductie van de Code geeft de EDP-auditor geen aanleiding om hiervan af te wijken. In de Code worden slechts de maatregelen beschreven om aan deze doelstellingen te voldoen. De maatregelen in de Code dienen derhalve gerelateerd te worden aan beveiligingsdoelstellingen. Als eerste aanzet hiertoe is aan het eind van dit artikel een raamwerk van beveiligingsdoelstellingen opgezet (tabellen 2 en 3). Per doelstelling wordt verwezen naar maatregelen in de Code die hieraan bijdragen.

- De structuur en daarmee de ingang van de Code is gebaseerd op de aard van de maatregelen. In een specifieke situatie zijn meestal niet alle maatregelen relevant. Een eenduidige interpretatie van de Code zal toenemen wanneer de Code een ingang heeft vanuit meerdere invalshoeken (zie figuur 1). Aan de hand van deze ingangen kan sneller inzicht worden verkregen welke maatregelen in een bepaalde situatie relevant zijn. Een geautomatiseerd hulpmiddel kan daarbij behulpzaam zijn.
Inmiddels is een aantal geautomatiseerde van de Code afgeleide vragenlijsten op de markt verkrijgbaar. Deze vragenlijsten blijken op dezelfde wijze te zijn ingedeeld als de Code. In dit opzicht voegen deze tools derhalve geen nieuwe invalshoeken toe.

- Hoewel de Code een groot deel van het gebied van informatiebeveiliging bestrijkt, is hij niet volledig. Een onderzoek naar ontbrekende maatregelen en het opnemen van deze maatregelen in een addendum kan op dit punt verbetering brengen. Het onderzoek zou kunnen plaatsvinden door een vergelijking van de maatregelen in de Code met bestaande beveiligingsstelsels.

W.S.C. Krol RE
Is werkzaam als intern EDP-auditor bij de Informatie Beheer Groep. Zijn aandacht richt zich op het adviseren over en het beoordelen van de kwaliteit van de geautomatiseerde informatievoorziening. Een belangrijke rol daarbij spelen vraagstukken over effectiviteit en efficiency van de inzet van informatietechnologie. Daarnaast houdt hij zich bezig met het ontwikkelen en bewaken van het auditbeleid, met name op het terrein van beveiliging.

Drs. M.M. Smits
Studeerde bestuurlijke informatiekunde aan de Katholieke Universiteit Brabant. Sinds 1992 is hij werkzaam bij de NV Nederlandse Spoorwegen, thans als adviseur Administratieve Organisatie bij NS Reizigers met als aandachtsgebied kwaliteitsbeheersing van de geautomatiseerde informatievoorziening.

