Grondslagen IT-auditing

tweede druk

Redactie
Rob Fijneman
Edo Roos Lindgreen
Piet Veltman
Kai Hang Ho

ACADEMIC SERVICE

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:
Sdu Klantenservice
Postbus 20014
2500 EA Den Haag
tel.: (070) 378 98 80
www.sdu.nl/service

1e druk 2005
2e druk 2011

Zetwerk: Redactiebureau R. Heijer, Markelo
Omslagontwerp: Carlito's Design, Amsterdam

ISBN: 978 90 395 2626 2
NUR: 163/982

Inhoud

Dankwoord

Onze bijzondere dank gaat uit naar Cees Coumou en Ronald van Langen, die een bepalende bijdrage aan dit boek hebben geleverd. Daarnaast zijn wij Bart Verbrugge, Margo de Groot en Paul Post van Academic Service erkentelijk voor hun aanmoediging, geduld en ondersteuning bij de totstandkoming van dit boek.

Amstelveen, 29 oktober 2010

Rob Fijneman
Edo Roos Lindgreen
Piet Veltman
Kai Hang Ho

Inleiding

Ontwikkelingen op het gebied van informatietechnologie (IT) hebben sinds de Tweede Wereldoorlog een groot stempel op onze samenleving gedrukt. Zestig jaar geleden was het bouwen van een computer nog een reusachtig, eenmalig project. Machines als de Harvard Mark I en de ENIAC bestonden uit tienduizenden relais en buizen en verbruikten evenveel elektriciteit als een kleine woonwijk. De uitvinding van de transistor en de ontwikkeling van geïntegreerde circuits, waarbij grote aantallen transistoren op kleine siliciumchips worden geplaatst, maakten de productie van compacte, zuinige en goedkope computers mogelijk. Deze trend, die veertig jaar geleden werd ingezet, heeft geleid tot de technologie zoals wij die nu kennen. Op dit moment is informatietechnologie niet meer uit onze samenleving weg te denken. Informatietechnologie is een gebruiksgoed geworden. Elke organisatie gebruikt computers voor de ondersteuning of realisatie van haar primaire en secundaire bedrijfsprocessen; bijna elk individu heeft er dagelijks mee te maken; informatietechnologie is ingebed in talloze dagelijkse gebruiksvoorwerpen. Informatietechnologie vormt de basis voor wereldomspannende communicatienetwerken die onze samenleving de afgelopen tien jaar drastisch hebben veranderd. Deze ontwikkeling is nog lang niet voorbij, en de verwachting is gerechtvaardigd dat informatietechnologie ook de komende decennia een grote impact zal hebben.

De toename van het gebruik van informatietechnologie heeft ook geleid tot een toename van de bijbehorende risico's. Hierdoor is een groeiende behoefte aan zekerheid ontstaan bij de partijen die op de een of andere manier afhankelijk zijn van de technologie: gebruikers, afnemers, toezichthouders enzovoort. Ziehier de belangrijkste reden voor de bloei van het vakgebied IT-auditing, het onderwerp van dit boek. IT-auditing geeft belanghebbenden (*stakeholders*) zekerheid over de beheersing van aan informatietechnologie gerelateerde risico's en helpt ze deze risico's te beheersen.

Het vakgebied IT-auditing is voortgekomen uit de accountancy. In het begin van de jaren zeventig kreeg de accountant te maken met financiële systemen die in steeds verdergaande mate geautomatiseerd waren. Om zijn controletaak te kunnen uitvoeren, was inzicht in deze nieuwe administratieve omgevingen en de daarbij gebruikte technieken een noodzakelijke voorwaarde. Binnen het accountantsberoep ontstond een kleine groep deskundigen: accountants met verstand van Electronic Data Processing (EDP). Het vakgebied EDP-auditing was geboren.

EDP-auditors werden aanvankelijk vooral ingeschakeld om een uitspraak te kunnen doen over de betrouwbaarheid van de geautomatiseerde administratieve omgeving in het kader van de jaarrekeningcontrole (financial audit) en bij controles in opdracht van het management (operational audit). De voor het uitvoeren van deze taken benodigde deskundigheid bleek ook voor andere doeleinden zeer waardevol te zijn. Sinds het begin van de jaren tachtig worden EDP-auditors daarom in toenemende mate ingezet als controleur en adviseur bij complexe IT-vraagstukken op uiteenlopende gebieden. Bij het uitvoeren van die taken wordt steeds nieuwe kennis en ervaring opgedaan. Wat de

EDP-auditor daarbij onderscheidt van andere IT-deskundigen in de markt zijn kwaliteiten die voor een deel zijn te herleiden tot de afkomst van het vakgebied: onafhankelijkheid, onpartijdigheid en professionele integriteit.

In plaats van de term EDP-auditor wordt de laatste jaren meer de term IT-auditor gehanteerd. Deze naamsverandering heeft geen gevolgen voor het takenpakket van de beroepsgroep. De EDP-auditor van toen heeft zich ontwikkeld tot de IT-auditor van nu. Hoewel de accountantsachtergrond nog steeds goed merkbaar is, biedt de IT-auditor van nu een veel bredere dienstverlening. Een andere veelgebruikte term is Information Systems Auditor of IS-auditor. Ofschoon kan worden beargumenteerd dat een IS-audit een bredere scope heeft dan een IT-audit, worden beide termen in dit boek als synoniem beschouwd, waarbij omwille van de consistentie uitsluitend de term IT-auditor wordt gebezigd.

In de praktijk vervult de IT-auditor verschillende rollen. Soms is hij de specialist die de accountant of interne auditor ondersteunt bij zaken die specifieke deskundigheid op het gebied van informatietechnologie vereisen. Soms opereert hij zelf als interne auditor met kennis van bedrijfsprocessen en interne controle en daarnaast ook gedegen kennis van informatietechnologie. Maar steeds vaker opereert hij als zelfstandig IT-auditor, waarbij hij een oordeel geeft over specifieke kwaliteitsaspecten van de informatievoorziening of onderdelen daarvan dat door verscheidene stakeholders wordt gebruikt. De IT-auditor dient zich in elk van deze rollen thuis te voelen en steeds in staat te zijn kwalitatief hoogwaardig onderzoek uit te voeren. De IT-auditor beperkt zich daarbij niet tot het beoordelen van aspecten van informatietechnologie, maar geeft hierover ook gevraagd en ongevraagd advies (Fijneman, 2005).

