ICT-governance en informatiebeveiliging

(een handreiking voor bestuurders en commissarissen/toezichthouders)

Inleiding
De bestuurder van een organisatie is de primair verantwoordelijke voor het bepalen van de strategische doelstellingen en daarin begrepen het managen van de risico's die de 'drivers' achter de strategie bedreigen. De Raad van Commissarissen of Raad van Toezicht wordt geacht hierop toe te zien en daarnaast de bestuurder met raad en daad terzijde te staan.

Bij het realiseren van de strategische doelstellingen is Informatie & Communicatie Technologie (hierna: ICT) vandaag de dag onmisbaar en niet meer weg te denken, waardoor een adequate beheersing van informatie en ICT-omgeving basisvoorwaarden voor de continuïteit van de onderneming zijn geworden.

Dat betekent dat de bestuurder het ICT-landschap moeten kunnen overzien, begrijpen welke rol hij hierin speelt en in de Plan-Do-Check-Act cyclus ten aanzien van ICT de noodzakelijke 'checks en balances' aanbrengt om dit landschap te kunnen beheersen. De Raad van Commissarissen of Raad van Toezicht wordt vervolgens geacht hierop toe te zien en de bestuurder hierover zo nodig kritisch te bevragen c.q. met raad en daad terzijde te staan.

In dat licht is het opvallend dat, blijkens recent onderzoeken onder bestuurders en commissarissen, zowel het onderkennen van het belang als de kennis van ICT in totaliteit bezien bij beide groepen vaak ver onder de maat is.

Het belang van deze zorgwekkende constatering wordt versterkt door de verwachte golf van innovaties in de nanotechnologie, de medische technologie en de biotechnologie in de komende vijf jaar en de opkomst van verregaand gedigitaliseerde exponentiële organisaties. Het is dus hoog tijd dat ICT in de boardroom eindelijk de plaats krijgt die het al lang verdient.

Het aantal voorbeelden van slecht beheerste ICT-projecten is legio. Volgens een 'veilige' schatting van de parlementaire onderzoekscommissie die in 2015 onderzoek deed naar ICT-projecten bij de overheid, verspilt de Nederlandse overheid jaarlijks tussen de 1 en 5 miljard euro door ICT-mislukkingen. Ook in de profitsector zullen deze verspillingen enorm zijn. Uit recent onderzoek blijkt dat bijna de helft van alle ICT-projecten niet op tijd en niet binnen budget kan worden afgerond.

Het vakgebied van ICT bevat elementen van leiderschap en governance, technologie, menselijk gedrag en kwaliteit van processen, is daardoor complex, en aan snelle veranderingen onderhevig. Daarom beoogt dit document, voor bestuurders en commissarissen/ toezichthouders die daar behoefte aan hebben, te beschrijven hoe het ICT-landschap er uitziet, structuur aan te brengen in de complexe materie en kennis aan te reiken om meer grip te krijgen op de eigen ICT-omgeving en hun eigen rol daarin.

De opbouw van dit document is als volgt:
- In hoofdstuk 1 wordt uitgelegd wat ICT-governance is.
- In hoofdstuk 2 met bijbehorende bijlagen wordt nader ingegaan op de verschillende ICT-domeinen.
- In hoofdstuk 3 wordt in de vorm van het INK-model een kader aangereikt waarin het complexe en uitgebreide ICT-landschap op overzichtelijke wijze vorm is gegeven.
- In hoofdstuk 4 is het belangrijke aspect Informatiebeveiliging verder uitgewerkt.
- In hoofdstuk 5 is de rol van de controlerend accountant ten aanzien van ICT nader belicht.
- In hoofdstuk 6 zijn gebruikte bronnen vermeld en wordt verwezen naar verdere informatie.

Inhoudsopgave

Pim van den Hoff/Van den Hoff Informatiebeveiliging
Cees in ’t Veld/Focus op verbeteren
Maart 2016

1. ICT-governance

1.1 Definitie
ICT-governance oftewel ICT-besturing is een onderdeel van Corporate Governance.

Eén van de belangrijkste en meest gebruikte definities van I(C)T-governance is die van het IT Governance Institute (ITGI): 'IT Governance is the responsibility of the Board of Directors and executive management. IT is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategy and objectives.'.

Een veel gebruikte definitie in het Nederlands luidt: 'ICT-besturing beschrijft de wijze waarop een organisatie de besluitvorming van ICT het beste kan organiseren en welke rollen (taken, verantwoordelijkheden en bevoegdheden) altijd in een organisatie belegd moeten zijn om ICT goed te laten functioneren. Elke rol brengt zijn specifieke eigenschappen in en het samenspel tussen deze rollen zorgt voor control en beheersing, maar ook innovatie, creativiteit en vernieuwing.'.

De sterke toename in de interesse voor IT-governance hangt mede samen met ontwikkelingen in wet- en regelgeving (zoals de Sarbanes-Oxley Act in de Verenigde Staten en Basel in Europa) en een grotere behoefte aan verantwoording van besluitvorming rondom ICT.

Het doel van ICT-governance is om de belangen van de (externe of interne) klant, het bestuur, de medewerkers, de aandeelhouders en andere belangrijke stakeholders systematisch in het ICT besluitvormingsproces te betrekken:
ICT-governance zorgt voor een transparant raamwerk voor organisaties waarin taken, verantwoordelijkheden en bevoegdheden zijn toegewezen aan personen of groepen.

1.2 Modellen
Er zijn verschillende modellen ontwikkeld met handvatten om ICT-governance praktisch in te richten:

- ISO/IEC 38500:2008 'Corporate governance of information technology' is een wereldwijde standaard die een overzicht geeft van zes richtlijnen omtrent IT-Governance: Responsibility, Strategy, Acquisition, Performance, Conformance en Human behavior. Het doel hiervan is het verbeteren van de effectiviteit, de efficiëntie en een aanvaardbaar gebruik van IT.

- 'Control Objectives for Information and related Technology' (COBIT) is een model dat is ontwikkeld door ISACA en ITGI, en focust op vijf hoofdthema's: Strategic alignment, Value delivery, Risk management, Resource management en Performance management. Dit is een zeer gedetailleerd model met het gevaar in zich dat het model een doel wordt in plaats van een middel.

1.3 Besluitvorming en rollen

Van belang bij het proces van besluitvorming zijn:

- Hoe verloopt het besluitvormingsproces?
- Waarover moeten besluiten worden genomen?
- Wie moet die besluiten nemen?

Het is van belang om hierover een procedure vast te stellen binnen de organisatie, bijvoorbeeld via een besluitvormingsmatrix. Door vooraf helderheid en overeenstemming te bereiken over het te volgen proces worden veelvuldig overleg en onnodige discussies voorkomen. Daarbij is het essentieel dat de juiste personen met enerzijds voldoende kennis en ervaring op ICT gebied en anderzijds de business als gebruiker participeren en het spanningsveld van ICT in relatie tot business expliciet in de besluitvorming wordt betrokken.

De ICT Governance matrix van Weill en Ross (2004) geeft duidelijk de verschillende rollen weer en daarbij welke beslissingen door wie worden genomen. Deze matrix geeft in mindere mate inzicht in de relaties tussen verschillende rollen.

Weill en Ross onderkennen vijf onderwerpen waarover in het kader van ICT-governance besluiten moeten worden genomen:

- De rol van ICT binnen de organisatie.
- De ICT-architectuur.
- De ICT-middelen.
- De functionaliteiten/business applicaties.
- De beschikbaarstelling van budgetten.

Als partijen in het besluitvormingsproces zijn in elk geval te onderkennen:

- Het topmanagement.
- Het ICT-management.
- Het Business Unit management.
- Het afdelingsmanagement.

Door de diversiteit aan onderwerpen waarover beslissingen moeten worden genomen is er geen eenduidig antwoord te geven op de vraag wie beslist over ICT.

2. Beheerdomeinen van ICT
Men onderscheidt in de ICT drie vormen van beheer (beheerdomeinen):

- Technisch Beheer (ITIL), zie bijlage 4

Richt zich op het beheer van de IT-infrastructuur en heeft ITIL als standaard. De IT-infrastructuur is een basis waarop applicaties kunnen draaien. Deze applicaties worden beheerd door Applicatiebeheer.

- Applicatiebeheer (ASL), zie bijlage 5

Onder dit beheer wordt verstaan het aanpassen van de applicatie naar aanleiding van geconstateerde fouten in de applicatie of veranderende technische of functionele eisen. Het gaat nadrukkelijk om bestaande applicaties en niet om nieuwbouw van applicaties. ASL is hiervoor de standaard. ASL is nieuwer dan en deels geïnspireerd door ITIL.

- Functioneel beheer (BiSL), zie bijlage 6

De applicaties worden gebruikt door de gebruikersorganisatie. Deze organisatie zal aan moeten geven aan welke eisen die applicatie moet voldoen en controleren of na een eventuele aanpassing deze applicatie inderdaad voldoet. Dit proces noemt men Functioneel Beheer en heeft als standaard BiSL.

De processen in de domeinen staan met elkaar in verbinding en vormen ketens. De output van het ene proces is input van het andere proces. Volgens COBIT5 is op de ICT-processen de (plan-do-check-act) levenscyclus-benadering van toepassing met als doel om de “capability” naar het gewenste ambitieniveau te krijgen en te houden.