Invalshoek	Onderverdeling	Voorbeelden uit de Code
Beveiligings-doelstellingen	integriteit vertrouwelijkheid beschikbaarheid	De drie hoofddoelstellingen worden in de Code op pagina 4 aangeduid als de drie `basisprincipes waarop informatie-beveiliging is gebaseerd'
Objecten	computer-, netwerk- en randapparatuur programmatuur gegevens/media mensen procedures en documentatie	5.2 `beveiliging van apparatuur', inclusief 5.2.3 'beveiliging van kabels' 8.2 'beveiliging van toepassingssystemen', 8.4.2 'technische controle op besturingssysteem' 6.6 'behandeling en beveiliging van computermedia' 4.2 'training voor gebruikers' 6.6.3 'beveiliging van systeemdocumentatie'
Processen	ontwikkeling installatie en onderhoud beheer en gebruik buitengebruikstelling en verwijdering	8 'ontwikkeling en onderhoud van systemen' en 5.2.4 'onderhoud van apparatuur' 6.2 'systeemplanning en acceptatie' 6.1 'bedieningsprocedures en verantwoordelijkheden' en 6.5 'netwerkbeheer' 5.2.6 'veilig afvoeren van apparatuur' en 6.6.4 'afvoer van media'
Aard van de organisatie	gebruikersorganisatie verwerkings- en netwerkorganisatie systeemontwikkelingsorganisatie	7.3 'verantwoordelijkheden van gebruikers' 6 'computer- en netwerkbeheer' 8.4 'beveiliging van ontwikkel- en ondersteunende afdelingen'
Soorten bedreigingen	onopzettelijk menselijk falen kwade wil technisch falen natuurrampen	4.2.1 'opleiding en training voor informatiebeveiliging' 6.3 'bescherming tegen kwaadaardige programmatuur' 5.2.2 'stroomvoorziening' 9.1 'continuïteitsplanning'
Aard van de maatregelen	organisatorisch (incl. procedureel) fysiek logisch (geprogrammeerd) juridisch (contractueel)	2 'beveiligingsorganisatie' 5 'fysieke beveiliging en beveiliging van de omgeving' 7 'toegangsbeveiliging voor systemen' 2.2.2 'beveiligingsvoorwaarden in contracten met derden
Management-niveaus	strategisch tactisch operationeel	2.1.1 'stuurgroep voor informatiebeveiliging' 2.1.3 'toewijzing van verantwoordelijkheden voor 'informatiebeveiliging' 6.1 'bedieningsprocedures en verantwoordelijkheden'
Fasen van de management-cyclus	beleidsbepaling implementatie uitvoering evaluatie	1 'beveiligingsbeleid' 2.1.3 'toewijzing van verantwoordelijkheden voor informatiebeveiliging' 6 'computer- en netwerkbeheer' 10.2 'beveiligingscontrole op IT-systemen'

Tabel 1. Invalshoeken van informatiebeveiliging.

Opzet van het doelstellingenraamwerk

In het doelstellingenraamwerk worden maatregelen van de Code gerelateerd aan beveiligingsdoelstellingen. Het doelstellingenraamwerk is tot stand gekomen door inventarisatie en ordening van beveiligingsdoelstellingen. Vervolgens zijn de maatregelen uit de Code toegedeeld aan de geïnventariseerde doelstellingen.

Inventarisatie van doelstellingen

Ten behoeve van de inventarisatie en ordening van doelstellingen is een aantal categorieën van doelstellingen afgeleid van de drie hoofddoelstellingen van beveiliging (beschikbaarheid, integriteit en vertrouwelijkheid). Per categorie is vervolgens een set van subdoelstellingen gedefinieerd. De volgende categorieën zijn onderkend:

– *Algemeen organisatorische condities*
De effectiviteit van de te treffen maatregelen hangt af van de mate waarin het stelsel van maatregelen een sluitend geheel vormt, afgestemd op de beveiligingseisen van de organisatie en haar omgeving. Daarnaast hangt de effectiviteit af van de mate waarin de in opzet getroffen maatregelen worden nageleefd. Om te bereiken dat de te treffen maatregelen effect sorteren dient daarom aan een aantal organisatorische vereisten te worden voldaan.

– *Beschikbaarheid van de IT-middelen*
De beschikbaarheid van de informatievoorziening wordt bepaald door de fysieke beschikbaarheid van de IT-middelen en het technisch naar behoren functioneren van deze middelen.

– *Integriteit van het verwerkingsproces*
De integriteit van het verwerkingsproces wordt bepaald door oordeelkundig gebruik van apparatuur, integere programmatuur en integere gegevens door daartoe opgeleide en bevoegde functionarissen.

– *Integriteit van gegevens*
De integriteit van de gegevens wordt bepaald door de mate van zorgvuldigheid in de omgang met en het gebruik van gegevensverzamelingen. De gegevens mogen slechts bewerkt worden door integere programmatuur.

– *Integriteit van programmatuur*
De integriteit van programmatuur wordt bepaald door een duidelijke definitie van de daaraan te stellen eisen alsmede het organisatorische traject van aanschaf, ontwikkeling, onderhoud en ingebruikneming.

– *Vertrouwelijkheid van gegevens*
De vertrouwelijkheid van gegevens wordt bepaald door de wijze waarop gegevens ter inzage komen aan de daarvoor geautoriseerde functionarissen en de procedures met betrekking tot opslag, bewerking, transport en vernietiging.