Er kan onderscheid worden gemaakt tussen interne en externe IT-auditors. De interne IT-auditor maakt veelal deel uit van een interne accountantsdienst en kan zowel een bijdrage leveren aan financial audits als aan operational audits. De interne IT-auditor rapporteert via het hoofd van de interne accountantsdienst direct aan de Raad van Bestuur, de hoofddirectie van de organisatie en/of het audit-committee. Veel organisaties beschikken op dit moment over interne IT-auditors; niet alleen internationale ondernemingen, maar ook overheidsinstellingen, not-for-profit-organisaties en middelgrote ondernemingen hebben de toegevoegde waarde van de IT-auditor ontdekt. De externe IT-auditor is doorgaans werkzaam bij een accountantskantoor. De externe IT-auditor kan op verschillende manieren worden ingeschakeld. In sommige gevallen maakt hij deel uit van het controleteam dat verantwoordelijk is voor de jaarrekeningcontrole. In andere gevallen wordt de externe IT-auditor direct ingeschakeld. Mogelijke opdrachtgevers zijn de interne accountantsdienst of het lijnmanagement van de organisatie. Door het relatief grote aantal roulerende opdrachten kunnen externe kantoren specialisten in dienst nemen, die bij verschillende cliënten kunnen worden ingezet.

De IT-auditor is inmiddels uitgegroeid tot een gewaardeerde en invloedrijke speler in de arena van de informatietechnologie en speelt een belangrijke rol bij de borging van de beheerprocessen binnen organisaties. Veel IT-auditors stromen door naar andere posities binnen de organisatie.

De hoofdtaak van de IT-auditor is auditing: het uitvoeren van een onderzoek, het toetsen aan normen en het geven van een oordeel. Naast auditing rekent de IT-auditor ook tal van andere activiteiten tot zijn takenpakket. De belangrijkste daarvan is advisering. Voor de meeste opdrachtgevers is een oordeel niet genoeg; een aanvullend advies, waaruit blijkt hoe eventueel geconstateerde tekortkomingen kunnen worden opgelost, wordt in de regel zeer op prijs gesteld. Ten slotte houden IT-auditors zich bezig met zulke uiteenlopende activiteiten als organisatieadvies, beleidsvoorbereiding, certificering, due-diligenceonderzoeken, marktonderzoeken, communicatietrajecten, technische beveiligingstesten, benchmarks, pakketselectietrajecten, onderwijs, training en onderzoek.

Een audit heeft altijd betrekking op een specifiek onderwerp, het auditobject. Auditobjecten zijn informatiesystemen, onderdelen daarvan, of aan informatiesystemen gerelateerde entiteiten. Onder auditobjecten vallen zowel technische componenten als organisatorische processen. Het duidelijk afbakenen van het auditobject is essentieel om een auditopdracht naar behoren te kunnen uitvoeren. Bij een onduidelijke afbakening bestaat het risico dat het uiteindelijke resultaat van het onderzoek niet voldoet aan de verwachtingen van de opdrachtgever.

Voor elk van de auditobjecten kan de kwaliteit worden beoordeeld door één of meer kwaliteitsaspecten daarvan te toetsen aan specifieke criteria. In ons vakgebied bestaat helaas geen eenduidige, algemeen aanvaarde definitie van deze kwaliteitsaspecten. In de praktijk worden verschillende termen naast en door elkaar gebruikt. Vaak worden de volgende kwaliteitsaspecten onderkend: effectiviteit, efficiency, exclusiviteit, integriteit, controleerbaarheid, continuïteit en beheersbaarheid. Een andere indeling die veel wordt gebruikt, is het drietal vertrouwelijkheid, integriteit en beschikbaarheid. In overeenstemming met de dagelijkse praktijk van de IT-auditor zullen beide indelingen in dit boek naast elkaar worden gebruikt.

Voor het uitvoeren van een IT-audit is in de eerste plaats deskundigheid op het gebied van informatietechnologie vereist. Maar deskundigheid alleen is niet voldoende. Voor een goede IT-audit is meer nodig. De IT-auditor dient te voldoen aan een groot aantal regels en richtlijnen die onder meer zijn vastgelegd door nationale en internationale beroepsorganisaties. Zo moet hij een duidelijke opdrachtomschrijving opstellen, moet hij vooraf zijn aanpak en toetsingsnormen afstemmen en moet hij zijn bevindingen en conclusies goed onderbouwen. Bij persoonsgebonden onderzoeken is het van belang dat de IT-auditor hoor en wederhoor toepast. De auditor moet in staat zijn om bevindingen en conclusies op een heldere manier te presenteren, waarbij hij voorbereid moet zijn op lastige vragen die soms nog jaren na het onderzoek kunnen worden gesteld. Een goede IT-auditor gaat planmatig te werk en legt zijn werkzaamheden nauwkeurig vast in een duidelijk dossier, dat ook weer aan tal van eisen moet voldoen.

Kortom, IT-auditing is een vak waarvoor veel meer nodig is dan alleen inhoudelijke deskundigheid op het gebied van informatietechnologie. De belangrijkste beginselen daarvan komen in dit boek aan de orde.

De indeling van dit boek is als volgt.

Hoofdstuk 1 – Toepassingen van informatietechnologie
Dit hoofdstuk gaat in op belangrijkste beginselen en toepassingen van informatietechnologie. Allereerst behandelen we hoe informatietechnologie zich de afgelopen jaren heeft ontwikkeld. Daarna geven we een korte toelichting bij de werking en toepassing van informatietechnologie, waarbij we ingaan op de levenscyclus van informatiesystemen, de relatie tussen de vraagzijde en de aanbodzijde van IT en IT-diensten, de stakeholders die betrokken zijn bij het inzetten van informatietechnologie en hun behoefte aan zekerheid. Ten slotte behandelt het hoofdstuk de wijze waarop informatietechnologie zich de komende jaren naar verwachting zal ontwikkelen, onder meer op het gebied van standaardisatie, miniaturisering en mobiele communicatie.