Het is van belang voor een organisatie om de juiste processen uit te voeren op het juiste beheersingsniveau passend bij de risicobereidheid en de beschikbare middelen van de organisatie. COBIT onderkent vijf stadia van beheersing als resultante van:

- De mate van documentatie, bewustzijn en monitoring.
- Het ontwerp en de operationele effectiviteit.

Stadium 0: Niet bestaande of incomplete beheersing (nonexistent).
Stadium 1: Het proces is onvoorspelbaar, slecht beheerst en reactief (initial).
Stadium 2: Het proces wordt gekenmerkt door projecten en vaak reactief (managed).
Stadium 3: Het proces wordt gekenmerkt door de organisatie en is proactief (defined).
Stadium 4: Het proces wordt gemeten en beheerst (quantitatively managed).
Stadium 5: Focus op continue verbetering (optimised).

3. Het ICT-landschap in het INK-model

Zoals uit het voorgaande blijkt bestaan er zeer uitgebreide standaarden en 'best practice' voorbeelden om goede ICT-governance handen en voeten te geven. De uitdaging is om dit ingewikkeld en uitgebreide landschap voor bestuurders en commissarissen/toezichthouders begrijpelijk en behapbaar te maken. Het INK-model leent zich daar uitstekend voor.

Het ICT-landschap kan in het INK-model als volgt schematisch worden weergegeven:

In COSO: S = Strategy, R = Reporting, C = Compliance, overige = Operations

3.1 Leiderschap, gedrag en organisatie

Een belangrijk onderdeel van leiderschap is het zorgdragen voor een cultuur van gewenst gedrag ten aanzien van ICT-gebruik (waaronder internet), ICT-beheer en ICT-beveiliging, het tonen van voorbeeldgedrag daarin, het definiëren en uitrollen van gedragsregels en het instellen van beheersmaatregelen die de naleving van deze gedragsregels borgen.

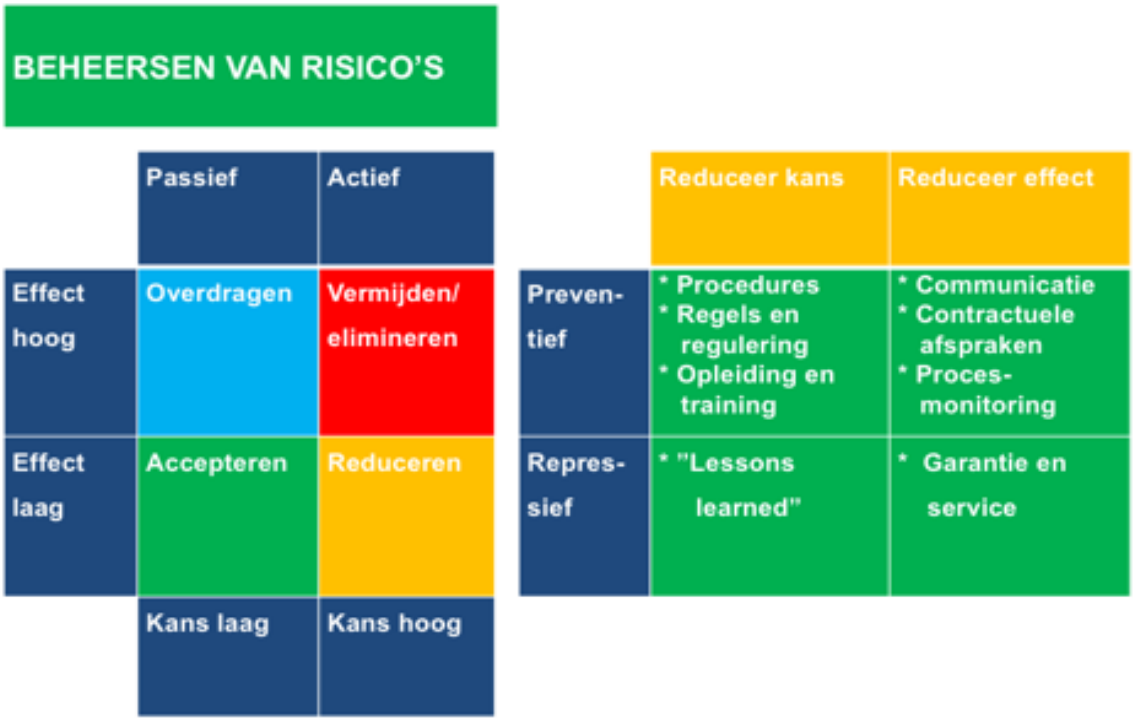
3.2 Strategie en beleid

3.2.1 ICT-strategie

Het is de primaire rol van de bestuurder om vanuit missie en visie een strategie te bepalen: welke doelstellingen wil de organisatie behalen, hoe moet dat gebeuren en welke mensen en middelen worden daar bij ingezet?

Anno 2016 is het bijna ondenkbaar dat ICT niet een van die ingezette middelen is.
Dat betekent dat door de bestuurder strategische keuzes moeten worden gemaakt over de rol van ICT binnen de organisatie, de ICT-architectuur (zie ook bijlage 7), de ICT-middelen, de functionaliteiten waaraan de ICT moet voldoen, de applicaties die worden ingezet en de beschikbaarstelling van budgetten. Vervolgens moet een beheersorganisatie worden ingericht die ervoor zorgt dat de geautomatiseerde gegevensverwerking in continuïteit zonder verstoringen en goed beveiligd kan plaatsvinden.

3.2.2 ICT-beveiliging en risicomanagement
Zodra de strategie is bepaald moet worden gedefinieerd wat de belangrijke 'drivers' achter de strategie zijn en wat de bedreigingen van deze 'drivers' zijn. Aan de hand van de in kaart gebrachte bedreigingen of risico's wordt een risicoprofiel opgesteld en de risicobereidheid (of 'risk appetite') bepaald. Vervolgens worden de beheersmaatregelen daarop ingericht.
Modelmatig kan dat er als volgt uitzien:



Bron: Bedrijfsvitaliteit/Van Heeswijk

Deze benadering geldt niet alleen voor de algehele strategie maar ook voor de ICT-strategie. Ook voor de ICT-omgeving moet worden beoordeeld wat de 'drivers' achter de ICT-strategie en de bijbehorende risico's zijn en hoe groot de risicobereidheid is. Op grond daarvan moeten de ICT-beheersmaatregelen worden bepaald.

3.2.3 ICT-management controles
Nadat de bestuurder betrokken is geweest bij de strategische ICT-keuzes, het risicomanagement, het beveiligingsbeleid en de inrichting van de ICT-beheeromgeving zullen de verdere executie en de dagelijkse operatie kunnen worden gedelegeerd.

Bij delegeren hoort echter ook controleren. Dit betekent dat ICT-managementcontroles moeten worden ingericht die de bestuurder in staat stellen te monitoren of inderdaad sprake is van een beheerste ICT-omgeving. Eén daarvan is de periodieke rapportage zoals beschreven onder paragraaf 3.5.5. Indien aan de orde is ook voor de controlerend accountant een belangrijke rol weggelegd.

3.3 Management van medewerkers

3.3.1 Gedrag

Medewerkers dienen zich bewust te zijn van de eisen ten aanzien van ICT-gebruik, ICT-beheer en ICT-beveiliging en de risico's die met ICT gepaard gaan.
Zaken als discipline in het naleven van regels, zich bewustzijn van risico's, alertheid op ongebruikelijke zaken (zoals phishing mails) en elkaar aanspreken op overtredingen behoren tot het gewenste gedrag.

3.3.2 Reglement

Het is gewenst om de spelregels omtrent ICT-gebruik (waaronder internet), ICT-beheer en ICT-beveiliging vast te leggen in (een) reglement(en) en deze te koppelen aan de arbeidsovereenkomst. Door het tekenen van de arbeidsovereenkomst ligt op die manier direct vast dat de werknemer kennis heeft genomen van de spelregels omtrent ICT en en dat hij deze spelregels naar beste kunnen zal naleven. Dit werkt preventief en ondersteunt de juridische positie van de organisatie bij overtredingen.

3.3.3 Opleiding en training

Risico's op ICT-gebied veranderen voortdurend. Dat betekent dat het personeel bij indiensttreding vertrouwd moet worden gemaakt met de gangbare risico's en de interne spelregels. Periodiek moet deze kennis worden geactualiseerd op grond van actuele ontwikkelingen.

3.4 Management van ICT-middelen (hard- en software)

3.4.1 Fysieke beveiliging

Net als gebouwen, machines en installaties moeten hard- en software fysiek worden beveiligd tegen brandschade, waterschade, diefstal en vernieling. Daarom moet de fysieke toegang tot hardware en software worden beperkt tot degenen die met deze activa werken. Tevens moet sprake zijn van een adequate activaregistratie, moeten hardware en software adequaat zijn verzekerd en moeten er procedures zijn voor de omgang met deze activa (met speciale aandacht voor draagbare activa als PC's, beamers, printers en gegevensdragers als USB-sticks).

3.4.2 Netwerkbeveiliging

ICT-middelen zijn vrijwel altijd met elkaar verbonden in een netwerk. Dit netwerk moet worden beschermd tegen ongeautoriseerde toegang van binnenuit en buitenaf alsmede van andere bedreigingen van buitenaf.