Toedeling van maatregelen uit de Code aan de doelstellingen

De maatregelen in de Code dragen bij aan het waarborgen van beveiligingsdoelstellingen. De Code maakt dit niet altijd expliciet. De doelstellingen waarop de maatregelen in de Code zijn gericht, zijn zoveel mogelijk expliciet gemaakt waarna de maatregelen zijn opgehangen aan de geïnventariseerde doelstellingen.

Opmerkingen bij het raamwerk

Bij het doelstellingenraamwerk kan een aantal opmerkingen worden geplaatst:

– De onderkende categorieën vertonen onderling afhankelijkheden. Zo zijn de integriteit en de vertrouwelijkheid van de gegevens bijvoorbeeld afhankelijk van de integriteit van het verwerkingsproces en de programmatuur. Dergelijke afhankelijkheden zijn slechts te voorkomen door alle subdoelstellingen die tot de laatstgenoemde categorieën behoren, op te nemen onder de categorieën integriteit en vertrouwelijkheid van gegevens. Wij zijn van mening dat dit de doorzichtigheid van het raamwerk niet ten goede komt.

– De relatie tussen de categorieën en de drie hoofddoelstellingen van beveiliging kan globaal als volgt worden weergegeven:

Categorie van doelstellingen	Integriteit	Vertrouwelijkheid	Beschikbaarheid
Algemeen organisatorische condities	×	×	×
Beschikbaarheid van de IT-middelen			×
Integriteit van het verwerkingsproces	×	×	×
Integriteit van gegevens	×		
Integriteit van programmatuur	×	×	
Vertrouwelijkheid van gegevens		×	

– Bij het opstellen van het raamwerk zijn keuzen gemaakt die enigszins arbitrair zijn. Verdere discussie omtrent de indeling, alsmede praktisch gebruik hiervan zal wellicht leiden tot een raamwerk waarover algemene consensus zal bestaan.

– De maatregelen zijn toegedeeld op het niveau van subparagraaf in de Code (x.x.x). Een nadere verfijning is mogelijk, aangezien de Code binnen een subparagraaf meerdere maatregelen onderscheidt.

Tabel 2. Doelstellingenraamwerk.

Tabel 3. Raamwerk beveiligings-doelstellingen.