Hoofdstuk 2 – Risico's van informatietechnologie
In dit hoofdstuk komen de risico's aan de orde die verbonden zijn aan het gebruik van informatietechnologie. Nadat is vastgesteld hoe wij tegen het begrip risico kunnen aankijken, geven we een overzicht van de manieren waarop risico's kunnen worden geclassificeerd. Vervolgens bespreken we op welke wijze risico's aan de orde komen in bekende standaarden op het gebied van corporate governance. Daarna gaan we in op de belangrijkste risico's rond informatietechnologie. Het hoofdstuk sluit af met een uiteenzetting over het proces van risicoanalyse.

Hoofdstuk 3 – Beheersing van informatietechnologie
Dit hoofdstuk behandelt de belangrijkste algemene beheersingsmaatregelen die een organisatie rond informatietechnologie kan treffen, uitgesplitst naar de verschillende fasen in de levenscyclus van informatiesystemen. Na een korte uiteenzetting over raamwerken voor beheersingsmaatregelen, waaronder COBIT, komen planning en organisatie, projectmanagement, het beheer van IT-omgevingen en informatiebeveiliging beknopt aan de orde.

Hoofdstuk 4 – Inleiding IT-auditing
In dit hoofdstuk brengen we de beginselen van IT-auditing aan de orde, toegepast op een aantal praktijksituaties. Zowel de theorie van IT-auditing als de aanpak van IT-auditing in de praktijk worden in de hierna volgende hoofdstukken verder uitgediept.

Hoofdstuk 5 – Beginselen van IT-auditing
In dit hoofdstuk gaan we in op de elementen van een IT-audit. Hiertoe behandelen we eerst wat IT-auditing inhoudt en hoe dit is ontstaan. Daarna kijken we naar de belangrijkste elementen van een IT-audit en geven een nadere uitwerking van de diverse begrippen uit de definitie van IT-auditing. Vervolgens gaan we in op het proces van een IT-audit en in het bijzonder op de rapportagefase.

Hoofdstuk 6 – Organisatie van IT-auditing
In dit hoofdstuk behandelen we de organisatie van IT-auditing. Wij gaan in op de verschillende beroepsorganisaties en hun taak en rol bij de professionalisering van het beroep van zowel externe als interne auditors. Ten slotte behandelen wij diverse nationale en internationale auditingstandaarden die beschikbaar zijn om een kwalitatief hoogwaardige audit te kunnen uitvoeren.

1 Toepassingen van informatietechnologie

Edo Roos Lindgreen

In dit hoofdstuk gaan we in op de belangrijkste toepassingen van informatietechnologie en de economische en maatschappelijke impact ervan. Hiertoe geven we eerst in grote lijnen aan wat informatietechnologie is, uit welke componenten informatiesystemen bestaan, en hoe de levenscyclus van een informatiesysteem eruitziet. Daarna kijken we naar de belangrijkste toepassingen van informatietechnologie. Vervolgens identificeren we de stakeholders: de partijen die op de een of andere manier een belang hebben bij een optimale inzet van informatietechnologie. Het hoofdstuk besluit met een verwachting over de wijze waarop informatietechnologie zich de komende jaren zal ontwikkelen.

Competentiedoelen

Na het bestuderen van dit hoofdstuk moet de lezer in staat zijn om aan te geven:

- wat informatietechnologie (IT) in grote lijnen is;
- voor welke toepassingen IT binnen organisaties wordt ingezet;
- hoe de levenscyclus van een informatiesysteem eruitziet;
- wat de relatie is tussen de vraagzijde en de aanbodzijde van IT en IT-diensten;
- wat de zakelijke en maatschappelijke impact van IT is;
- wie de stakeholders zijn bij het inzetten van IT;
- welke behoefte aan zekerheid er bij deze stakeholders bestaat;
- hoe IT zich de afgelopen decennia heeft ontwikkeld;
- hoe IT zich de komende jaren naar verwachting zal ontwikkelen, onder meer op het gebied van standaardisatie, miniaturisering en mobiele communicatie.

Computer doet bestelwerk AH

'De onvoorspelbaarheid van consumenten maakt bestellen voor een supermarkt tot een lastige zaak. Bij Albert Heijn neemt de computer het daarom over van het fingerspitzengefühl van de winkelier. Accuraat bestellen is vandaag de dag voor een supermarktmanager een complexe zaak en niet alleen door de explosieve toename van het aantal versproducten met een beperkte houdbaarheid van vier tot vijf dagen. De winkels zijn de afgelopen jaren een stuk groter en tellen al snel zo'n 15.000 verschillende artikelen, een verdubbeling in tien jaar. Tel daarbij op de impulsieve en veeleisende consument en de verstopte binnensteden en het is duidelijk waarom de retailers zelf van mening zijn dat de komende oorlog in hun sector aan de achterkant van de winkel wordt gewonnen. Albert Heijn maakt zich op voor de strijd door de logistiek verregaand te automatiseren. Acht jaar geleden is er een proces in gang gezet waarbij de bestelmacht geleidelijk verschuift van de winkel en het distributiecentrum naar een centrale

computer in Zaandam. Niet langer wachten op de dagelijkse bestelling van de winkelier, het is de kassascan die het systeem in beweging zet: feitelijk is het de klant die de bestelling doet.