Veel voorkomende beveiligingsmiddelen zijn:

- Een firewall die ongeautoriseerde toegang tot het netwerk blokkeert.
- Webfilters, om internetverkeer te filteren op inhoud.
- Intrusion prevention systemen om aanvallen snel te kunnen identificeren.
- Antivirussoftware.
- Data Loss Prevention, waarmee het uitlekken van informatie wordt voorkomen.
- Network Access Control, om ongeautoriseerde apparatuur van het netwerk te weren.
- Security Incident and Event Management, om logbestanden te analyseren.
- Logische toegangsbeveiliging tot het netwerk.
- Virtual Private Networks (VPN) voor beveiligde toegang op afstand.

3.4.3 Back up, recovery en uitwijk

Ingeval het gebruik van hardware of software ondanks alle genomen maatregelen wordt verstoord of er gegevens verloren gaan zal de organisatie dit zo snel mogelijk moeten herstellen. Daarom dient volgens afgesproken procedures permanente back-up van de gegevensverwerking plaats te vinden en dienen er procedures te zijn om de geautomatiseerde gegevensverwerking zo snel mogelijk te kunnen hervatten. Eén van de mogelijkheden is het uitwijken naar reservecapaciteit elders. Back up, recovery en uitwijk dienen volgens overeengekomen procedures periodiek te worden getest.

3.4.4 Change management (wijzigingsbeheer)

Een betrouwbare geautomatiseerde gegevensverwerking staat of valt met het gebruik van geautoriseerde hard- en software die voor ingebruikname grondig is getest. In elke automatiseringsorganisatie vinden wijzigingen plaats in de vorm van nieuwe hardware, software-uitbreidingen, software-updates en dergelijke. Deze wijzigingen dienen uitsluitend te worden uitgevoerd volgens geautoriseerde procedures, waarvan het testen van de wijzigingen en een ongestoorde werking na wijziging het sluitstuk zijn.

3.4.5 Logging

Logging raakt het management van middelen én van processen en is het automatisch registreren van gebeurtenissen in de ICT-systemen waarmee zowel de goede werking van interne beheersingsmaatregelen alsmede de inbreuk op ICT-systemen kan worden gesignaleerd. De continue analyse van logginggegevens door daartoe aangewezen personen inclusief de periodieke rapportage daarover (zie 3.5.5) is daarom een belangrijke beheersingsmaatregel.

3.4.6 Incident/probleem management

Bij de geautomatiseerde gegevensverwerking kunnen problemen ontstaan of zich incidenten voordoen die de de gegevensverwerking verstoren. Deze incidenten dienen tijdig te worden vastgelegd, de oorzaken onderzocht en geëvalueerd op mogelijke structurele gevolgen. Op grond hiervan zullen acties worden bepaald en geautoriseerd door daartoe bevoegde personen. Over deze problemen en incidenten dient op structurele wijze te worden gerapporteerd (zie 3.5.5).

3.5 Management van processen

3.5.1 Application controles

Application controls zijn geautomatiseerde of handmatige, preventieve of detectieve controles die op het niveau van het specifieke bedrijfsproces c.q. applicatie zijn geregeld en zijn gericht op de juiste en volledige verwerking en vastlegging van transacties.

3.5.1.1 Logische toegangsbeveiliging

Een zeer belangrijke application control is de logische toegangsbeveiliging: uitsluitend daartoe bevoegde personen mogen toegang hebben tot de applicatie en de daarin opgenomen data. Logische toegangsbeveiliging bestaat uit drie elementen:

- Identificatie; hierbij moet een gebruiker zich identificeren met gebruikersnaam.
- Authenticatie; hierbij moet een gebruiker zich identificeren met wachtwoord.
- Autorisatie is erop gericht dat de gebruiker na identificatie en authenticatie toegang krijgt tot de applicatie.

De logische toegangsbeveiliging is de digitale resultante van de ingerichte functiescheidingen om een adequate gegevensverwerking en informatievoorziening te borgen.
Rechten van gebruikers liggen vast in een competentietabel die permanent up-to-date moet worden gehouden, hetgeen onder meer betekent dat geautoriseerde wijzigingen uit hoofde van in- en uitdiensttreding, promoties, wijzigingen in bevoegdheden en dergelijke juist, volledig en tijdig moeten worden doorgevoerd. Bijzonder aandacht in de interne controle verdient de superuser.

3.5.1.2 Invoercontroles

Invoercontroles zijn gericht op de betrouwbaarheid van de invoer van gegevens in de applicatie en omvatten bestaan, juistheid als volledigheid en omvatten zowel detailcontroles, totaalcontroles als verbandcontroles.

3.5.1.3 Verwerkingscontroles

Verwerkingscontroles zijn gericht op de betrouwbare verwerking binnen de applicatie en omvatten zowel detailcontroles, totaalcontroles als verbandcontroles.

3.5.1.4 Interfacecontroles

Een interface is een koppeling tussen verschillende onderdelen van het geautomatiseerde systeem. Interfacecontroles zijn gericht op de juiste en volledige informatie-uitwisseling tussen onderdelen van het systeem en hebben meestal het karakter van totaal- en verbands-controles zoals batch- en hashtotalen.

3.5.1.5 Databasecontroles

Een database, gegevensbank of databank is een digitaal opgeslagen archief, ingericht met het oog op flexibele raadpleging en gebruik. Databasecontroles zijn gericht op de juistheid en volledigheid van de gegevens die in de database zijn opgeslagen en hebben meestal het karakter van totaal- en verbandcontroles zoals batch- en hashtotalen.

3.5.1.6 Uitvoercontroles
Uitvoercontroles zijn controles op de betrouwbaarheid van fysieke (documenten) of digitale (e-mails) output van systemen.

3.5.2 Geprogrammeerde controles
Geprogrammeerde controles zijn in de applicatie geprogrammeerde rekenregels die zorgen voor de juiste verwerking van gegevens.

3.5.3 Gebruikerscontroles
Gebruikerscontroles zijn door de gebruikers handmatig uitgevoerde controles op de geautomatiseerde gegevensverwerking, al dan niet ondersteund door output van het systeem. Door de feilbaarheid van mensen en eventuele verkeerde intenties worden deze controles als minder betrouwbaar beschouwd en ze dienen daarom strakker intern te worden gemonitord.

3.5.3.1 Door IT ondersteunde gebruikerscontroles
Bij deze controles wordt output uit het systeem gebruikt. Alvorens hierop te kunnen steunen dient de betrouwbaarheid van de output te worden vastgesteld.

3.5.3.2 Overige gebruikerscontroles
Bij deze gebruikerscontroles wordt geen output uit het systeem gebruikt.

3.5.4 Naleven wet- en regelgeving
Met betrekking tot ICT is onder meer de volgende specifieke regelgeving van toepassing:
- Wet Bescherming Persoonsgegevens (WBP), met de meldplicht datalekken.
- Telecomwetgeving, waarvan de cookiewetgeving deel uit maakt.
- Wet Computercriminaliteit, een wet die verbiedt om in te breken op computers.
- EU-wet Databescherming (2018), een Europees geregelde privacywetgeving.

De naleving van deze wet- en regelgeving moet door interne beheersingsmaatregelen worden geborgd. Deze beheersingsmaatregelen moeten permanent worden gemonitord, overtredingen worden periodiek gerapporteerd in de onder 3.5.5 genoemde rapportage.

3.5.5 Monitoring en rapportage
Procedures en controles die samenhangen met het in 3.3 genoemde management van medewerkers, het in 3.4 genoemde management van middelen en het in 3.5 genoemde management van processen moeten permanent worden gemonitord door daartoe aangewezen personen. De bevindingen hierover moeten periodiek, bijvoorbeeld maandelijks, worden gerapporteerd.

3.6 Personeelstevredenheid
Een gebruikersvriendelijke en ongestoord functionerende ICT, ondersteund door een goede helpdesk, is een belangrijk element van personeelstevredenheid. Het is daarom raadzaam om de mate van tevredenheid inzake ICT op te nemen in periodieke onderzoeken naar personeelstevredenheid.

3.7 Klanttevredenheid

Een klantvriendelijke en ongestoord functionerende ICT, ondersteund door een goede helpdesk, voor die onderdelen van de ICT-omgeving waarmee de klant in aanraking komt, is een belangrijk element van klanttevredenheid. Het is daarom raadzaam om de mate van tevredenheid inzake ICT op te nemen in periodieke onderzoeken naar klanttevredenheid.

3.8 Stakeholdertevredenheid

Een gebruikersvriendelijke en ongestoord functionerende ICT, ondersteund door een goede helpdesk, voor die onderdelen van de ICT-omgeving waarmee andere externe relaties dan de klant in aanraking komen, kunnen een belangrijk element van stakeholdertevredenheid en imago zijn (zie ook 4.3). Het is daarom raadzaam om daarop alert te zijn.

4. Informatiebeveiliging

4.1 Algemeen
Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen voor elke organisatie. Daarom moet er beveiligingsbeleid worden gedefinieerd om informatie adequaat te kunnen beveiligen. ISO 27001:2013 (eisen aan Information Security Management System) en ISO 27002:2013 (code voor informatiebeveiliging) zijn hiervoor belangrijke standaarden.