Beveiligingsdoelstellingen	**Maatregelen in de Code**		
Algemeen organisatorische condities			
Het topmanagement dient te demonstreren dat informatiebeveiliging voor hem een serieuze zaak vormt.	1.1.1	2.1.1	2.1.2
Hiertoe dient het topmanagement uitgangspunten voor informatiebeveiliging vast te stellen.	1.1.1		
Het stelsel van informatiebeveiliging, gebaseerd op de door het management vastgestelde uitgangspunten, dient een samenhangend geheel te vormen.	1.1.1	2.1.1	2.1.2
Bij het vaststellen van de uitgangspunten dient rekening te worden gehouden met risico's en wettelijke en contractuele verplichtingen.	10.1.1 10.1.4	10.1.2	10.1.3
De organisatie dient hiertoe te beschikken over actuele kennis van beveiligingsrisico's, wetgeving, contractuele verplichtingen en te treffen beveiligingsmaatregelen.	2.1.5	2.1.6	
De vastgestelde uitgangspunten dienen in de vorm van een beleidsdocument kenbaar gemaakt te worden aan voor de beveiliging verantwoordelijke functionarissen.	1.1.1	2.1.1	2.1.2
Verantwoordelijkheden voor het definiëren, implementeren, uitvoeren en toetsen van de beveiliging dienen expliciet te zijn vastgesteld.	2.1.1	2.1.3	
Ter voorkoming van kwaadwil en onachtzaamheid dienen bij de toedeling van taken en verantwoordelijkheden tegengestelde belangen gecreëerd te worden.	6.1.3	6.1.4	6.5.1
De te beveiligen IT-middelen dienen bekend te zijn.	3.1.1		
Er dienen naamgevingsconventies gehanteerd te worden voor de registratie van IT-middelen.	geen maatregelen aangetroffen		
Aan ieder IT-middel dient een eigenaar toegewezen te zijn, die verantwoordelijk is voor de beveiliging.	2.1.3	3.1.1	
Verantwoordelijkheid voor de beveiliging van apparatuur op afstand dient vastgesteld te worden.	6.5.1		
Per IT-middel dient het beveiligingsniveau vastgesteld en kenbaar gemaakt te worden.	3.2.1	3.2.2	
Bij aanneming dient gelet te worden op de integriteit van functionarissen.	4.1.2		
Functionarissen dienen vertrouwd te zijn met de voor hen van toepassing zijnde beveiligingstaken en verantwoordelijkheden.	4.1.1	4.1.3	4.2.1
Functionarissen dienen gestimuleerd te worden beveiligingsmaatregelen na te leven.	4.1.1 4.3.4	4.1.3	4.2.1
Bij verlening van toegang aan derden tot de eigen voorzieningen dienen de door beide partijen in acht te nemen beveiligingsvoorwaarden contractueel te worden vastgelegd.	2.2.1	2.2.2	
Bij gebruik van voorzieningen van derden dienen de door beide partijen in acht te nemen beveiligingsvoorwaarden contractueel te worden vastgelegd.	2.2.2	6.1.5	
Bij uitwisseling van gegevens met derden dienen de beveiligingsvoorwaarden contractueel te worden vastgelegd.	6.7.1	6.7.3	
Beveiligingsincidenten (incl. storingen) dienen gerapporteerd te worden teneinde de schade te beperken en er lering uit te trekken.	4.3.1	4.3.3	
Er dienen procedures aanwezig te zijn voor de afhandeling van beveiligingsincidenten.	4.3.1	4.3.4	
Zwakke plekken in de beveiliging dienen te worden gerapporteerd teneinde schade te beperken en er lering uit te trekken.	4.3.2		
Periodiek dient vastgesteld te worden dat het beveiligingsbeleid daadwerkelijk is geïmplementeerd en dat het beoogde effect is bereikt.	2.1.7	10.2.1	10.2.2

Beveiligingsdoelstellingen	Maatregelen in de Code
Beschikbaarheid van de IT-middelen	
IT-middelen dienen opgesteld te zijn in een omgeving die beschermd is tegen calamiteiten.	5.1.1 5.1.3 5.2.1
De toegang tot IT-middelen dient beperkt te zijn tot geautoriseerde personen.	5.1.1 5.1.2 5.1.3 5.1.4 5.2.1
De continuïteit van de energievoorziening dient gewaarborgd te zijn.	5.2.2
Kabels dienen beschermd te worden tegen beschadiging en interferentie.	5.2.3
Er dient zorg gedragen te worden voor de juiste klimatologische omstandigheden.	6.4.4
Ter voorkoming van storingen dient zorg gedragen te worden voor voldoende verwerkingscapaciteit.	6.2.1
Alle wijzigingen in IT-middelen dienen te worden geautoriseerd en technisch te worden goedgekeurd.	2.1.4 6.2.2 6.2.4
IT-middelen dienen volgens de daarvoor geldende voorschriften te worden onderhouden.	5.2.4
IT-middelen mogen het bedrijf niet zonder toestemming verlaten.	5.1.6
De beveiliging dient zich ook uit te strekken tot IT-middelen die zich (tijdens transport) buiten het bedrijf bevinden.	5.2.5 6.7.2
Er dient zorg gedragen te worden voor de aanwezigheid van kopieën van gegevens en programmatuur.	6.4.1
Ten behoeve van kennisoverdracht dienen procedures schriftelijk vastgelegd te zijn.	6.1.1
Vervanging van functionarissen op een kritieke positie dient geregeld te zijn.	geen maatregelen aangetroffen
De onderhoudbaarheid van door derden geleverde programmatuur dient gewaarborgd te zijn.	geen maatregelen aangetroffen
De organisatie dient verzekerd te zijn tegen schade voortvloeiend uit calamiteiten.	geen maatregelen aangetroffen
Er dient zorg gedragen te worden voor uitwijkvoorzieningen, zodat kritieke bedrijfsprocessen ook na het optreden van storingen en calamiteiten doorgang kunnen vinden.	6.2.3 9.1.1 9.1.2 9.1.3 9.1.4
De toereikendheid van uitwijkvoorzieningen dient periodiek vastgesteld te worden.	6.2.3 9.1.1 9.1.2 9.1.3 9.1.4
Integriteit van het verwerkingsproces	
Het gebruik van IT-middelen dient beperkt te zijn tot daartoe geautoriseerde personen.	7.1 t/m 7.7
IT-middelen dienen gebruikt te worden volgens daarvoor geldende bedieningsprocedures.	6.1.1 6.5.1
Functionarissen dienen vertrouwd te zijn met het gebruik van IT-middelen.	4.2.1 6.2.2
Verwerking dient plaats te vinden met geautoriseerde versies van programmatuur.	6.1.4 8.3.1
Incidenten dienen tijdig en effectief afgehandeld te worden.	6.1.1 6.1.2
Aanwezigheid van kwaadaardige programmatuur dient voorkomen te worden en in voorkomende gevallen tijdig gesignaleerd te worden.	6.3.1
Achteraf dient vastgesteld te kunnen worden welke (kritieke) handelingen zijn verricht.	6.4.2
Achteraf dient vastgesteld te worden welke storingen zijn opgetreden en hoe deze zijn opgelost.	6.4.3
De gegevensverwerking dient niet beïnvloed te worden door het gebruik van audit-tools.	10.3.1 10.3.2