Die ontwikkeling nadert bij AH zijn voltooiing. Nu al wordt een beperkt aantal producten (gebak, verse maaltijden) volautomatisch, zonder menselijke interventie aangeleverd. Het is de bedoeling om binnen enkele jaren de gehele winkel op deze wijze te vullen, én op basis van de beschikbare computerdata de schappen in te richten met producten die passen bij het consumptiepatroon van de buurt. Dat maatwerk is temeer van belang nu AH nieuwe winkeltypes opent, zoals non-food, snacks en de internetwinkel Albert. Voor ieder een eigen logistiek systeem bouwen is onbetaalbaar. Ook het grote verloop in de Randstad maakt computerhulp gewenst. 'Het is moeilijk om op die manier expertise op te bouwen. Mensen gaan bovendien op vakantie, hebben atv. Ook op die dagen wil ik een accurate bestelling en geen verschil op basis van de man of vrouw die toevallig op die afdeling staat.' Wat AH feitelijk doet is zoveel mogelijk afstappen van prognoses en op basis van elke transactie een bestelling doen. Minimale voorraden en maximale flexibiliteit. Om fabrikanten daarbij te helpen, gunt AH een klein aantal van hen (waaronder Heineken, Coca Cola, Vezet) een blik in de keuken: deze comakers krijgen toegang tot de Zaanse supercomputer. Vezet is AH's hofleverancier voor salades en versgesneden groente. Op topdagen verlaten zo'n half miljoen zakjes vers gesneden sla (levensduur vijf dagen) de verscentra in Warmenhuizen. Zaandam bestelt hier niet een keer per dag, maar smeert dat uit over vijf momenten waarbij Vezet de individuele bestellingen op zijn computer binnenkrijgt.' (Couwenberg, 2002)

1.1 Inleiding

Informatietechnologie is een integraal onderdeel van ons leven geworden. We maken er dagelijks gebruik van, vaak zonder erbij stil te staan. Kleine en grote organisaties kunnen niet meer zonder. Het openbare leven is ervan afhankelijk. Maar wat is informatietechnologie eigenlijk? Wat doen we er allemaal mee? Hoe gaan we ermee om? Hoeveel geven we eraan uit? Wat is de economische en maatschappelijke impact? En wat staat ons te wachten?

Het spreekt voor zich dat een goede IT-auditor het antwoord weet op deze vragen, zich bewust is van de context waarbinnen hij opereert, weet hoe belangrijk het onderwerp van zijn onderzoek voor zijn opdrachtgever is. Maar dat betekent niet dat de IT-auditor op de hoogte moet zijn van alle ins en outs van informatietechnologie. Dat kan ook niet meer. De technologie ontwikkelt zich zo snel, dat het nog maar weinigen gegeven is werkelijk alle details ervan te kennen. Toch is een elementair begrip van informatietechnologie en haar toepassingen wel noodzakelijk. Dit hoofdstuk biedt een algemene

beschrijving van informatietechnologie die de lezer voldoende houvast moet bieden om de rest van het boek te kunnen lezen.

Opdracht 1.1
Formuleer welke betekenis informatietechnologie voor uzelf heeft. Maak daarbij onderscheid tussen persoonlijke en zakelijke toepassingen.

1.2 Begrippenkader

Zoals in de inleiding werd vermeld, vormen informatiesystemen en onderdelen daarvan de belangrijkste objecten van een IT-audit. De meeste informatiesystemen laten zich goed beschrijven op basis van een gelaagd model, waarvoor de basis is gelegd door Parnas (1972).

Een *informatiesysteem* wordt hier gedefinieerd als een samenhangend en georganiseerd geheel aan hardware, software, documenten en de daarbij betrokken partijen, dat tot doel heeft het verzamelen, verwerken, produceren, opslaan en uitwisselen van informatie ten behoeve van specifieke bedrijfsprocessen en gebruikers. Het begrip informatie wordt hier niet nader gedefinieerd. Intuïtief bestaat informatie uit gegevens die een representatie vormen van feiten, gebeurtenissen, afbeeldingen, getallen, geluid, kennis enzovoort, en die worden opgeslagen, verwerkt en getransporteerd door middel van elektromagnetische signalen en toestanden. De term *informatievoorziening* wordt gebruikt om een verzameling relevante informatiesystemen aan te duiden.

De *hardware* bestaat uit de fysieke, elektronische, magnetische en optische componenten waaruit het informatiesysteem is opgebouwd, zoals computers, netwerken, randapparatuur en opslagmedia. Computers en randapparatuur bestaan op hun beurt weer uit kleinere componenten, zoals processors, geheugenchips, printplaten, voeding, vaste opslagmedia en netwerkinterfaces. Tot op de dag van vandaag zijn de meeste computersystemen gebaseerd op een hardwarearchitectuur die in 1945 werd ontwikkeld door de Amerikaanse wetenschapper John von Neumann.

De *software* is de programmatuur die nodig is om de hardware te laten doen wat hij moet doen. Software bestaat uit een binaire code die door het besturingssysteem in het geheugen kan worden geladen en door de processor kan worden uitgevoerd. Deze binaire code wordt verkregen door het vertalen van een programma dat is geschreven in een hogere programmeertaal, de broncode. De software van een informatiesysteem bestaat uit twee belangrijke onderdelen of lagen: het besturingssysteem en de applicatieprogrammatuur.

Het *besturingssysteem* stuurt de hardware aan en maakt het uitvoeren van applicatieprogrammatuur door die hardware mogelijk. Het besturingssysteem regelt onder meer de toewijzing van processortijd en geheugencapaciteit aan applicatieprogrammatuur en bevat daarnaast programmatuur om datacommunicatie mogelijk te maken. Het geheel aan hardware en besturingssystemen wordt aangeduid met de term *IT-infrastructuur.*

De *applicatieprogrammatuur* bepaalt de functionaliteit van het informatiesysteem; zij biedt specifieke functies aan eindgebruikers of aan andere programma's, maakt de invoer, verwerking, vastlegging en uitwisseling van gegevens mogelijk, enzovoort. Vaak maken verschillende applicatieprogramma's gebruik van gemeenschappelijke software voor databasebeheer, datacommunicatie of gegevensrepresentatie; zulke software wordt *middleware* genoemd. Koppelingen tussen verschillende applicaties om het uitwisselen van gegevens mogelijk te maken, heten *interfaces*.

De *documenten* in een informatiesysteem bestaan onder meer uit documentatie, handleidingen, beleid, richtlijnen en procedures voor het beheer en het gebruik van het informatiesysteem, zowel op papier als in elektronische vorm. Ook de invoer en uitvoer van een informatiesysteem behoren hiertoe.

De *betrokken partijen* die deel uitmaken van een informatiesysteem zijn de organisatieonderdelen en personen die het systeem gebruiken, maar ook de organisaties en personen die het systeem onderhouden en beheren of op een andere wijze bij het systeem betrokken zijn.