Informatiebeveiliging bestaat al sinds mensheugenis. Fundamentele principes bij informatiebeveiliging zijn beschikbaarheid, exclusiviteit (vertrouwelijkheid) en integriteit. Alle beveiligingsacties worden uitgevoerd om een of meer van deze principes af te dekken. Door de opkomst van ICT in de 20e eeuw zijn informatiebeveiliging en ICT-beveiliging steeds meer parallel gaan lopen. Daardoor zijn veel aspecten ten aanzien van informatiebeveiliging in hoofdstuk 3 van dit document al aan de orde geweest.
In dit hoofdstuk worden aanvullend een aantal niet eerder genoemde informatiebeveiligingsaspecten nader uitgewerkt.

4.2 Wetgeving en ICT
In dit hoofdstuk gaan we verder in op de in 3.5.4 genoemde wet- en regelgeving.
Met uitzondering van de Wet Computercriminaliteit is de wetgeving vooral gericht op het beschermen van persoonsgegevens. Een persoonsgegeven gaat altijd over een individu en het eigenaarschap kan nooit bij een ander komen te liggen. De wetten leggen vast welke rechten de eigenaren van de gegevens hebben en hoe organisaties om dienen te gaan met het beveiligen van de gegevens.

Dat de wetgever het beschermen van persoonsgegevens serieus neemt blijkt uit het feit dat er boetes kunnen worden opgelegd als organisaties onverantwoord omgaan met deze gegevens. Je zult als organisatie duidelijk in beeld moeten hebben welke persoonsgegevens er verwerkt worden en hoe dit gebeurt. De systemen en applicaties waarin deze gegevens zijn opgeslagen zullen voldoende beveiligd moeten zijn om misbruik te voorkomen.

Persoonsgegevens zijn een zeer gewild doelwit van criminelen. Een persoonsgegeven biedt namelijk een scala van mogelijkheden voor misbruik, en dat is niet alleen het stelen van geld van een bankrekening. Een crimineel die een identiteit in handen heeft kan zich namelijk voordoen als iemand anders en daar zijn voordeel mee doen. De hoge waarde van een gestolen identiteit wordt daarnaast bepaald door de lange periode waarin de crimineel misbruik kan maken. Iemand kan zijn identiteit immers niet zomaar veranderen.

4.3 Informatiebeveiliging in de keten
Bij het uitbesteden van processen buiten de organisatie blijft informatiebeveiliging een belangrijk aandachtspunt voor de bestuurder. Bij het overdragen van activiteiten naar een dienstverlener of partner zal er door de andere partij ook informatie worden verwerkt.
De risico's en de gerelateerde maatregelen zijn ook dan relevant. De eindverantwoordelijkheid voor de bescherming van de informatie blijft altijd een zaak van de eigenaar van de informatie.

Voor informatie waarvoor de organisatie zelf eindverantwoordelijk is, zoals Intellectueel eigendom, kan de organisatie zelf bepalen of zij de mate van beveiliging bij de ketenpartner afdoende vindt. Dit is anders wanneer de partner ook persoonsgegevens gaat verwerken of informatie die eigendom is van bijvoorbeeld een opdrachtgever. In dat geval zijn er aanvullende eisen van kracht vanuit wetgeving (Wet Bescherming Persoonsgegevens) of externe normenkaders.

Bij de uitbesteding van de verwerking van informatie in een keten zijn er telkens twee zaken die beoordeeld worden:

- juridische kaders waaronder de uitbesteding plaatsvindt, en
- beveiligingsmaatregelen die minimaal getroffen moeten zijn.

Via de juridische kaders wordt onderling afgestemd wat de partijen van elkaar verwachten en hoe er met de informatie wordt omgegaan. Met betrekking tot persoonsgegevens is het verplicht om dit vast te leggen in bewerkersovereenkomsten.
De beveiligingsmaatregelen moeten aansluiten op de eisen die vanuit het risicomanagement zijn opgelegd.

De bestuurder zal op elk gewenst moment inzicht willen hebben in de status van de uitbestede processen, de informatie die extern wordt verwerkt en de mate van beveiliging. Dit wordt gedaan door de eerdergenoemde ICT-beheeractiviteiten ook bij ketenpartijen te beleggen. Anderzijds zal de bestuurder ook inzichtelijk willen hebben dat zijn/haar organisatie voldoet aan de eisen die door anderen zijn opgelegd voor informatie waarvan het eigenaarschap niet in de eigen organisatie ligt.

4.4 Informatiebeveiliging en Cloud Computing

Bij het uitbesteden van informatieverwerking is Cloud Computing direct een aandachtspunt. Als de organisatie ervoor kiest om applicaties in de Cloud te gaan gebruiken zijn juridische- en beveiligingseisen van toepassing. De organisatie moet zelf goed weten welke eisen er op beide vlakken aan de Cloudleverancier moeten worden gesteld.

Vanuit juridisch oogpunt zijn de eisen met betrekking tot het gebruik van Cloud met name van belang als er ook persoonsgegevens worden verwerkt. Europese regels stellen dat de verwerking van persoonsgegevens niet mag worden uitbesteed naar landen waar de vertrouwelijkheid van de gegevens niet kan worden gegarandeerd. Op dit moment wordt de VS beschouwd als onvoldoende veilig. Je zult daarom als organisatie goed moeten weten welke informatie door welke Clouddiensten wordt verwerkt en of er wordt voldaan aan de geldende wet- en regelgeving.

De controle op en het inzicht in het gebruik van Cloudapplicaties zijn ook relevant wanneer de organisatie informatie verwerkt van klanten. Opdrachtgevers blijven eindverantwoordelijk voor hun eigen informatie en stellen eisen aan de beveiliging en de verwerking van die informatie. Het komt regelmatig voor dat in overeenkomsten is vastgelegd dat een klant op de hoogte moet worden gesteld indien de gegevens in de Cloud zullen worden verwerkt. Hier dient rekening mee te worden gehouden bij het inzetten van Cloudapplicaties.

4.5 Shadow IT

Het voordeel van Cloud is dat een organisatie niet zelf hoeft te investeren in ICT-middelen, een verbinding met het internet is vaak de enige voorwaarde. Dit heeft als gevolg dat elke afdeling of elk individu gebruik kan maken van applicaties die niet door de organisatie zijn goedgekeurd. Dit ongecontroleerde gebruik van onder andere Cloud wordt vaak aangeduid als Shadow-IT.

Traditioneel kon niemand gebruik maken van applicaties zonder dat de afdeling ICT daarvan af wist. Er moest immers een systeem zijn waarop de software geïnstalleerd moest worden. Met de komst van Cloud is dit achterhaald. Hiermee is ook het controlepunt in het applicatiebeheer komen te vervallen met als gevolg dat applicaties ingezet kunnen worden zonder dat deze onderdeel zijn van gestructureerd risicomanagement.

Medewerkers willen gewoon hun werk doen en zijn gewend om een scala van handige applicaties (apps) te gebruiken voor persoonlijke doeleinden. Het is daarom niet vreemd dat zij de middelen die zij privé gebruiken ook zakelijk inzetten (denk hierbij aan het recente voorbeeld dat artsen röntgenfoto's via WhatsApp uitwisselden. In dit geval ging het om gevoelige persoonsgegevens die worden verwerkt door een Amerikaans bedrijf waarmee geen aanvullende afspraken zijn gemaakt).

Om de risico's met betrekking tot Shadow-IT te kunnen beheersen zullen medewerkers er van bewust moeten worden dat er risico's zijn en wat het beleid van de organisatie op dit vlak is.

5. De rol van de controlerend accountant ten aanzien van ICT

Middelgrote en grote ondernemingen zijn op grond van het Burgerlijk Wetboek deel 2 Titel 9 (BW2 Titel 9) controleplichtig waardoor sprake is van verplichte accountantscontrole.
Ook zijn er kleine ondernemingen waar sprake is van vrijwillige accountantscontrole.
Bij de accountscontrole van de jaarrekening is de accountant verplicht de Nadere Voorschriften Controle- en Overige Standaarden (NVCOS) toe te passen, waarin op een aantal plaatsen wordt gerefereerd aan ICT. Belangrijke Standaarden in dit verband zijn:

- Standaard 315 'Risico's op een afwijking van materiaal belang identificeren en inschatten door inzicht te verwerven in de entiteit en haar omgeving'.
- Standaard 330 'Inspelen door de accountant op ingeschatte risico'.
- Standaard 402 'Overwegingen met betrekking tot controles van entiteiten die gebruik maken van een serviceorganisatie'.

Dat betekent dat de accountant die voor de jaarrekeningcontrole steunt op interne beheersmaatregelen:

- De opzet van die maatregelen moet beoordelen.
- Het bestaan ervan moet vaststellen.
- De permanente werking ervan moet toetsen.

Dat geldt dus ook voor de ICT-aspecten van die maatregelen. Concreet betekent dit dat, afhankelijk van de mate waarop de accountant voor zijn controle steunt op ICT, de accountant in meerdere of mindere mate de volgende onderdelen van het INK-model (zie inleiding paragraaf 3) in zijn controle betrekt:

- Leiderschap (met name gedrag/cultuur).
- Strategie.
- Personeel.
- Management van middelen.
- Management van processen.

Op grond van Standaard 260 'Meedelen van tekortkomingen in de interne beheersing aan de met governance belaste personen en het management' moet de accountant tekortkomingen melden. Dit kan in het wettelijk verplichte deskundigenverslag zoals genoemd in BW2 Titel 9 artikel 393 lid 4 (in de wandelgangen: het accountantsverslag) waar is opgenomen:
'De accountant brengt omtrent zijn onderzoek verslag uit aan de raad van commissarissen en aan het bestuur. Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.'.