Tabel 3. Raamwerk beveiligings-doelstellingen, vervolg.

Tabel 3. Raamwerk beveiligings-doelstellingen, vervolg.

Beveiligingsdoelstellingen	Maatregelen in de Code
Integriteit van gegevens	
Gegevens dienen slechts toegankelijk te zijn voor geautoriseerde personen.	7.1 t/m 7.7
Gegevensdragers dienen tijdens opslag en transport zorgvuldig behandeld te worden.	5.1.5 5.1.6 6.6.1 6.6.2 6.7.1 6.7.2
Gegevens dienen tijdens elektronische overdracht beschermd te worden tegen wijziging en verlies.	5.2.3 5.7.1 6.5.1 6.7.3 6.7.4 8.2.3 8.2.4
De integriteit van gegevens dient vastgesteld te worden voordat invoer in toepassingssystemen plaatsvindt.	8.2.1
De integriteit van gegevens dient tijdens de verwerking gewaarborgd te blijven.	8.2.2
Programmatuur dient slechts toegankelijk te zijn voor geautoriseerde personen.	7.1 t/m 7.7
Documentatie dient beveiligd te worden tegen ongeautoriseerde toegang.	6.6.3
Beveiligingseisen ten aanzien van systemen dienen (voorafgaand aan de ontwikkeling) expliciet vastgesteld en vastgelegd te worden.	8.1.1
Wijzigingen in standaardprogrammatuur dienen zoveel mogelijk te worden vermeden. Eventuele noodzakelijke wijzigingen dienen op beheerste wijze plaats te vinden.	8.4.3
Nieuwe (versie van) programmatuur dient op beheerste wijze (getest, geaccepteerd en geautoriseerd) in produktie genomen te worden.	6.1.4 6.2.2 6.2.4 8.3.1 8.4.1 8.4.2
Vertrouwelijkheid van gegevens	
Gegevens dienen slechts toegankelijk te zijn voor geautoriseerde personen.	7.1 t/m 7.7
Apparatuur dient zodanig geplaatst te worden dat vertrouwelijke gegevens niet (toevallig) kunnen worden waargenomen.	5.1.1 5.1.2 5.1.4 5.1.5 5.2.1
Gegevensdragers dienen tijdens opslag en transport zorgvuldig behandeld te worden.	5.1.5 5.1.6 5.2.5 6.6.1 6.6.2 6.7.1 6.7.2
Gegevens dienen tijdens elektronische overdracht beschermd te worden tegen onbevoegde kennisname.	5.2.3 6.5.1 6.7.1 6.7.3 6.7.4 6.7.5 8.2.3 8.2.4
De vertrouwelijkheid van (test)gegevens dient tijdens het testen gewaarborgd te zijn.	8.3.2
Gegevensdragers met gevoelige gegevens dienen op een veilige manier te worden afgevoerd wanneer zij niet langer nodig zijn.	5.2.6 6.6.1 6.6.4

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact
Een compilatie van artikelen over informatica en recht die in eerdere Compacts zijn verschenen, is, aangevuld met actuele bijdragen over dit onderwerp, opgenomen in *Twintig over Informatietechnologie en recht*. Twintig auteurs behandelen een breed spectrum van aspecten van de raakvlakken van informatietechnologie en recht op voor EDP-auditor, manager, adviseur, jurist en accountant toegankelijke wijze.
Het boek is verkrijgbaar via de boekhandel onder ISBN 90 14 04634 0.

2 20e jaargang 93/2 zomer 1993

Informatietechnologie duur? I/T Assessment: een beproefde methode voor het beoordelen van effectiviteit en efficiëntie van de informatieverzorging
Drs. B.T. Janssen, ing. W.J.D. Koot en ir. E.J. Mutsaers

Prioriteitenstelling met Decision
Dr. P.J. van Meel RI

De audit van een IT-investeringsaanvraag
Drs.ing. S.R.M. van den Biggelaar en drs. P.P.M.G.G. Brouwers

Verzekerbaarheid van automatiseringsrisico's
Mw.mr.drs. A.W. Duthler
Beveiligingsstandaard voor informatiesystemen
Prof.dr.ir. R. Paans RE

Global electronic mail: integratie van elektronische post met X.400
Ir. A. van Kooij

3 20e jaargang 93/3 herfst 1993

De toegevoegde waarde van EDP-auditing bij systeemontwikkeling
Ir. J.A. Verstelle

Normenstelsels voor systeemontwikkeling: hoe bruikbaar zijn deze?
Mw.drs. C.D.M. van der Veen

Projectbeheersing en -audit: contingency-benadering vereist
Ir. B.A.W.M. Bruns

De toegevoegde waarde van inspectietechnieken tijdens het ontwikkeltraject
B. Rooth

Invoering van informatiesystemen
Drs. Th.H. van Hesteren

Twintig vuistregels voor 'foutloos' onderhoud
E. Bergler

4 20e jaargang 93/4 winter 1993

Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving
Drs. R.G.A. Fijneman RE RA

Aandacht voor interne controle tijdens systeem-ontwikkeling
Drs. J.J. van Beek RE RA

Audit automation
Drs. L.H. Dam RA en drs. P. Veltman RE RA

Operational auditing en EDP-auditing; is hier sprake van een begripsverwarring?
J.C. Boer RE RA

Accountant, EDP-auditor en jurist: een multidisciplinaire samenwerking
Mw.mr.drs. A.W. Duthler

Automatiseringsrisico's, verzekeringen en de rol van de accountant
Drs. G.J.W.C. Vankan

Geautomatiseerde betalingen
Drs. R. Oudega en drs. P. Veltman RE RA

1 21e jaargang 94/1 lente 1994

De invloed van informatietechnologie op de beheersing van organisaties
Prof. A.W. Neisingh RE RA

Rekencentra: normen voor menskracht
Prof.dr.ir. R. Paans RE

Accountant en de kosten- en batenbeheersing van informatietechnologie
Prof. H.B. Moonen RE RA

Informatiebeveiliging: de tijd is rijp
Drs. H.G.Th. van Gils RE RA

Het beoordelen van het testen van systemen
P. van Berge

2 21e jaargang 94/2 zomer 1994

Audit van een SNA-netwerk
M.M. Buijs RI en E.J.M. Ridderbeekx RE RI

Beveiliging van analoge kieslijnen
Drs.ing. D. Brouwer RE

Beveiliging van UNIX
Mw.drs. M.C. van Lith RE

Typologie van workflow-managementsystemen
Drs. D.J.P. Witte

3 21e jaargang 94/3 herfst 1994

Inleiding tot op TCP/IP gebaseerde netwerken
Ir. P. Kornelisse

Internet? Maar dan wel met een firewall!
H. van Hulst

Netwerkverbindingen in een OpenVMS-omgeving
Ir. J.H. Lie-Tjauw

Enige juridische wegwijzers voor de elektronische snelweg
Mw.mr. G.P. van Duijvenvoorde

Betrouwbaarheid en beveiliging van een CICS-omgeving
Ing. G.H.M. Meijer RE en mw. J.A.M. Holla

4 21e jaargang 94/4 winter 1994

Geautomatiseerde gegevensbewerking en jaarrekeningcontrole
R.A. Jonker RA

De invloed van informatietechnologie op de interne-controleprincipes
J.C. Boer RE RA

Audit van een logistiek systeem
Drs. J.A.C. van Geel, ing. A.P.J. Mouwen en drs. E.P.R. van Vroenhoven RE RA

Informatiebeveiliging van theorie naar praktijk
Drs. P. Veltman RE RA

Informatie(beveiligings)beleid in concernverband
Prof. A.W. Neisingh RE RA

1 22e jaargang 95/1 lente 1995

Internetworking; beheerproblematiek en security-risico's
H. Roos RA en ir. M.T.H. Heesbeen

Geïntegreerd netwerkbeheer
Ing. W.A.A. Zoon

Client/server geconcretiseerd
J.C. van Praat RE RA

Radio-LAN's in de praktijk
Ir. B.J. Busropan, ir. G.J. de Groot, ir. W. Hollemans, ir. E.C. den Toom en ir. A. Verschoor

3DAS-kenmerk, een uniek middel voor identificatie en authenticatie
Ir. W.H.M. Sipman RI

2 22e jaargang 95/2 zomer 1995

Het beheer van PC-netwerken
Drs.ing. R.F. Koorn CISA

Multimedia nader bekeken
Drs. A.M. Buren

Introductie van een bancair systeem in een wide area netwerkomgeving
W.N.P. Zethof RE RA

GEBIT. Gestructureerd Evalueren van de Baten van IT-investeringen
Mw. M.S. Hablous

3 22e jaargang 95/3 herfst 1995

Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering
Mw. W.A. de Munck RA

Plaats en taken van de EDP-auditfunctie bij de KLM
J.G. de Vries RE RA

Wet op het consumentenkrediet: systeemgericht onderzoek vereist
R. van den Hoorn RA

Third party review en -mededeling bij uitbesteding van IT-services
Drs. P. Veltman RE RA

Maatwerk past informatiebeveiliging
Drs. E. Roos Lindgreen en mw.drs. C. Schönfeld RI

Stroomlijnen en herontwerpen in een onderhoudsbedrijf: gelijktijdig en/of volgtijdig?
Drs. O.C. van Leeuwen RA en drs. M.C. van Veen RC

Het ontwikkelen van methoden en technieken van EDP-auditing
Drs. R.G.A. Fijneman RE RA

4 22e jaargang 95/4 winter 1995

Informatieplanning en standaardpakketten
Drs. J. de Boer en ir. J.A.M. Donkers RE

Certificatie van een standaardpakket voor financiële administraties
Drs. H.G.Th. van Gils RE RA

AO en standaardpakketten: integratie verhoogt de kans op een succesvolle selectie en implementatie
Drs. J.J. van Beek RE RA, drs. W. Boogaard RA CPIM en drs. J.J.B. van den Oever

Waardebepaling van software
Ir. J.A.M. Donkers RE en drs. G.J.J. Timmer

Business Process Controlling
Drs. J.J. van Beek RE RA en W. Teeuwissen RA

KPMG EDP Auditors

Samsom BedrijfsInformatie