Tabel 1.1 *Componenten van een informatiesysteem, met voorbeelden*

Component	Voorbeelden
Hardware	Desktop, laptop, server, netwerk, interface
Besturingssysteem	Windows, Linux, Mac OS/X
Middleware	Oracle, SQL Server, filesysteem, communicatiesoftware
Applicatieprogrammatuur	SAP, Exact, Microsoft Office
Documenten	Systeemdocumentatie, beleid, richtlijnen, procedures
Betrokken partijen	Gebruiker, systeembeheerder, serviceorganisatie, IT-auditor

De ontwikkeling en het gebruik van informatiesystemen vinden in de regel plaats volgens een informatiestrategie en een informatieplan. Om de informatiesystemen operationeel te kunnen houden, dienen specifieke beheerprocessen te worden ingericht en bewaakt.

Opdracht 1.2
Welk van de informatiesystemen die u zakelijk gebruikt, is voor u het belangrijkst? Uit welke componenten bestaat dat informatiesysteem?

1.3 Soorten toepassingen

1.3.1 Overzicht

Van de computersystemen van een middelgrote bank tot het motormanagementsysteem in een auto, van gebitsfoto's bij de tandarts tot de laatste fantasyfilm in de bioscoop, van waterleiding tot breedbandaansluiting, van kinderbijslag tot pensioen: informatietechnologie is letterlijk overal. De toepassingen van informatietechnologie zijn te talrijk om hier uitgebreid, laat staan uitputtend te behandelen. Wij beperken ons in dit hoofdstuk tot een beknopt overzicht en concentreren ons daarbij op zakelijke toepassingen bij grote en middelgrote organisaties.

De meeste van deze organisaties maken gebruik van een groot aantal verschillende informatiesystemen – tientallen voor middelgrote organisaties, duizenden voor internationale organisaties. Die systemen kunnen bestaan uit standaardpakketten, zelf ontwikkelde applicaties en mengvormen daarvan, geleverd door een breed scala aan leveranciers. De onderliggende infrastructuur bestaat uit computers van uiteenlopende typen, zoals bureaucomputers, draagbare computers, handcomputers, servers en mainframes. Deze computers zijn onderling verbonden via netwerken die bestaan uit actieve netwerkapparatuur, zoals routers, hubs, switches en firewalls, en netwerkverbindingen, zoals koperdraad, glasvezel, draadloos en infrarood. Zelfs de informatiesystemen van kleine of middelgrote organisaties kunnen relatief complex zijn.

Neem als voorbeeld een zakenbank met tweehonderd medewerkers. Een bank van deze omvang gebruikt tientallen informatiesystemen, zoals een boekhoudsysteem, een treasurysysteem, een factureringssysteem, een aantal betalingssystemen, een kennissysteem, een systeem voor e-mail en agendabeheer, systemen voor het ontvangen van financiële informatie en een externe website.

Elk van deze systemen bestaat uit de in paragraaf 1.2 beschreven componenten. Neem bijvoorbeeld het boekhoudsysteem:

- *Betrokken partijen* – Het boekhoudsysteem wordt gebruikt door de afdeling Finance & Administration en wordt beheerd door de afdeling ICT.
- *Documenten* – Het boekhoudsysteem is gedocumenteerd en de bank beschikt over tal van richtlijnen en procedures die voorschrijven hoe medewerkers met het systeem moeten omgaan.
- *Applicatieprogrammatuur* – De applicatieprogrammatuur bestaat uit een standaardpakket van een grote leverancier, dat voor deze bank is aangepast. Zo zijn er interfaces ontwikkeld met andere applicaties van de bank.
- *IT-infrastructuur* – Het standaardpakket draait op een middelgrote server van leverancier IBM, met het besturingssysteem OS/400. De computer is net als alle andere computersystemen aangesloten op het interne netwerk van de bank. Daarnaast maakt de bank gebruik van een wereldwijd netwerk voor communicatie met vestigingen in het buitenland.

Ook voor de andere informatiesystemen van de bank is deze analyse te maken; zie tabel 1.2.

Tabel 1.2 *Voorbeeld van een overzicht van de informatiesystemen van een middelgrote bank. Voor alle systemen zijn documentatie, beleid, richtlijnen en procedures aanwezig; alle systemen worden beheerd door de IT-afdeling.*

Systeem	Gebruiker	Applicatie	Besturingssysteem	Hardware
Grootboek	F&A	Balance	OS/400	IBM iSeries 800
Treasury	Risk mgt	Eagle+	Solaris	Sun Fire V250
Facturering	Billing	Billsys	OS/400	IBM AS/400
Swift	Payments	Swift	Windows	HP ProLiant dl380
Intranet	Allen	Netscape	Linux	HP ProLiant dl380
E-mail	Allen	Lotus Notes	Linux	IBM xSeries 225
Reuters	Allen	Reuters	Windows	HP personal computer
Website	Clienten	Apache	Solaris	Sun Fire V250

1.3.2 Indeling van toepassingen

Bovenstaand voorbeeld geldt voor een middelgrote bank. Maar zoveel organisaties, zoveel toepassingen. Hoe houd je die uit elkaar? Een zeer bruikbaar instrument voor het rubriceren van informatiesystemen is het procesmodel. Op basis van een beschrijving van de verschillende primaire en secundaire bedrijfsprocessen binnen een organisatie (inkoop, verkoop, logistiek, financiën, enzovoort) kunnen de verschillende informatiesystemen binnen een organisatie in kaart worden gebracht.

Organisaties in dezelfde branche gebruiken in de regel min of meer dezelfde informatiesystemen. Binnen organisaties in verschillende branches kunnen zeer verschillende informatiesystemen worden aangetroffen. Zie tabel 1.3 voor een niet-uitputtende lijst voorbeelden. Merk op dat sommige toepassingen in meerdere categorieën thuishoren en dat verschillende categorieën in elkaar kunnen overvloeien.