Ook in de adviesbrief (in de wandelgangen vaak: de management letter) zullen dergelijke tekortkomingen – vaak meer in detail - een plaats krijgen.

In specifieke gevallen kunnen ook Standaard 240 'De verantwoordelijkheid van de accountant met betrekking tot fraude in het kader van een controle van financiële overzichten' en Standaard 250 'Het in aanmerking nemen van wet- en regelgeving bij een controle van financiële overzichten' van toepassing zijn.

6. Bronnen en verdere informatie

6.1 Gebruikte bronnen:

- Draft NCSU IT Governance Directions V2.3 2/16/2010
- Handboek Regelgeving Accountancy, NVCOS
- www.cio.nl
- www.managementboek.nl
- www.trouw.nl/tr/nl/4516/Gezondheid/article/detail/4251024/2016/02/24/Artsen-moeten-niet-appen-over-hun-werk.dhtml
- www.wikipedia.nl

6.2 Leestips/nuttige websites:

- Boek Basiskennis informatiebeveiling op basis van ISO 27001 en ISO 27002,
  Hans Baars/Jule Hintzbergen/Kees Hintzbergen/Andre Smulders,
  Van Haren Publishing, ISBN 978-94-018-0013-6, zie verdere informatie in bijlage 8.
- www.beschermjebedrijf.nl.
- www.hoffmannbv.nl (Hoffmann ICT-Security).
- www.ncsc.nl (Nationaal Cyber Security Centrum).
- www.veiliginternetten.nl.

Bijlage 1 Aandachtspuntenlijst voor bestuurders en commissarissen/toezichthouders

Par.	Eis	Ja	Nee	Nvt	Toelichting
1.2	Is een model in gebruik voor ICT-governance?				
1.3	Liggen rollen en bevoegdheden schriftelijk vast?				
2.	Worden standaarden gebruikt voor: • Technisch beheer (bijvoorbeeld ITIL?) • Applicatiebeheer (bijvoorbeeld ASL)? • Functioneel beheer (bijvoorbeeld BiSL)? • Infrastructuur (bijvoorbeeld TOGAF)?				
3.1	Worden gewenste cultuur en gedrag: • Expliciet gemaakt? • Uitgedragen door het management?				
3.2	Ligt ICT-beleid op hoofdlijnen vast?				
3.2	Ligt ICT-risicomanagement schriftelijk vast?				
3.2	Ligt ICT-beveiligingsbeleid schriftelijk vast?				
3.2	Zijn management controls en de rapportage daarover adequaat?				
3.3	Wordt het gedrag van medewerkers adequaat gemonitord?				
3.3	Zijn er reglementen voor het het gebruik, het beheer en de beveiliging van ICT? Zo ja, zijn deze gekoppeld aan het arbeidscontract?				
3.3	Is opleiding en training van medewerkers ten aanzien van ICT adequaat geregeld? Zo ja, vindt hierover rapportage plaats?				
3.3	Vindt over het management van medewerkers rapportage plaats?				
3.4	Is het management van middelen procedureel adequaat geregeld? Zo ja, vindt hierover rapportage plaats?				
3.5	Is het management van processen procedureel adequaat geregeld? Zo ja, vindt hierover rapportage plaats?				
3.6	Is ICT opgenomen in het medewerkerstevredenheidsonderzoek?				
3.7	Is ICT opgenomen in het klanttevredenheidsonderzoek?				
3.8	Is er zicht op de tevredenheid over ICT onder overige belangrijke stakeholders?				
4	Ligt het informatiebeveiligingsbeleid schriftelijk vast?				
5	Wordt optimaal gebruik gemaakt van de rol van de controlerend accountant?				

Bijlage 2 Faalfactoren van ICT-processen (Bron: www.cio.nl - Hemant Kogekar)

Vage doelstellingen
Veel grote projecten falen omdat de doelstelling niet duidelijk genoeg is. Er is geen heldere probleemdefinitie en de eisen worden niet duidelijk geformuleerd en is er verwarring over de scope van het project. De ene manager start het project met een doelstelling, maar als het project vordert, haken er andere mensen aan die ook hun ideeën uiten en invloed op het concept uitoefenen. Het resultaat is dat de doelstellingen onduidelijk worden, de scope vaak te groot wordt en het projectontwerp eronder lijdt.
Dit leidt vaak tot ellenlange vergaderingen en continue verruiming van deadlines.

Een teveel aan optimisme
Vertegenwoordigers van het project en projectleiders willen dat hun project slaagt. Helaas maken ze in het 'verkooppraatje' van hun project fouten – ze onderschatten de kosten en overschatten de voordelen. In het maken van de businesscase ligt altijd de neiging op de loer om zoveel mogelijk voordelen te bedenken en de kosten zo laag mogelijk te houden om zo tot een zo gunstig mogelijke *return on investment* te komen. Vaak gebeurt dit onbewust, maar ook vaak is dit te wijten aan gebrekkige kennis bij de manager als het gaat om de huidige situatie en de requirements.
Een teveel aan optimisme resulteert in te optimistische tijdplanningen. Vaak is er ook sprake van te veel vertrouwen in de technologie (het product, de leverancier of intrinsieke mogelijkheden). De complexiteit van de oplossing wordt vaak ook niet goed geëvalueerd.

Complexiteit
Veel ICT-projecten zijn enorm complex vanwege de nieuwe technologie, interfaces met andere systemen, dataconversies of omdat het projectteam wat betreft resources moet concurreren met andere projecten. Soms moeten ook legacyprocessen gereproduceerd of herontwikkeld worden voor het nieuwe systeem, wat ook complexiteit toevoegt. Wat projectmanagers en bestuurders vaak niet goed begrijpen, is dat het risico en de benodigde expertise bij een project exponentieel toenemen met een toename in complexiteit. Systemen en processen worden broos als mensen deze complexiteit in een beperkte tijdspanne willen doorgronden en met workarounds gaan werken. De complexiteit stijgt projectmanagers vervolgens boven het hoofd en het project is niet langer in bedwang te houden.

Zwak 'ownership'
Grote projecten worden meestal gesteund door verschillende bestuurders die als stakeholder er ieder een eigen agenda op nahouden. Deze bestuurders hebben elk andere verwachtingen van de voordelen van een project en de opties; soms gaan die niet hand in hand. Geen enkele bestuurder durft volledige verantwoordelijkheid voor het project te nemen en niemand treedt op bij het ontstaan van conflicten tussen stakeholders. Zwak 'ownership' resulteert in het missen van deadlines, gaten in de planning en het niet kunnen overkomen van obstakels omdat niemand verantwoordelijk is; projecten raken onbeheersbaar waardoor de kans op mislukking toeneemt.

Governance
Mensen accepteren te snel dat een gebrek aan betrokkenheid van hogere kaders de reden is voor het mislukken van een project. In de meeste grote projecten is het tegenovergestelde vaak het probleem; er is te veel bureaucratie.

Soms moeten beslissingen langs te veel mensen om goedgekeurd te worden of lopen de kosten uit de hand omdat er te veel mensen betrokken raken. In grotere organisaties hebben risicomanagers, compliance medewerkers, methodologie-experts en architecten veelal te maken met chefs en strengere eisen op gebied van governance.

Te veel nadenken
Projectmanagement is slachtoffer van de moderne neiging om vorm boven inhoud te verkiezen. Dit is een quote van een CIO die stelt dat er teveel wordt nagedacht:
'In het verleden spendeerden we tijd aan het oplossen van een probleem. We keken naar de verschillende mogelijkheden van aanpak en onderzochten de verschillende opties om een doelstelling te behalen.
We richtten ons op de behoeften en verwachtingen van de klant. We richtten ons op wat er afgeleverd moest worden. Tegenwoordig ligt de focus meer op de planning van hoe je het gaan doen, gekoppeld aan een fascinatie met methodologieën en standaarden. Het resultaat is dat we meer bezig zijn met de methodologie en aanpak van een project dan met het werken aan de requirements of aan de delivery. Het volume van de documentatie is sterk toegenomen. Nu ligt er altijd een plan, aanvullende risico-analyses, procesflows, summary tijdlijnen en allerlei soorten formulieren die laten zie wie wat wanneer waar gedaan heeft.
Dit is aanleiding voor veel meer officiële bijeenkomsten en heeft geleid tot de opkomst van een nieuw type projectmanager die zich vooral richt op documentatie en het plannen van vergaderingen – dit voegt vaak (onnodig) overhead toe, zowel op gebied van tijd als kosten. Een tweede consequentie is dat de werkpaarden naast hun reguliere werk ook een stapel formulieren moet invullen en bijhouden.'