Tabel 1.3 *Toepassingen van informatietechnologie (niet uitputtend), met voorbeelden*

Toepassing	Voorbeelden
Financieel	Boekhoudpakketten, betalingssystemen, treasurysystemen, consolidatie- en rapportagesystemen, factureringssystemen, systemen voor effectenverkeer
Administratief	Administratie van cliënten, relaties, debiteuren, orders, vastgoed, hypotheken
Managementinformatie	Systemen voor het genereren van managementinformatie, datawarehousing, consolidatie
Workflow	Systemen voor het automatiseren van werkprocessen bij administratieve bedrijven, systemen voor het digitaliseren en verwerken van documenten

Toepassing	Voorbeelden
Reservering	Reserveringssystemen voor luchtvaart, transport, hotels, vakantieparken, bioscopen
Matching	Systemen voor matching van vracht en transportcapaciteit, werkzoekenden en vacatures, aankooporders en verkooporders
Logistiek	Systemen voor distributie en voorraadbeheer, planningssystemen, systemen voor tracking en tracing van goederen
Inkoop	Systemen voor automatisch inkopen bij voorkeursleveranciers, systemen voor opvragen en vergelijken van prijzen bij inkoop van bulkgoederen en energie
Verkoop	Systeem voor verkopen aan andere ondernemingen (business-to-business), website voor verkoop aan consumenten via internet, systemen voor bijhouden van klantgegevens
Medisch	Elektronisch patiëntendossier, software voor MRI-scanner, ziekenhuisinformatiesystemen, medische databases
Wetenschappelijk	Modellering van natuurkundige, chemische, biologische, economische enz. processen, visualisatie van moleculaire structuren, simulatie
Educatief	Educatieve software, systemen voor het werken in groepen, onlinetrainingen
Militair	Systemen voor communicatie tussen militaire eenheden, software voor besturing van intelligente wapens, modellering van oorlogssituaties
Technisch	Software voor sterkteberekeningen, ontwerpsoftware, software voor geografische en geofysische modellering
Industrieel	Software voor besturing van programmeerbare machines in een fabriek, programmeerbare robots in productielijn
Beslissingsondersteuning	Expertsystemen voor het bepalen van de kredietwaardigheid van klanten, systemen voor het detecteren van frauduleuze creditcardtransacties
Kennis	Systemen voor het uitwisselen van kennis, intranettoepassingen, expertsystemen, diagnosesystemen
Ingebed	Chips met software in bankpas, camera, autosleutels, koelkast, geldautomaat, mobiele telefoon
Artistiek	Systemen voor grafisch ontwerp, compositie van muziek, visualisatie van architectuur, digitale studio's

Enkele van de systemen in tabel 1.3 zijn zogeheten procesbesturingssystemen. Deze systemen, die onder meer worden ingezet voor de besturing van apparaten en elektromechanische, elektrische en chemische processen, worden nog niet tot het werkgebied van de IT-auditor gerekend en komen in dit boek slechts beperkt aan de orde.

1.3.3 Recente ontwikkelingen

Wie kijkt naar de ontwikkeling van de automatisering sinds de jaren vijftig van de vorige eeuw, ziet achtereenvolgens de invoering van grote mainframes voor administratieve en technisch-wetenschappelijke toepassingen in de jaren vijftig en zestig, de opkomst van middelgrote systemen voor de ondersteuning van specifieke bedrijfsprocessen bij divisies of afdelingen in de jaren zeventig en de verspreiding van personal

computers, servers en netwerken in de jaren tachtig. De afgelopen vijftien jaar worden gekenmerkt door drie ontwikkelingen die vrijwel elke organisatie heeft doorgemaakt: de invoering van ERP-systemen, het toenemend gebruik van internet en de alomtegenwoordige toepassing van kantoorapplicaties (Roos Lindgreen, 2002).

ERP-systemen
De eerste ontwikkeling is de grootschalige invoering van systemen voor Enterprise Resource Planning (ERP), zoals SAP of Oracle. Deze systemen integreren een breed scala aan ondersteunende functies voor de meest uiteenlopende bedrijfsprocessen, zoals logistiek, boekhouding, personeelszaken, planning en productie. Kenmerkend voor ERP-systemen is dat zij gebaseerd zijn op één enkele database die kan bestaan uit duizenden tabellen en waarin alle relevante gegevens slechts één keer zijn opgeslagen. Dit heeft grote voordelen voor de efficiency, de uitwisselbaarheid en consistentie van informatie en informatieverwerking.

Internet
De tweede belangrijke ontwikkeling is het toenemend gebruik van internet als medium voor communicatie, verkoop, marketing en informatie-uitwisseling. Vrijwel alle organisaties zijn inmiddels op internet 'aanwezig' met websites waarmee consumenten of zakenpartners productinformatie kunnen opvragen, reserveringen kunnen maken, producten of diensten kunnen bestellen, enzovoort. Internet wordt in de meeste gevallen niet in plaats van, maar naast de traditionele communicatie-, marketing- en verkoopkanalen ingezet. Waar internet werkelijk een hoge vlucht heeft genomen, is in de communicatie tussen en het uitwisselen van informatie door particuliere gebruikers, al dan niet legaal. Het gebruik van internet brengt nieuwe risico's met zich mee en heeft mede hierdoor de behoefte aan zekerheid bij de diverse betrokken partijen verhoogd.

Kantoorapplicaties
De laatste ontwikkeling is het alomtegenwoordige gebruik van kantoorapplicaties, zoals tekstverwerkers, spreadsheets, tekenprogramma's, on-line-agenda's en natuurlijk e-mail. Deze toepassingen zijn zo algemeen ingeburgerd dat een nadere toelichting op deze plaats overbodig is. De afhankelijkheid van deze systemen is hoger dan vaak wordt gedacht. Zo blijkt e-mail voor veel organisaties een kritieke toepassing te zijn, die niet langer dan een of twee dagen uit de lucht mag zijn.

Naast deze algemene ontwikkelingen zijn er vele specifieke toepassingen die een hoge vlucht hebben genomen; zie de toepassingen in tabel 1.3, maar denk ook aan mobiele toepassingen, ingebedde systemen, en natuurlijk digitale fotografie, films en muziek. Ook de komende jaren zullen wij vele nieuwe toepassingen van informatietechnologie zien; zie paragraaf 1.8 voor een blik vooruit.

Opdracht 1.3
Bestudeer op internet de websites van drie belangrijke leveranciers van ERP-systemen en beschrijf in uw eigen woorden wat de functionaliteit van de aangeboden oplossingen is.

1.4 De levensfasen van een informatiesysteem

Een informatiesysteem kent verschillende levensfasen. In de ontwikkelingsfase wordt het systeem ontworpen en gebouwd. Hierna wordt het systeem in productie genomen en volgt de operationele fase, waarin het systeem wordt gebruikt, onderhouden en beheerd. Hieronder gaan wij kort op deze fasen in.

Ontwikkelingsfase
De ontwikkelingsfase van een informatiesysteem loopt van het allereerste prille idee tot het realiseren en in productie nemen van het systeem. Hierbij wordt een proces doorlopen dat overeenkomsten vertoont met veel andere ontwikkelactiviteiten: van een eerste idee komt men tot een definitiestudie, vervolgens wordt een globaal ontwerp gemaakt, daarna iets dat lijkt op een blauwdruk, waarna men volgens een proces van stapsgewijze verfijning komt tot een min of meer gedetailleerd systeemontwerp. Dit ontwerp wordt vervolgens omgezet in een werkend systeem, bijvoorbeeld door het aanschaffen, installeren en instellen van een standaardpakket, het integreren van standaardmodules, of het programmeren van een geheel nieuw maatwerksysteem. Tijdens deze fase – die wel de bouwfase wordt genoemd – worden testactiviteiten uitgevoerd om te controleren of het systeem werkt volgens de specificaties. Is het systeem eenmaal gereed, dan volgt de acceptatiefase. In deze fase wordt het systeem integraal getest en, indien het systeem akkoord wordt bevonden, formeel door de ontvangende partij geaccepteerd. Al deze activiteiten kunnen geheel of gedeeltelijk worden uitbesteed aan externe partijen. Voor het structureren van de ontwikkeling van een informatiesysteem bestaan verschillende methoden en technieken, waaronder System Development Methodology (SDM) en Rapid Application Development (RAD).

Operationele fase
Is de nieuwe toepassingsprogrammatuur eenmaal geaccepteerd door de ontvangende partij, dan kan het systeem in productie worden genomen. Hiermee begint de operationele fase. Na de nodige training en opleiding van de toekomstige gebruikers en het aanpassen van de werkprocessen binnen de organisatie kan het systeem door de organisatie in gebruik worden genomen. Dit gaat in de meeste gevallen gepaard met aanloopproblemen en kinderziektes; om die reden wordt bij veel invoeringstrajecten gedurende een korte tijd een periode ingesteld waarin extra capaciteit beschikbaar is om vragen van gebruikers te beantwoorden en problemen op te lossen. Daarna komt het systeem doorgaans in een stabiele gebruiksfase, die jaren kan duren. Belangrijke activiteiten tijdens deze fase zijn het onderhoud en het beheer van het systeem. Het onderhoud omvat het oplossen van problemen en het aanbrengen van wijzigingen en uitbreidingen in het systeem. Bij het beheer wordt wel onderscheid gemaakt tussen het functioneel beheer en het technisch beheer. Het functioneel beheer omvat alle activiteiten die nodig zijn voor het beschikbaar stellen van de functionaliteit van het informatiesysteem: het toewijzen van functies aan gebruikers, het inrichten van autorisaties en het indienen van aanvragen om wijzigingen of uitbreidingen in het systeem aan te brengen. Het technisch beheer omvat alle technische activiteiten die nodig zijn om het systeem volgens de eisen van de gebruikers beschikbaar te stellen. Denk hierbij aan zaken als het bijhouden en doorvoeren van wijzigingen en uitbreidingen, het instal-

leren van nieuwe versies, het daadwerkelijk configureren van het systeem, het wijzigen van systeeminstellingen en het maken van back-ups.

Naast de toepassingsprogrammatuur moeten ook de andere componenten van het informatiesysteem worden beheerd. Een belangrijk onderdeel hierbij is de IT-infrastructuur: de netwerken, servers, besturingssystemen en andere componenten waarop de toepassingsprogrammatuur draait.

Voor het inrichten van beheersactiviteiten maken veel organisaties tegenwoordig gebruik van standaarden. De bekendste hiervan in Europa is de Information Technology Infrastructure Library (ITIL). Deze standaard definieert een groot aantal organisatorische processen die noodzakelijk worden geacht voor het beheer van informatiesystemen. Deze processen hebben betrekking op onderwerpen als het formuleren van beleid, het aanvragen en verwerken van wijzigingen (change management), het plannen van systeemcapaciteit (capacity management), informatiebeveiliging (security management), het waarborgen van de beschikbaarheid van het systeem (availability management), het bijhouden van de componenten van het informatiesysteem (configuration management) en de dagelijkse bediening van de systemen (operations management). Meer over dit onderwerp in hoofdstuk 3.

Ontwikkeling, onderhoud en beheer worden in veel gevallen uitbesteed aan externe partijen. Het beheer van de applicatieprogrammatuur en onderdelen van de infrastructuur kan daarbij worden uitbesteed aan verschillende serviceorganisaties. Daarbij leggen de afnemer en de serviceorganisatie in de regel afspraken vast over het gewenste niveau van dienstverlening in zogeheten Service Level Agreements (SLA's), waarin zaken aan de orde komen als responsietijd, minimumniveau van beschikbaarheid, onderhoudstijden, beveiliging en de beschikbaarheid van de serviceorganisatie bij het aanmelden en afhandelen van problemen.

Om deze zaken in goede banen te leiden, hebben veel organisaties een functie ingericht die informatiemanagement wordt genoemd. De informatiemanager representeert de vraagzijde: de afdelingen en medewerkers die informatietechnologie gebruiken. Tot de taken van de informatiemanager horen onder meer het formuleren van informatiebeleid, het opstellen van eisen en wensen ten aanzien van informatiesystemen, het opstellen van een informatieplan en de daaruit voortvloeiende begrotingen en investeringsplannen, het mede opstellen van SLA's, het opstellen van richtlijnen en procedures, en het bewaken van de naleving van de gemaakte afspraken. In veel gevallen is de verantwoordelijkheid voor informatietechnologie belegd binnen de directie of Raad van Bestuur, in sommige gevallen zelfs bij een speciaal hiertoe aangesteld directielid, de Chief Information Officer (CIO).