De factor management
Een cruciale factor voor projecten groot en klein is projectmanagement (PM). Een certificaat voor PM meebrengen is één ding, maar de benodigde expertise en know-how hebben is minstens zo belangrijk.
Een projectmanager moet precies weten hoe hij de eisen aan een project combineert met goede governance. De projectmanager moet de juiste methodologie toepassen, op het juiste moment en in de juiste hoeveelheid. Kennis van zaken is van groot belang. De aanname dat een goede projectmanager ieder project tot een goed einde zou kunnen brengen is een misvatting.
Iets anders wat belangrijk is op te merken, is dat projecten nooit van de ene op de andere dag als mislukt beschouwd kunnen worden. Er is altijd sprake van een overgangsperiode waarin het project in zwaar weer verkeert. Als de PM in staat is door de bomen het bos te zien en de werkelijke problemen te identificeren, is er altijd nog een kans dat het project van de afgrond gered kan worden. Aangezien de mensen die bij het project betrokken zijn het liefst willen zien dat het project slaagt, is het niet gek dat zij soms de waarheid niet onder ogen willen zien. Het inzetten van externe reviewers om waarschuwingssignalen op te sporen en de sponsor ertoe te bewegen een corrigerende actie te maken, kunnen een project redden.

Think big, act small
Grote IT-projecten falen om verschillende redenen. Hoewel er verschillende manieren zijn om de bovengenoemde risico's te mitigeren, is er nog één laatste feit de moeite waard om op te merken: Uit onderzoek van de Standish Group blijkt dat kleinere projecten een hogere kans van slagen hebben (76 procent) dan grotere projecten (10 procent), onafhankelijk of ze zijn gebaseerd op de Agile of Waterfall-methode. Veel CIO's zweren er daarom bij om een project in kleinere stappen te voltooien om de uiteindelijke kans op positief resultaat te vergroten. Groot denken is niet erg, maar maak daarbij kleine stapjes.

Bijlage 3 Twaalf tips voor het beheersen van ICT-kosten (Bron: www.cio - Hemant Kogekar)

Er zijn drie zaken die ervoor zorgen dat de ICT-kosten binnen een organisatie toenemen:

- nieuwe vraag door veranderingen binnen de business;
- de vraag als gevolg van al eerder genomen besluiten;
- de consumptie van IT-diensten.

Tips voor het beheersen van dergelijke kosten zijn:

Nieuwe vraag door veranderingen binnen de business

1. Vraag of de veranderingen aan de business-kant meer waarde zullen creëren dan de kosten die ermee gemoeid zijn. Selecteer vervolgens alleen die veranderingen die daadwerkelijk flink wat kunnen opleveren. En betrek daarbij de ondersteuningskosten die door blijven lopen.
2. Kijk nogmaals kritisch naar voorstellen. De omvang en de risico's van een project kunnen in de loop van de tijd veranderen. Door op vaste tijden nogmaals projecten nogmaals onder de loep te nemen, is het mogelijk om onrendabele projecten tijdig te herkennen. Beperk de omvang, kijk of er extra inkomsten mee zijn te genereren en maak een einde aan projecten die onvoldoende doordacht blijken.
3. Kies voor 80-20-oplossingen. Probeer de duurste oplossingen te vermijden en vraag altijd naar alternatieve oplossingen. Als het mogelijk is om 80 procent van de gevraagde functionaliteit te leveren tegen 20 procent van de kosten, moet er wel een hele goede reden zijn om te kiezen voor de 100 procent-oplossing.
4. Maak gebruik van pilots. Doe eerst een test voordat u van start gaat met een compleet nieuw project. Dat is een goedkope manier om te kijken of u op de goede weg zit. Het is ook veel makkelijker om een proef te beëindigen dan een daadwerkelijk project.
5. Houd de kosten en inkomsten scherp in de gaten. Vraag hiervoor hulp van de financiële afdeling. En zorg ervoor dat alle kosten (ook de toekomstige) scherp in de gaten worden gehouden.

De vraag als gevolg van al eerder genomen besluiten

1. Achterhaalde features en applicaties. Werk samen met de gebruikers om achterhaalde features en onnodige producten op te sporen en vervolgens aan te passen of te beëindigen.
2. Shared services. Applicaties en diensten die dubbel worden aangeboden, maken de zaken complexer en zorgen ervoor dat de organisatie minder wendbaar is. Overweeg daarom gebruik te maken van shared services en virtualisatie.
3. Standaardisatie. Besluiten uit het verleden hebben mogelijk geleid tot een lappendeken van hardware, besturingssystemen en applicaties. Probeer te standaardiseren en de infrastructuur simpeler te maken.

De consumptie van ICT-diensten

1. Pas de servicelevels aan, gebaseerd op de werkelijke vraag. Maak duidelijk dat er een trade-off bestaat tussen servicelevels en kosten. Support die 24/7 beschikbaar is, is nu eenmaal duurder dan als er alleen tijdens werktijden ondersteuning hoeft te zijn.
2. Maak de business duidelijk wat de kosten van ICT zijn en wat gebruikers kunnen doen om die kosten binnen de perken te houden. Beperk het ICT-jargon en leg gebruikers duidelijk uit waar ze aan toe zijn.
3. Veel organisaties hebben ongebruikt materiaal (pc's, printers, software, servers) waarvoor kosten in rekening worden gebracht. Werk samen met de business om die verborgen kosten te ontdekken.
4. Maak accountmanagers verantwoordelijk voor ICT-beslissingen. Zorg ervoor dat zij de vraag rationaliseren en duplicatie tegengaan.

Bijlage 4 Information Technology Infrastructure Library (ITIL)

ITIL is ontwikkeld als een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie en kijkt vanuit de aanbodkant. Het is geen methode of model, maar eerder een reeks van best practices en concepten. Het resultaat van procesimplementatie met behulp van ITIL is vergelijkbaar met ISO 9000-regulering in de niet-ICT-branche, waarbij alle onderdelen van de organisatie zijn beschreven en in een bepaalde hiërarchie qua bevoegdheid/verantwoordelijkheid zijn gerangschikt.

ITIL versie 2 heeft de ICT-beheerprocessen ingedeeld in een achttal delen:

- Service Delivery:
  - Financial Management for IT Services (FMITS).
  - Capacity Management.
  - Availability Management.
  - IT Service Continuity Management (ITSCM).
  - Service Level Management.
  - Security Management.
- Service Support:
  - Change Management.
  - Release Management.
  - Problem Management.
  - Incident Management.
  - Configuration Management.
  - Service Desk.
- Planning to Implement Service Management.
- Security Management.
- ICT Infrastructure Management:
  - Network service Management.
  - Operations Management.
  - Management of local processors.
  - Computer installation and acceptance.
  - Systems Management.
- The Business Perspective.
- Application Management.
- Software Asset Management.

ITIL versie 3 richt zich op de complete Service Lifecycle. Daarnaast wordt een duidelijk klantgerichte benadering gehanteerd, vanuit een service en end-to-end perspectief. De Service Lifecycle wordt opgedeeld in 5 fases, die weer onderverdeeld worden in verschillende processen:

- Service Strategy:
  - Financial Management for IT-services.
  - Service Portfolio Management (SPM).
  - Demand Management.
  - Strategy Management for IT-services.
  - Business Relationship Management.

- Service Design:
  - Service Catalogue Management.
  - Service Level Management.
  - Capacity Management.
  - Availability Management.
  - IT Service Continuity Management (ITSCM).
  - Information Security Management.
  - Supplier Management.
  - Design Coordination.
- Service Transition:
  - Transition Planning and Support.
  - Change Management.
  - Service Asset and Configuration Management.
  - Release and Deployment Management.
  - Service Validation and Testing.
  - Change Evaluation.
  - Knowledge Management.
- Service Operation:
  - Event Management.
  - Incident Management.
  - Request Fulfilment.
  - Problem Management.
  - Access Management.
- Continual Service Improvement:
  - Seven Step Improvement Process.
- Service Operation (de enige fase waarbinnen (vier) functies gedefinieerd zijn):
  - Service Desk.
  - Technical Management.
  - Application Management.
  - IT Operations Management.

Beoogde voordelen van ITIL zijn:
- Verbetering in dienstverlenende organisatie door gebruik van de beste praktijkoplossingen.
- Verbetering in klanttevredenheid door een professioneler benadering.
- Standaardisering en begeleiding.
- Verhoging van de productiviteit.
- Verhoging van gebruik van ervaring en vaardigheden.

De beoogde voordelen worden soms niet bereikt. De belangrijkste redenen hiervoor zijn:
1. Onvoldoende oog voor de bedrijfscultuur.
2. Onvoldoende draagvlak bij het management en de medewerkers.
3. Te veel vasthouden aan procedures en documenten.

Geslaagde ITIL-implementaties zijn gebaseerd op een veranderkundige aanpak.

Bijlage 5 Application Services Library (ASL)

ASL is een procesraamwerk, ondersteund door best practices, dat de processen van het beheer, onderhoud en vernieuwing van informatiesystemen en applicaties beschrijft. ASL is een Nederlandse standaard in het publieke domein, beschikbaar voor iedere organisatie, en wordt beheerd door een stichting, die wordt ondersteund door een aantal grote ICT-bedrijven. Het biedt een handvat bij het verbeteren van organisaties, die applicatiebeheer uitvoeren. Door gebruik van best practices en diagnose-instrumenten, zoals zelfevaluaties, kan men pragmatisch aan de slag met het verbeteren van het applicatiebeheer. Specifiek voor ASL is de nadruk op de ontwikkelcyclus (onderhoud /vernieuwing).

ASL beschrijft de processen op uitvoerend (operationeel), sturend (tactisch) en richtinggevend (strategisch) niveau. Het kent zes clusters, met daarin processen.
Waar ITIL als beheermethodiek sterk gericht is op het beheren van IT-infrastructuren, legt ASL de nadruk op applicatiebeheer, op de processen rond het beheren en onderhouden van software en de gegevensbanken. De ITIL-processen zijn voor een groot deel binnen ASL terug te vinden, met name in de hoek van de beheerprocessen en de tactische processen.
ASL is een procesmodel. Dit houdt in dat de werkzaamheden in een bedrijf beschreven worden aan de hand van processen die niet noodzakelijkerwijs hoeven samen te vallen met afdelingen of personen met een bepaalde functie. Een proces omvat werkzaamheden die volgens het ASL-model bij elkaar horen. In de praktijk kan een afdeling meerdere processen uitvoeren en een proces kan door meerdere afdelingen uitgevoerd worden. ASL kent de volgende processen:

Beheerprocessen

Er zijn vijf beheerprocessen in ASL. Deze processen zijn belangrijk omdat ze het gebruik van de applicaties ondersteunen met zo weinig mogelijk middelen en zo weinig mogelijk applicatie-onderbrekingen. Al deze processen zijn ook gedefinieerd in ITIL maar omdat ze hier vanuit applicatiebeheer gedetailleerd zijn, kunnen de processen enigszins afwijken. De volgende beheerprocessen zijn te onderscheiden:

- Incidentbeheer.
- Configuratiebeheer.
- Beschikbaarheidsbeheer.
- Capaciteitsbeheer.
- Continuïteitsbeheer.

Onderhouds- en vernieuwingsprocessen

Men schat dat zo'n 80% van het werk binnen applicatiebeheer te maken heeft met onderhouds- en vernieuwingsprocessen. Omdat de bedrijfsprocessen die door applicaties ondersteund worden continu veranderen, moeten de applicaties mee veranderen. Voor elke verandering zullen de onderhouds- en vernieuwingsprocessen doorlopen moeten worden. In ITIL zijn deze processen niet terug te vinden. Het gaat om de volgende processen:

- Uitwerkingsanalyse.
- Ontwerp.
- Realisatie.
- Test.
- Implementatie.

Verbindende processen

De verbindende processen verbinden de hierboven genoemde beheersprocessen met de onderhouds- en vernieuwingsprocessen. Er zijn twee verbindende processen. Wijzigingsbeheer bepaalt de inhoud van releases en aan welke releases onderhouds- en vernieuwingsprocessen mogen werken.
Programmabeheer en distributie controleert de status van applicatiecomponenten en bepaalt welke applicatiecomponenten door de beheersprocessen gebruikt mogen worden. Het gaat om de volgende processen:

- Wijzigingsbeheer.
- Programmabeheer en distributie.

Sturende processen

Sturing is noodzakelijk om de hierboven genoemde processen optimaal te doen verlopen. Hierbij zijn vier aspecten van belang oplevertijd, kosten, kwaliteit voor de medewerker en kwaliteit voor de klant. Dit leidt tot de volgende processen:

- Planning en control.
- Kostenmanagement.
- Kwaliteitsmanagement.
- Servicelevel management.

Elk proces kent drie soorten activiteiten. Ten eerste moet er een plan opgesteld worden of afspraken gemaakt worden: een resource planning, budgettering, kwaliteitsplan of SLA. Vervolgens moet dit plan of deze afspraken bewaakt worden.

ACM-processen

De ACM-processen (Applications Cycle Management) zorgen voor een lange termijn strategie met betrekking tot de applicatie. Hierbij zijn drie zaken van belang: de technologische ontwikkelingen, de ontwikkelingen bij de gebruikers- of klantorganisatie en ontwikkelingen in de omgeving van gebruikers- of klantorganisatie (bijvoorbeeld bij bedrijven waarmee de gebruikersorganisatie samenwerkt). Deze zaken leiden tot een strategie met betrekking tot de toekomst van de applicatie, de bijbehorende benodigde onderhoudsacties en een strategie met betrekking tot de applicatieportfolio.

OCM-processen

De OCM-processen (Organization Cycle Management) zorgen voor een lange termijn strategie met betrekking tot de ICT-organisatie waarbinnen het applicatiebeheer plaatsvindt. Hierbij zijn de volgende zaken van belang: marktontwikkelingen, de gewenste benadering van de gebruikers- of klantorganisatie, de gewenste kennis en vaardigheden binnen de ICT-organisatie en de gewenste technologische middelen voor de ICT-organisatie. Deze zaken leiden tot een bepaling van de te leveren diensten op lange termijn.

De processen in detail:

Beheerprocessen

Incidentbeheer

Tijdens gebruik van applicaties kunnen storingen, vragen of wensen ontstaan. Deze worden als incident gemeld bij een helpdesk of servicedesk die onderdeel is van het proces incidentbeheer. Dit proces streeft een handhaving van de dienstverlening na, opdat voldaan wordt aan de afgesproken service levels. Ingewikkelde incidenten of vaak optredende incidenten worden als probleem doorgezet naar Kwaliteitsmanagement. Naast het reageren op incidenten wordt er ook proactief gehandeld, bijvoorbeeld door het communiceren van ontwikkelingen rond een bepaalde applicatie.

Configuratiebeheer

De applicaties en onderdelen daarvan en de afgesproken diensten en service levels moeten geadministreerd worden. Dit is de taak van configuratiebeheer. Ook wanneer iets op dit vlak wijzigt, moet er geadministreerd worden. De administratie wordt de CBDB (Configuratie Beheer DataBase) genoemd.

Beschikbaarheidsbeheer

Het is belangrijk dat een applicatie de afgesproken en gewenste functionaliteit kan bieden op de afgesproken tijden. Beschikbaarheidsbeheer zorgt hiervoor door het meten en rapporteren van beschikbaarheidsniveaus, het analyseren van eventuele tekortkomingen in de applicatie of het beheer, het initiëren van verbeteringen en het betrokken zijn bij nieuwe wijzigingen. Deze activiteiten en maatregelen worden in een beschikbaarheidsplan vastgelegd.

Capaciteitsbeheer

De middelen die een applicatie gebruikt zoals geheugenruimte, diskruimte en CPU-vermogen moeten optimaal worden ingezet. Het moment, de hoeveelheid en de kosten zijn hierbij belangrijke aspecten. Capaciteitsbeheer verricht metingen ten aanzien van de gevraagde en beschikbare capaciteit, analyseert de metingen, rapporteert hierover en neemt zo nodig maatregelen. Mogelijke maatregelen zijn het verschuiven of opdelen van verwerkingen, vergroten van de capaciteit en het optimaliseren van de prestaties. Deze activiteiten en maatregelen worden in een capaciteitsplan vastgelegd.

Continuïteitsbeheer

Alle maatregelen die moeten garanderen dat de applicaties en de dienstverlening ook op langere termijn kunnen blijven functioneren, vallen onder continuïteitsbeheer. Er dient tegen diverse bedreigingen beveiligd te worden. Het gaat om bedreigingen zoals: virussen, hackers, fraude, brand, overstroming. Ook dient men rekening te houden met het wegvallen van leveranciers van wie men afhankelijk is. Aangezien het om dure maatregelen gaat, zal men het risico tegen de kosten moeten afwegen. Deze activiteiten en maatregelen worden in een continuïteitsplan vastgelegd.

Onderhoud en Vernieuwing

Impactanalyse

Onderhoud van een applicatie begint altijd met het analyseren van de uitwerking van de gewenste wijzigingen. Het gaat daarbij om de inspanning die benodigd is om de wijziging te realiseren en de consequenties voor gebruikers(organisatie) en beheerders. Hiervoor is nodig dat duidelijk wordt welke onderdelen van de applicatie gewijzigd moeten worden en door wie de betrokken applicatie(vrijgaven) gebruikt worden. Op basis van deze informatie wordt ook bepaald wat de beste oplossingsrichting is voor de wijziging. Ook wordt nu al in kaart gebracht hoe er getest moet gaan worden. Tijdens deze fase is er veel overleg met Technisch en Functioneel beheer.

Ontwerp

Tijdens deze fase worden de gewenste wijzigingen in overleg met Functioneel Beheer uitgewerkt en eenduidig gespecificeerd. Onderdeel van deze specificatie is onder andere een functionele beschrijving van de te verwerken informatie, de gewenste bewerkingen en de gewenste output in de nieuwe situatie. Ook aan samenhang en volgorde dient aandacht besteed te worden. Voor het specificeren maakt men veelal gebruik van een functioneel ontwerp. Verder wordt er ook uitgewerkt hoe er na realisatie getest dient te worden.

Realisatie

Tijdens de realisatie wordt de functionele specificatie uit de vorige fase technisch uitgewerkt tot een technisch ontwerp. Vervolgens wordt er nader uitgewerkt en gebouwd. Het resultaat is een change package, de gewijzigde programmaonderdelen en databestanden. Ook ondergaan de gewijzigde delen een eerste test: de unit-test waarbij de delen afzonderlijk van elkaar getest worden. Een belangrijk aspect hierbij is het voorkomen van het opnieuw optreden van fouten die reeds bij eerdere releases eruit zijn gehaald.

Test

Om te voorkomen dat de wijzigingen tot fouten in de applicatie leiden en om te borgen dat de gewenste functionaliteit in de nieuwe release verwerkt is, moet er getest worden. Onderdeel van het proces *testen* zijn de volgende soort testen:

- Technische systeemtest (met betrekking tot opgestelde specificaties en onderhoudbaarheid van de software).
- Functionele systeemtest (met betrekking tot afgesproken functionaliteit en kwaliteit).
- (Ondersteuning van de) productietest door Technisch Beheer (met betrekking tot exploiteerbaarheid).