Opdracht 1.4

a Geef aan waarom 'betrokkenheid van de gebruiker' en 'commitment van het topmanagement' kritieke succesfactoren zijn voor het slagen van een automatiseringsproject en bedenk zelf nog twee van zulke factoren.

b Geef aan waarom een zorgvuldige registratie van de automatiseringsmiddelen (configuration management) en een zorgvuldige verwerking van wijzigingen in het informatiesysteem (change management) noodzakelijke voorwaarden zijn voor een goede beveiliging (security management).

1.5 Waarom organisaties investeren in informatietechnologie

Exacte cijfers zijn niet te geven, maar veel organisaties besteden tussen de 3 en 10% van hun omzet aan informatietechnologie, onder meer aan licenties, hardware, personeel en aan informatietechnologie gerelateerde dienstverlening. Er zijn vele redenen voor organisaties om in informatietechnologie te investeren. Dat kunnen *externe redenen* zijn, zoals de wens om nieuwe producten of diensten te leveren, nieuwe verkoopkanalen aan te boren, de klant beter te kunnen bedienen, een profiel van de klant op te bouwen om beter op diens wensen te kunnen inspelen of gerichte marketing te kunnen bedrijven, de kwaliteit van de dienstverlening te verhogen, deel te gaan uitmaken van een distributieketen of bijvoorbeeld te voldoen aan de eisen van een wetgever of toezichthouder. Er zijn ook *interne redenen*, zoals de wens om de efficiency te verbeteren, kosten te verlagen, bedrijfsprocessen te stroomlijnen, de capaciteit van de bedrijfsvoering te verhogen, kennis binnen de organisatie te delen, de managementinformatie te verbeteren, voorraden terug te dringen, interne beheersingsmaatregelen te versterken, noodzakelijke veranderingen door te voeren of allerlei problemen op te lossen. Tabel 1.4 en 1.5 bevatten een overzicht van vaak voorkomende externe en interne redenen om te investeren in informatietechnologie, met voorbeelden.

Tabel 1.4 *Extern georiënteerde redenen om te investeren in informatietechnologie*

Reden	Voorbeeld
Nieuwe producten of diensten	Online juridisch advies op abonnementsbasis
Nieuwe verkoopkanalen	Verkoop boeken via internet
Klant beter bedienen	Website voor werkzoekenden
Klantprofiel opbouwen	Loyalty managementprogramma inrichten
Kwaliteit dienstverlening verhogen	Call center met online-clientdossiers
Deel uitmaken van distributieketen	Aansluiten op grote afnemers met nieuw systeem
Voldoen aan eisen wetgever	Aanpassen systeem voor boekhoudstandaard

Tabel 1.5 *Intern georiënteerde redenen om te investeren in informatietechnologie*

Reden	Voorbeeld
Efficiency verbeteren	Systeem voor online-urenregistratie
Kosten verlagen	Systeem voor automatische afhandeling claims
Processen stroomlijnen	Workflowmanagementsysteem bij verzekeraar

Reden	Voorbeeld
Capaciteit verhogen	Matching van werkzoekenden en vacatures
Kennis delen	Wereldwijd intranet
Managementinformatie verbeteren	Datawarehousing met tools voor eindgebruiker
Voorraden terugdringen	ERP-systeem t.b.v. just-in-time delivery
Interne controle versterken	Systeem voor identiteitsmanagement
Veranderingen doorvoeren	Systeem voor afdwingen uniforme werkprocessen
IT-problemen oplossen	Upgraden van de netwerkinfrastructuur

Investeringen in informatietechnologie zouden altijd in lijn moeten zijn met de strategische doelstellingen van de organisatie (strategic alignment) en de behoeften van de bedrijfsprocessen (business alignment). Een bekend model hiervoor is ontwikkeld door Henderson en Venkatraman (1992) en verder verfijnd door Abcouwer, Maes en Truijens (1997). In de praktijk zijn strategic alignment en business alignment nooit volledig gewaarborgd, mede als gevolg van veranderingen in strategie en bedrijfsvoering die gelijktijdig kunnen optreden met technologische ontwikkelingen.

Daar komt bij dat investeringen in informatietechnologie niet alleen het gevolg zijn van een rationeel, bewust besluitvormingsproces, waarbij kosten en opbrengsten klinisch tegen elkaar worden afgewogen. De praktijk leert dat vele andere factoren een rol spelen bij het nemen van dergelijke investeringsbeslissingen. Voorbeelden van zulke factoren zijn:

- emoties, zoals de angst om achter te blijven bij de concurrent, of enthousiasme voor een bepaalde oplossing;
- menselijke drijfveren, zoals de wens zich te onderscheiden of zich te bewijzen;
- groepsprocessen, waarbij de leden van een groep elkaars beslissing beïnvloeden;
- politieke omstandigheden, waarbij een investering deel uitmaakt van de politieke agenda.

Simon (1983) noemt het de theorie van begrensde rationaliteit: mensen nemen geen beslissingen door zuiver rationeel alle mogelijke alternatieven en de implicaties daarvan tegen elkaar af te wegen, maar door hun aandacht op een begrensd deel van de werkelijkheid te richten, allerlei onzekerheden voor lief te nemen, en zich niet alleen te laten beïnvloeden door feiten en logica, maar ook door intuïtie en emoties.

Veel organisaties hebben ondervonden dat het doen van een investering in informatietechnologie het begin is van een spiraal van verdere investeringen. Een voorbeeld is het voortdurend upgraden van besturingssystemen en applicaties. Stel, een bedrijf schaft na een zorgvuldig selectietraject een goed werkend softwarepakket aan dat de bedrijfsprocessen optimaal ondersteunt. Kan deze applicatie tot in lengte van dagen blijven draaien? Helaas niet. De leverancier van de applicatie zal steeds nieuwe versies op de markt brengen om omzet te blijven genereren en de oude versie na verloop van tijd niet meer ondersteunen. Afnemers worden zo gedwongen de nieuwe versie aan te schaffen.