Zo mogelijk worden deze testen zo opgezet dat ze herbruikbaar zijn bij elke nieuwe release. Op die manier kan er efficiënt gewerkt worden. Om het testen nog meer gestructureerd aan te pakken zijn methoden ontwikkeld zoals TMAP en TestFrame. Deze methoden vallen niet onder ASL.

Implementatie

Anders dan het woord *implementatie* suggereert gaat het bij het proces implementatie niet om de daadwerkelijk implementatie van de nieuwe release in de productie omgeving. Deze actie wordt namelijk uitgevoerd door *technisch beheer* in samenwerking met *functioneel beheer* die de gebruikersondersteuning voor zijn rekening neemt. Wel ondersteunt dit proces *Technisch beheer* en *Functioneel* Beheer hierbij. Daarnaast sluit dit proces de release en de opdracht af na ontvangst van een verklaring van acceptatie opdrachtdecharge vanuit *Functioneel beheer*.

Verbindende processen

Wijzigingsbeheer

Diverse processen dienen wijzigingsverzoeken in bij *wijzigingsbeheer*. Deze wijzigingen worden vervolgens geregistreerd, geclusterd en ingepland in releases. Dit gebeurt in overleg met processen zoals *servicelevel management*, *functioneel beheer*, *planning en control* en *impactanalyse*. Vervolgens bewaakt dit proces uitvoering van het maken van een nieuwe release in de *onderhouds- en vernieuwingsprocessen*.

Programmabeheer en distributie

Dit proces moet voorkomen dat er ongeautoriseerde wijzigingen plaatsvinden. Wanneer in het Onderhouds- en vernieuwingsproces bepaalde applicatie onderdelen gewijzigd dienen te worden dan zal dat onderdeel eerst door dit proces ter beschikking gesteld moeten worden. Wanneer de applicatie in productie genomen moet worden dan zal dit proces voor de distributie zorgen zodat de juiste applicatie onderdelen operationeel gemaakt worden. Daarbij let dit proces onder andere op interferenties en overlappingen tussen verschillende parallel lopende vrijgaven.

Bijlage 6 Business Information Services Library (BISL)

BISL is een raamwerk voor het uitvoeren van functioneel beheer en informatiemanagement. Deze standaard richt zich, anders dan frameworks als ASL en ITIL, niet op ICT-organisaties (aanbod), maar juist op de gebruikersorganisatie (vraag). In dit raamwerk staat beschreven hoe een gebruikersorganisatie ervoor kan zorgen dat informatievoorziening adequaat werkt, hoe men behoeften in het bedrijfsproces vertaalt naar ICT-oplossingen en niet-ICT-oplossingen, hoe men de informatievoorziening en ICT-dienstverlening vanuit een gebruiksoptiek stuurt en hoe men de informatievoorziening op lange termijn vormgeeft. Het is derhalve voor alle organisaties bestemd. Het BiSL raamwerk omvat 23 taken op richtinggevend, sturend en uitvoerend niveau en wordt ondersteund door een aantal 'best practices', waarmee men invulling kan geven aan functioneel beheer en informatiemanagement binnen een organisatie. Het raamwerk wordt al door diverse grote Nederlandse organisaties gebruikt en toegepast en sluit aan op de proces frameworks ASL en ITIL.

Er zijn binnen BISL 7 procesclusters met bijbehorende processen, verdeeld over 3 niveaus:

Strategisch /Richtinggevend niveau

- Opstellen IV-organisatiestrategie (organisatie):
  - Relatiemanagement gebruikersorganisatie.
  - Strategie inrichting IV-functie.
  - Leveranciersmanagement.
  - Ketenpartners management.

- Verbindende processen (richtinggevend niveau):
  - Informatiecoördinatie.

- Opstellen informatiestrategie (vormgeving):
  - Informatie lifecycle management.
  - Informatie portfolio management.
  - Bepalen keten-ontwikkelingen.
  - Bepalen technologieontwikkelingen.
  - Bepalen bedrijfsprocesontwikkelingen.

Sturend niveau

- Sturende processen (management):
  - Planning en control.
  - Financieel management.
  - Behoeftemanagement.
  - Contractmanagement.

Uitvoerend niveau

- Gebruiksbeheer (organisatie):
  - Gebruikersondersteuning.
  - Operationele IT-aansturing.
  - Beheer bedrijfsinformatie.

- Verbindende processen (uitvoerend niveau):
  - Wijzigingenbeheer.
  - Transitie.

- Functionaliteitenbeheer (vormgeving):
  - Specificeren.
  - Vormgeven niet-geautomatiseerde IV.
  - Voorbereiden transitie.
  - Toetsen en testen.

Bijlage 7 The Open Group Architecture Framework (TOGAF)

The Open Group Architecture Framework (TOGAF) is een methode voor het ontwikkelen en beheren van de enterprise-architectuur. TOGAF is een open standaard. TOGAF bevat een verzameling aan technieken en best practices. Centraal in de methode staat de Architecture Development Method (ADM). Deze beschrijft de verschillende fasen van ontwikkeling en beheer van de enterprise-architectuur.

TOGAF kent 4 type architecturen:

- Business-architectuur - definieert strategie, beleid, organisatie en de belangrijkste werkprocessen binnen de organisatie;
- Applicatie architectuur - geeft een blauwdruk voor de te gebruiken individuele systemen, de interacties tussen de applicatiesystemen en hun relaties met de kernprocessen van de organisatie, waarbij de frameworks voor diensten als functies voor de integratie worden ingezet;
- Data architectuur - beschrijft de structuur van de logische- en fysieke data binnen de organisatie en de hierbij behorende datamanagementbronnen;
- Technische architectuur of technologie-architectuur - beschrijft de hardware, software en netwerk infrastructuur die nodig is om de organisatie-kritieke applicaties te ondersteunen.

Om deze architecturen te ontwikkelen is TOGAF onderverdeeld in drie onderdelen:

- ADM: Architecture Development Method;
- Enterprise Continuüm;
- Resource base.

De ADM is het hart van TOGAF. Het is een methode om architecturen te ontwikkelen. De methode bevat de volgende stappen:

- Preliminary phase: Frameworks en Principles
- A: Architecture Vision
- B: Business Architecture
- C: Information Systems Architecture
- D: Technology Architecture
- E: Opportunities and Solutions
- F: Migration Planning
- G: Implementation Governance
- H: Architecture Change Management

Elke stap bestaat uit weer een (groot) aantal kleinere stappen.
In principe worden alle stappen cyclisch doorlopen. Als in fase H tot de conclusie wordt gekomen dat er een wijziging in de architectuur moet komen, dan kan weer gestart worden in fase A.

Het Enterprise Continuum is een virtuele repository met alle architectuur assets (models, patterns, descriptions) van een bedrijf. In eerste instantie is dit een leeg raamwerk, dat gedurende de uitvoering van de ADM steeds verder gevuld wordt.

De basis voor een Enterprise Continuum kan de TOGAF foundation architecture zijn.
Deze bestaat uit:

- Technical Reference Model (TRM) - een algemeen model met meerdere lagen waarin systemen gemodelleerd kunnen worden;
- Standards Information Base (SIB) - een lijst met geaccepteerde standaarden die gebruikt kunnen worden;
- Integrated Information Infrastructure Reference Model (III_RM) - een model voor de ontwikkeling van applicatie architecturen.

Ook standaarden uit de industrie kunnen onderdeel uitmaken van het Enterprise Continuum.

De Resource base is een verzameling resources, guidelines, templates en achtergrondinformatie voor het gebruik van de ADM, waarin onder andere organisatorische aspecten van governance staan.

Bijlage 8 Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002

Dit boek is in eerste instantie ontwikkeld als studieboek voor het examen Information Security Foundation based on ISO/IEC27002 (ISFS) van EXIN. De tweede druk is een ingrijpende herziening van de eerste druk (uit 2010), waarbij de inhoud is aangepast aan de nieuwe versie van de standaards: ISO/IEC 27001:2013 en ISO/IEC 27002:2013. Dit boek is ook verkrijgbaar in een Engelstalige versie.

Het bevat de basiskennis die onmisbaar is voor iedereen die beroepsmatig betrokken is bij informatiebeveiliging of IT. In al deze gevallen is informatiebeveiliging van belang, al is het maar vanwege de beveiligingsmaatregelen die een organisatie genomen heeft.
Deze beveiligingsmaatregelen zijn soms afgedwongen door wet- en regelgeving.
De inhoud is afgestemd op de Nederlandse context, zonder de internationale samenhang van informatiebeveiliging uit het oog te verliezen. Informatietechnologie kent immers geen grenzen.

Kortom, dit boek is bedoeld voor iedereen die basiskennis van informatiebeveiliging op wil doen:
- Lijnmanagers die kennis moeten hebben van informatiebeveiliging omdat zij daarvoor binnen hun afdeling verantwoordelijk zijn.
- Directieleden en zelfstandigen zonder personeel omdat ook zij verantwoordelijk zijn voor het beschermen van de eigendommen en informatie die zij bezitten.
- Iedereen die thuis met computers werkt; ook dan is een bepaald gevoel van bewustwording belangrijk.

Inhoudsopgave: