Inleiding ict-auditing

JAN VAN PRAAT EN HANS SUERINK

ACADEMIC SERVICE

zesde druk

Inleiding ICT-auditing

zesde druk

Jan van Praat en Hans Suerink

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 1992
2e druk 1994
3e druk 1998
4e druk 2001
5e druk 2004
6e druk 2013

Zetwerk: Redactiebureau Ron Heijer, Markelo
Omslagontwerp: Studio Bassa, Culemborg
Omslaguitvoering: Carlito's Design, Amsterdam

ISBN 978 90 395 2712 2
NUR 982

Voorwoord

Bij de zesde druk
Met de vijfde druk kozen wij voor een volledig nieuwe en gewijzigde opzet van het boek *Inleiding EDP-auditing*. De titel van het leerboek bleef hetzelfde. Bij deze zesde druk is de titel ruim twintig jaar na de eerste druk gewijzigd in *Inleiding ICT-auditing*.

De NOREA noemt zichzelf de beroepsorganisatie van IT-auditors. Wij zijn van mening dat niet alleen de informatietechnologie object van onderzoek is, maar dat tevens kennis van de communicatietechnologie essentieel is voor ons vakgebied. Vandaar onze keuze voor ICT-auditing.

Als u in dit boek de term EDP-auditor (EDP staat voor Electronic Data Processing) tegenkomt, is dit nagenoeg altijd in combinatie met Register – de RE-titel die leden van NOREA dragen. Als u de term IT-auditor tegenkomt, is het nagenoeg altijd in een uiting van NOREA.

In het eerste deel wordt, zoals u van ons gewend bent, uitgebreid ingegaan op het begrip auditing. Hierbij wordt tevens, veel meer dan in de vorige drukken, ingegaan op de meer formele aspecten van de auditfunctie, zoals die vastgelegd is in de reglementen, de richtlijnen en de aanbevelingen van ISACA en de NOREA.

In het tweede deel worden de objecten van de ICT-auditor uitgebreid aan de orde gesteld. Hierbij is de opzet in principe hetzelfde gebleven; er is nog steeds sprake van de begripsbepaling – wat is het auditobject en welke norm is van toepassing– en beheersing – welke maatregelen moet de organisatie treffen voor de handhaving van de kwaliteit en de auditactiviteiten. In het kader van de audit wordt conform het proces van normconcretisering veelal weer onderscheid gemaakt tussen de beoordeling van de opzet, het bestaan en de werking. Ook zijn er meer algemeen aanvaarde normen beschikbaar gekomen die leidend zijn geweest bij de uitwerking van de objecten. Met name ITIL, ISAE 3402, PRINCE2 en NEN ISO 27001 hebben een belangrijke rol gespeeld.

December 2012,
Jan van Praat
Hans Suerink

Inhoud

1 Inleiding 1
1.1 Definities 1
1.2 Het eerste deel 2
1.3 Het tweede deel 4

Deel 1

2 De organisatie van het beroep 7
2.1 Nederlandse Orde van Register EDP-auditors 7
2.1.1 Doelstellingen van de Orde 8
2.1.2 De Register EDP-auditor en de andere leden van de Orde 8
2.1.3 De organen van de Orde 11
2.2 Regelgeving 12
2.3 ISACA 13
2.4 International Federation of Accountants (IFAC) 14

3 De houding van de auditor 15
3.1 De deskundigheid 15
3.2 Bestuurlijke informatievoorziening en organisatiekunde 16
3.2.1 Organisatiekunde 18
3.2.2 Bestuurlijke informatievoorziening uitgewerkt 21
3.2.3 Afhankelijkheids- en kwetsbaarheidsanalyse 25
3.2.4 Afhankelijkheidsanalyse 28
3.2.5 Kwetsbaarheidsanalyse 31
3.3 Onpartijdigheid en onafhankelijkheid 35
3.3.1 ICT-auditgrondslagen 36
3.3.2 Het Reglement Gedragscode Register IT-auditors ('Code of Ethics') 36
3.3.3 Het Reglement Beroepsbeoefening Register IT-auditors 38
3.3.4 Samenwerking tussen auditors en andere deskundigen 39
3.3.5 Het kwaliteitssysteem – Reglement Kwaliteitsbeheersing NOREA (RKBN) 39
3.3.6 Opdrachtgerichte kwaliteitsbeoordeling RKBN artikel 20 en verder 41

4 Het auditproces 43
4.1 Inleiding 43
4.2 Het doel van de opdracht 44
4.3 Verantwoordelijkheid van de ICT-auditor 45
4.4 De verantwoordelijkheden van de opdrachtgever 46

4.5 De reikwijdte (scope) van de opdracht 46
4.6 De onderzoeksperiode 47
4.7 De (kwaliteits)aspecten 47
4.8 De context waarbinnen de opdracht plaatsvindt 48
4.8.1 De belangen van de opdrachtgever 48
4.8.2 Aanwezigheid van bijzondere omstandigheden 48
4.8.3 De fundamentele beginselen 49
4.9 De te hanteren normering 49
4.9.1 Toetsingsnormen 50
4.9.2 Uitvoeringsnormen 50
4.10 De gewenste betrouwbaarheid evenals de bij het onderzoek te hanteren toleranties 50
4.10.1 Tolerantie 51
4.10.2 Betrouwbaarheid 52
4.10.3 De statistische steekproef 53
4.11 De aanpak 61
4.12 De doelgroep 62
4.13 De vorm en wijze van rapporteren 63
4.14 De beschikbaarheid van documentatie en medewerkers van de opdrachtgever 64

5 Het auditbewijsmateriaal 65
5.1 De auditmiddelen en -technieken 65
5.1.1 Het auditplan 66
5.1.2 Inlichtingen van gecontroleerde 67
5.1.3 Bewijsstukken en overige vastleggingen 68
5.1.4 Eigen waarnemingen 69
5.2 Het gebruik van Computer Assisted Audit Techniques 70
5.2.1 Voorbereiding en afronding van een audit 71
5.2.2 Uitvoering van een audit 72
5.3 De toereikende inzet van auditmiddelen en -technieken 73
5.4 De dossiervorming van de auditor 75

6 Concluderen en rapporteren 79
6.1 Formuleren van conclusies 79
6.2 Risicoanalyse 80
6.2.1 Relatie tussen risico's en beheersingsmaatregelen 84
6.2.2 Het proces van concluderen door de auditor 87
6.3 Assurancerapporten 87
6.3.1 Algemene eisen aan auditrapporten 87
6.3.2 Direct reporting en assertion based reporting 90
6.3.3 Voorbeeld van een Goedkeurend oordeel direct reporting (redelijke mate van zekerheid) 91
6.3.4 Voorbeeld van een Goedkeurend oordeel assertion based (redelijke mate van zekerheid) 93

7 De auditcriteria 95
7.1 Het kwaliteitsdenken 95
7.2 Normen voor de ICT-auditor 100
7.2.1 Capability Maturity Model 101
7.2.2 Code voor Informatiebeveiliging NEN/ISO 17799:2005 102
7.2.3 Control Objectives for Information and related Technology (COBIT5) 104
7.2.4 Information Technology Infrastructure Library (ITIL.V3) 106
7.2.5 Het Clark/Wilson-model 107
7.2.6 Richtlijn 3402 109

Deel 2

8 Organisatie van de informatievoorziening 115
8.1 Eisen met betrekking tot organisatie van de informatievoorziening 115
8.2 Strategiebepaling voor de organisatie van de informatievoorziening (application management) 116
8.3 Van strategie tot uitvoering 117
8.4 Inrichten van de bedrijfsprocessen 119
8.5 Realiseren van projecten 120
8.6 Wet- en regelgeving met betrekking tot de informatievoorziening 121
8.7 Aanpak van het onderzoek naar de organisatie van de informatie-voorziening 122
8.7.1 Beoordeling van de opzet 122
8.7.2 Beoordeling van het bestaan 123
8.7.3 Beoordeling van de werking 123

9 Informatiesystemen en systeemontwikkeling 125
9.1 Projecten 125
9.2 De organisatie binnen de implementatiecyclus 127
9.3 Projectbestuur 129
9.4 Kwaliteitsbeheersing 131
9.5 Systeemontwikkelmethoden 132
9.6 Projects in Controlled Environments (PRINCE2) 133
9.7 Systeemontwikkelproces 142
9.7.1 Maatwerk of standaardprogrammatuur 143
9.7.2 De invoering van een ERP-systeem 145
9.7.3 Pakketimplementatie 146
9.8 Systeemontwikkelcycli 153
9.8.1 De watervalmethode 153
9.8.2 Agile systeemontwikkeling 157
9.8.3 Prototyping 158
9.8.4 Rapid Application Development 159
9.8.5 End User Development 160
9.9 Testen 164

9.10 Ontwikkelen 166
9.10.1 De datageoriënteerde benadering (data-oriented development) 166
9.10.2 De objectgeoriënteerde benadering (object-oriented development) 168
9.10.3 De webgeoriënteerde benadering (web-based development) 169
9.11 De audit van de organisatiestructuur van de systeemontwikkeling 170
9.11.1 Structuur van de organisatie van de systeemontwikkeling 173
9.12 De audit van het bestaan – procesgericht 175
9.13 Beoordeling van de werking – productgericht 176

10 Technische infrastructuur 181
10.1 De organisatie van het beheer van de technische infrastructuur 181
10.1.1 Inventarisatie en analyse 182
10.1.2 Functiescheidingen 183
10.1.3 Inrichting van het systeembeheer 183
10.1.4 Besturing van het systeembeheer 188
10.2 De beoordeling van de organisatie van het beheer van de technische infrastructuur 189
10.3 De processen met betrekking tot het beheer van de technische infrastructuur 190
10.3.1 Dienstniveaubeheer 191
10.3.2 Configuratiebeheer 193
10.3.3 Capaciteitsbeheer 195
10.3.4 Calamiteitenbeheer 196
10.3.5 Beschikbaarheidsbeheer 196
10.3.6 Financieel beheer 197
10.3.7 Programmatuurbeheer en distributie 198
10.3.8 Incidentenbeheer 198
10.3.9 Probleembeheer 200
10.3.10 Wijzigingenbeheer 200
10.4 Beoordeling van de processen met betrekking tot het beheer van de technische infrastructuur 202
10.4.1 Beoordeling van de opzet 202
10.4.2 Beoordeling van het bestaan 209
10.4.3 Beoordeling van de werking 211
10.5 De producten van de technische infrastructuur 212
10.6 Besturingssystemen 213
10.6.1 Begripsbepaling 214
10.6.2 Beoordeling van besturingssystemen 215
10.7 Databasemanagementsystemen 216
10.7.1 Beheersingsaspecten rond databasemanagementsystemen 218
10.7.2 Beoordeling van de databaseomgeving 222
10.8 Datacommunicatie 224
10.8.1 Begripsbepaling 224
10.8.2 Beheersingsaspecten rond datacommunicatie 226
10.8.3 Beoordeling van de datacommunicatie 230

11 Informatiebeveiliging 233
11.1 Belang van informatiebeveiliging 233
11.2 Externe beveiliging 236
11.2.1 Identificatie 238
11.2.2 Authenticatie 240
11.2.3 Autorisatie 242
11.2.4 Rapportering 243
11.3 Organisatie met betrekking tot de toegangsbeveiliging 244
11.3.1 Beveiligingsbeleid en -plan 244
11.3.2 Aandacht management 246
11.4 Fysieke beveiliging 247
11.4.1 Actieplan 248
11.4.2 Back-upplan 249
11.4.3 Reconstructieplan 249
11.5 Aanpak van het onderzoek 253
11.5.1 Beoordeling van de opzet 253
11.5.2 Beoordeling van het bestaan 255
11.5.3 Beoordeling van de werking 256

Literatuur 259

Index 263

Hoofdstuk 1

Inleiding

In dit boek wordt uitgebreid aandacht besteed aan het vakgebied ICT-auditing (ICT = informatie- en communicatietechnologie). In dit hoofdstuk wordt eerst ingegaan op de definitie van ICT-auditing, waarna de kaders worden uitgezet voor de verdere inhoud van het boek. Het boek bestaat uit twee delen. In het eerste deel wordt eerst het vakgebied auditing nader uitgewerkt. Hierbij wordt onder andere aandacht besteed aan de aanpak van een audit en de meer formele aspecten van ICT-auditing. Dit betekent dat met name de beroepsorganisatie aan de orde wordt gesteld, alsmede de regelgeving die op het vakgebied ICT-auditing van toepassing is. In het tweede deel wordt ICT-auditing toegepast. De objecten die in het kader van ICT-auditing van belang zijn, worden systematisch uitgewerkt, waarbij aandacht wordt besteed aan de beoordeling van de organisatorische aspecten, de beoordeling van informatiesystemen en de beoordeling van de technische infrastructuur. Het boek wordt afgesloten met een hoofdstuk waarin alle objecten nog eens de revue passeren, maar dan onder de gemeenschappelijke noemer informatiebeveiliging. Dit laatste is belangrijk omdat vooral de beveiliging van informatie en informatiesystemen het primaire aandachtgebied van de ICT-auditor is geweest. Later heeft zich dat verbreed naar andere kwaliteitsaspecten zoals efficiency en effectiviteit.

1.1 Definities

De definitie van ICT-auditing luidt:

> Het vakgebied dat zich bezighoudt met het geven van assurance en advisering over het (toekomstig) gebruik van informatie- en communicatietechnologieproducten in organisaties. Het doel hiervan is kwalitatief en/of kwantitatief een bijdrage te leveren aan een toereikende organisatie van de informatievoorziening, waarbij de doelstellingen van de opdrachtgever gerealiseerd worden.

Uit deze definitie blijken de volgende twee, voor het vakgebied ICT-auditing kenmerkende, elementen:

- Er wordt assurance (zekerheid) geboden en in voorkomende gevallen advisering. Deze assurance wordt geboden door het uitvoeren van een audit met gebruik van bepaalde normen. Wanneer de normen niet door de opdrachtgever vooraf zijn vastgesteld, kan de ICT-auditor adviseren bij het vaststellen van de normen.

- ICT-auditing richt zich op objecten, die of betrekking hebben op de organisatie van de ICT (het gebruik) of de ICT-producten zelf.

Deze twee elementen (het geven van assurance en objecten) komen in dit boek in twee afzonderlijke delen uitgebreid aan de orde.

1.2 Het eerste deel

In het eerste deel wordt aandacht besteed aan auditing in meer algemene zin. Om de inhoud van het eerste deel wat verder te verduidelijken, gaan we uit van de definitie van auditing zoals die is vastgelegd in de zogenaamde ISO-normen:[1]

> Auditing is het systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal en het objectief beoordelen daarvan om vast te stellen in welke mate aan overeengekomen auditcriteria is voldaan.

In deze definitie is een aantal elementen genoemd die voor de verdere uitwerking van het eerste deel van belang zijn. Dit zijn:
- *Oordeel:* de auditor moet conclusies trekken. Dit oordeel is het product van de auditor.
- *Het onderzoeksobject:* de auditor moet zich een oordeel vormen ten aanzien van een object.

Aspecten die enerzijds samenhangen met de persoonlijke houding van de auditor en aspecten die betrekking hebben op het auditproces.

Met betrekking tot de houding van de auditor gaat het om de volgende persoonlijkheidskenmerken:
- *Deskundig:* de auditor moet deskundig zijn, dat wil zeggen, er moet sprake zijn van zowel een theoretisch als een praktisch fundament.
- *Onpartijdig:* de auditor moet onpartijdig zijn, dat wil zeggen, de auditor mag geen uitingen doen indien conflict of interest dit hem of haar onmogelijk maakt. Auditors spreken in dit verband ook wel over objectiviteit.
- *Onafhankelijkheid:* de auditor moet onafhankelijk zijn, dat wil zeggen, de auditor moet zorgen voor een optimale onafhankelijkheid in zijn of haar optreden.

1 De ISO-normen zijn uitgegeven door de International Organization for Standardization. Deze definitie is opgenomen in de Nederlandse versie van EN ISO 19011, 2011. De norm is vertaald door het Nederlands Normalisatie-instituut (NNI) en heeft dezelfde status als de officiële versie.

Met betrekking tot het auditproces komen in de definitie de volgende aspecten aan de orde:

- *Systematisch:* de auditor moet zijn werkzaamheden op een systematische en gestructureerde wijze uitvoeren. Het gaat hierbij om het auditproces, waaronder we verstaan het geheel van samenhangende of elkaar beïnvloedende activiteiten dat input omzet in output.
- *Gedocumenteerd:* de auditor moet ervoor zorgen dat hij zijn oordeel aantoonbaar kan onderbouwen. In dit verband speelt de dossiervorming een wezenlijke rol.
- *Auditbewijsmateriaal:* ten behoeve van de oordeelsvorming zal de auditor bewijsmateriaal moeten verzamelen. Het betreft hier verifieerbare registraties, beweringen op basis van feiten of andere informatie die relevant zijn voor de auditcriteria. Het auditbewijsmateriaal kan kwalitatief of kwantitatief zijn.
- *Auditcriteria:* controleren is toetsen aan een norm. Vooraf moet duidelijk zijn welke norm de auditor hanteert bij de uitvoering van zijn werkzaamheden. Het gaat hierbij om het geheel van beleidslijnen, procedures of eisen die gebruikt worden als een referentie.

In de hoofdstukken 2 en 3 komen de organisatie van het beroep en de houding van de auditor aan de orde. Het gaat hierbij enerzijds om de wijze waarop de auditor zich georganiseerd heeft en anderzijds om de attitude van de auditor. Deze organisatie is nodig om de belangen van het beroep te kunnen behartigen. Voor de ICT-auditor betreft dit de NOREA (Nederlandse Orde van Register EDP-auditors). De NOREA is het onderwerp van hoofdstuk 2. De NOREA waakt over de deskundigheid van de Register EDP-auditors (RE's) en bindt hen tevens aan regels voor de beroepsuitoefening. In hoofdstuk 3 wordt meer concreet ingegaan op de onafhankelijkheid en de objectiviteit van de auditor. Deze aspecten worden in meer algemene zin behandeld, terwijl in dit hoofdstuk ook ingegaan zal worden op de deskundigheid van de auditor. Hoewel het onderzoeksobject zelf concreet aan de orde zal komen, wordt naast kennis over de informatie- en communicatietechnologie van de ICT-auditor specifieke deskundigheid verwacht ten aanzien van bestuurlijke informatievoorziening en organisatiekunde. In dit hoofdstuk gaan we ook al de A&K-analyse (Afhankelijkheids- en kwetsbaarheidsanalyse) behandelen als voorbeeld van hoe men de noodzaak voor beheersmaatregelen kan identificeren en articuleren. Verder wordt in hoofdstuk 3 aandacht besteed aan de 'Code of Ethics', het Reglement Beroepsuitoefening Register IT-auditors en het Reglement Kwaliteitsbeheersing NOREA.

In de hoofdstukken 4 tot en met 7 wordt ingegaan op auditing. Hierbij komen de hiervoor genoemde elementen in afzonderlijke hoofdstukken aan de orde. In hoofdstuk 4 wordt het auditproces in zijn algemeenheid beschreven. De activiteiten die de auditor uit moet voeren, komen hier aan de orde. Centraal staan hierbij de regelgeving, fundamentele beginselen, kwaliteitsaspecten en normconcretisering. Door het auditproces systematisch uit te voeren kan inderdaad tot het geven van assurance worden gekomen. Een bijzonder aspect dat in dit hoofdstuk uitgewerkt wordt betreft de rapportering. De Richtlijn Assurance-opdrachten door IT-auditors stelt duidelijke eisen aan de uitingen van ICT-auditors.

In hoofdstuk 5 staat het auditbewijsmateriaal ('evidence') centraal. Uitgaande van de dossiervorming, die nodig is voor de documentatie, wordt in dit hoofdstuk ingegaan op het auditbewijsmateriaal. Op welke wijze wordt dit verkregen en hoe wordt de kwaliteit van het verkregen bewijsmateriaal gewogen? Vanzelfsprekend worden hier ook de eisen uit de Richtlijn Documentatie NOREA 230 behandeld.

In hoofdstuk 6 wordt aandacht besteed aan Concluderen en rapporteren. Op basis van het verkregen auditbewijsmateriaal trekt de ICT-auditor conclusies. Hoe hij dit doet komt in dit hoofdstuk aan de orde. Tevens wordt het product van de audit ten behoeve van het geven van assurance behandeld. Het betreft de rapportage van de ICT-auditor. Met het rapport presenteert de auditor zich aan zijn opdrachtgever. De behandeling van het verschil tussen direct reporting en assertion based reporting sluit dit hoofdstuk af.

Ten slotte komen in hoofdstuk 7 de auditcriteria aan de orde. Het betreft hier de normen die de auditor als uitgangspunt hanteert bij de uitvoering van de audit. Omdat dit boek betrekking heeft op het vakgebied ICT-auditing ligt het voor de hand in dit hoofdstuk vooral aandacht te besteden aan de normen voor de auditor. Hiermee wordt in feite een geleidelijke overgang gecreëerd naar het tweede deel van het boek: de informatie- en communicatietechnologie (ICT).

Tabel 1.1 geeft een samenvatting van de onderwerpen die in eerste deel aan de orde komen.

Tabel 1.1 *De hoofdstukken uit het eerste deel*

Hoofdstuk	Onderwerp
2	De organisatie van het beroep
3	De houding van de auditor
4	Het auditproces
5	Het auditbewijsmateriaal
6	Concluderen en rapporteren
7	De auditcriteria

1.3 Het tweede deel

In het tweede deel wordt ingegaan op de objecten die een ICT-auditor bij het uitvoeren van een audit kan onderscheiden. De definitie van een ICT-auditobject luidt:

> Het door de opdrachtgever in de opdracht gedefinieerde onderwerp, dat door de ICT-auditor wordt geëvalueerd of getoetst. Dit onderwerp kan

> zijn een structuur, proces of product in een bepaalde fase, dat gebruikt wordt of gaat worden voor informatievoorziening met behulp van informatie- en communicatietechnologie.

De opdrachtgever van de ICT-auditor bepaalt welke ICT-auditobjecten, al dan niet in samenhang met andere ICT-auditobjecten, onderwerp van een ICT-audit worden.

Uit deze definitie blijkt dat een ICT-auditobject kan behoren tot drie deelverzamelingen:
- *Structuur:* dit kan een organisatorische structuur zijn binnen de gehele organisatie, maar ook delen van een organisatie, die zich uitsluitend en specialistisch bezighoudt met de informatievoorziening, bijvoorbeeld een afdeling systeembeheer.
- *Proces:* dit kunnen bedrijfsprocessen, koop- of bouwprocessen zijn voor producten te gebruiken in ICT-processen.
- *Product:* hieronder worden mede diensten begrepen. Deze producten kunnen als invoer dienen van, als component worden gebruikt binnen of het resultaat zijn van de informatievoorziening.

Het zal duidelijk zijn dat er een oneindig aantal ICT-auditobjecten te onderkennen zijn. Neem bijvoorbeeld een ziekenhuis. Een beperkte greep uit de ICT-auditobjecten: de aansturing door de directie van de ICT-organisatie, de werking van hartbewakingsapparatuur, de urenregistratie van het verplegend personeel, de projectgroep die zich bezighoudt met de aanschaf van een nieuw ziekenhuisinformatiesysteem, de programmatuur die de bestralingsapparatuur aanstuurt of de website van het ziekenhuis.

Het ICT-auditobject kan zich in een van de volgende drie fasen bevinden:
- *De architectuurfase:* in deze fase worden de eisen vastgesteld waaraan het ICT-auditobject moet voldoen. Voorbeelden zijn het ontwerp van een netwerk, het informatiebeleid en een functioneel ontwerp voor een informatiesysteem.
- *De verwervingsfase:* in deze fase wordt het ICT-auditobject gebouwd, of gekocht en getest. Bijvoorbeeld de aanleg van een lokaal netwerk, de implementatie van een ERP-pakket of de aanschaf van een personal computer.
- *De gebruikersfase:* de fase start met het in productie nemen en eindigt met het buiten gebruik stellen. In deze fase zijn verschillende processen te onderkennen, zoals het bewaken van de goede werking, het foutherstel en het aanpassen aan veranderende eisen van de gebruiker.

In dit tweede deel worden de ICT-auditobjecten opgedeeld in drie clusters. Deze clusters zijn:
- de organisatie van de informatievoorziening;
- de informatiesystemen en systeemontwikkeling;
- de technische infrastructuur.

Hoofdstuk 2

De organisatie van het beroep

In 1992 is de Nederlandse Orde van Register EDP-auditors (NOREA[1]) opgericht. Deze beroepsorganisatie is het onderwerp van dit hoofdstuk. Het bestaat uit drie paragrafen. De eerste paragraaf behandelt de beroepsorganisatie. Vervolgens wordt in de tweede paragraaf aandacht besteed aan de regelgeving die ontstaan is door initiatieven van de NOREA. Ten slotte wordt nog aandacht besteed aan de internationale aspecten van het vakgebied ICT-auditing. In dit kader wordt ingegaan op de internationale beroepsorganisatie ISACA[2].

2.1 Nederlandse Orde van Register EDP-auditors

NOREA is de beroepsorganisatie voor Register EDP-auditors (RE). De NOREA waakt over de deskundigheid van de RE's en bindt hen tevens aan regels voor de beroepsuitoefening. De NOREA is opgericht op 30 maart 1992 door een initiatiefgroep bestaande uit vertegenwoordigers van het universitair overleg EDP-auditing, de studenten- en afgestudeerdenverenigingen van de Erasmus Universiteit (EUR Rotterdam) en Katholieke Universiteit Brabant (KUB Tilburg) en de toen reeds bestaande Orde van Register EDP-auditors (ORE) die enkele jaren eerder was opgericht door afgestudeerden van de Vrije Universiteit (VU Amsterdam). Op dit moment beschikken vier universiteiten (EUR, KUB, VU en Universiteit van Amsterdam (UVA) elk over een eigen zogenoemde postgraduate opleiding IT-auditing, die recht geeft op de titel Executive Master of IT Auditing (EMITA) Na het behalen van deze graad kan men in principe ingeschreven worden bij de NOREA. De NOREA stelt voor inschrijving als lid een aantal ervaringseisen.

Figuur 2.1 *Het logo van de NOREA*

1 Op de website van de NOREA (www.norea.nl) kan de nodige aanvullende informatie worden verkregen over de NOREA. De inhoud van dit hoofdstuk is mede gebaseerd op de inhoud van de website. Tevens is gebruikgemaakt van RE-GIDS 2012/2013, hierin zijn onder meer alle namen van de geregistreerde EDP-auditors opgenomen en de organisaties waarvoor zij werken.

2 Op de website van ISACA (www.isaca.org) kan de nodige aanvullende informatie worden verkregen over ISACA.

2.1.1 Doelstellingen van de Orde

De Orde heeft de volgende doelstellingen geformuleerd:
- Het bevorderen van een goede beroepsuitoefening door de RE's (kwaliteitsbevordering). Hiertoe wordt invulling gegeven aan:
  - de beroepsreglementering;
  - het bewaken van de instroom van nieuwe RE's;
  - het tuchtrecht;
  - een verplichting tot voortgezette educatie.
- Het bevorderen van de verdere ontwikkeling van het vakgebied EDP-auditing en van het beroep van RE (beroepsontwikkeling). Dit geschiedt door:
  - het organiseren van symposia;
  - het uitdiepen van vaktechnische onderwerpen;
  - het uitgeven van het tijdschrift *De IT-auditor.*
- Het bevorderen van relevante opleidingen, gericht op het op peil houden van de deskundigheid van de leden. Hiertoe worden de volgende activiteiten uitgevoerd:
  - het erkennen en visiteren van EDP-auditingopleidingen;
  - het verzorgen van activiteiten ten behoeve van permanente educatie;
  - het stimuleren van wetenschappelijk onderzoek.
- Het behartigen van de belangen van de leden voor zover deze de beroepsuitoefening raken (belangenbehartiging). Hiertoe wordt aandacht besteed aan:
  - het behartigen van de vaktechnische belangen van de RE's;
  - het gevraagd en ongevraagd adviseren van derden met betrekking tot vraagstukken op het gebied van ICT-auditing;
  - het geven van voorlichting op het vakgebied ICT-auditing en het beroep RE aan leden en derden.

Het hoogste orgaan binnen de Orde is de Algemene Vergadering waarin conform de statuten door de leden besluiten worden genomen over beleid, financiën, reglementen, richtlijnen en aanbevelingen van de NOREA. De Algemene Vergadering benoemt tevens de leden van het Bestuur, de Raad voor Beroepsethiek, de Raad van Tucht, de Raad van Beroep en de Raad van Advies.

2.1.2 De Register EDP-auditor en de andere leden van de Orde

Volgens de statuten van de NOREA is een Register EDP-auditor iemand die gewoon lid of erelid is van de NOREA. Als men ingeschreven is in het register van de orde dan is de Register EDP-auditor ook formeel gerechtigd deze naam te vermelden achter de eigen naam. Ook kan men gebruikmaken van de afkorting RE achter de naam. NOREA noemt zich de beroepsorganisatie van IT-auditors.

Volgens de publicaties van de NOREA is een Register EDP-auditor een IT-auditor die een garantie biedt voor een hoge kwaliteit bij de beroepsuitoefening. Deze kwaliteit wordt gegarandeerd door de RE als hij of zij zich onderwerpt aan de eisen van de beroepsorganisatie. De Register IT-auditor is op grond van zijn opleiding en ervaring de aangewezen deskundige om IT-assuranceopdrachten uit te voeren.

> Een IT-assuranceopdracht is een opdracht waarbij een IT-auditor een conclusie formuleert die is bedoeld om het vertrouwen van beoogde gebruikers, niet zijnde de partij die zich verantwoordt, in de uitkomst van een evaluatie of de toetsing van het object van onderzoek ten opzichte van de toetsingsnormen te versterken.

In deze nogal uitgebreide definitie wordt getracht de IT-assuranceopdracht[3] te beschrijven:
- er is een object van onderzoek;
- er is een partij die zich verantwoordt (de verantwoordelijke voor het object);
- het gaat om het vertrouwen van beoogde gebruikers;
- het object van onderzoek wordt geëvalueerd of getoetst aan toetsingsnormen;
- er wordt een conclusie geformuleerd (de uitkomst van auditwerkzaamheden);
- met als doel het vertrouwen te versterken in het object van onderzoek (assurance).

Het begrip assurance is breder is dan audit. De assuranceprovider hoeft niet altijd auditwerkzaamheden uit te voeren om assurance te kunnen verschaffen. Dit blijkt uit de definitie: als er wordt geëvalueerd, hoeft er niet altijd een audit (toets aan toetsingsnormen) plaats te vinden. Bij assurance worden de volgende soorten onderscheiden:
- historische financiële informatie – bijvoorbeeld jaarrekeningen;
- overige financiële informatie – bijvoorbeeld een subsidieaanvraag;
- niet-financiële informatie – bijvoorbeeld een milieu-effectrapportage (MER) of een sociaal jaarverslag;
- systemen en processen – bijvoorbeeld een 'in control'-verslag van een serviceprovider;
- gedrag – bijvoorbeeld naleving privacyvoorschriften.

Historische financiële informatie en overige financiële informatie zijn het expertiseterrein van (register)accountants. De overige soorten kunnen op het kennis- en ervaringsterrein van de ICT-auditor liggen.

NOREA maakt volgens haar toelichting op de richtlijn Assurance-opdrachten door IT-auditors weinig woorden vuil aan het onderscheid, door te stellen: 'Deze richtlijn geeft aanwijzingen voor het uitvoeren van IT-audits'.

Het beroep van RE vereist deskundigheid op het gebied van informatie- en communicatietechnologie, bestuurlijke informatievoorziening en organisatiekunde. Deze

3 Ontleend aan de brochure *Het assurance-raamwerk – De accountant en het verstrekken van zekerheid* van het Koninklijk Nivra. Er is sprake van een assuranceopdracht als:
- er drie partijen zijn (verschaffer van informatie, assurance provider en gebruiker);
- er een geschikt object van onderzoek is;
- er criteria zijn waaraan het object getoetst kan worden;
- er voldoende en geschikte informatie beschikbaar is;
- er een schriftelijk assurancerapport is.

laatste twee onderwerpen komen in het volgende hoofdstuk uitgebreid aan de orde. Het onderwerp informatie- en communicatietechnologie wordt uitgewerkt in het tweede deel van dit boek. Verder hebben de RE's kennis van methoden en technieken voor onderzoek, toetsing en risicoanalyse. In de hoofdstukken 4 tot en met 7 worden deze onderwerpen verder uitgewerkt. De ICT-auditors beschikken veelal over specifieke deskundigheid op bepaalde objecten.

Met betrekking tot de leden onderscheidt de NOREA vier soorten leden:
- gewone leden;
- ereleden;
- geassocieerde leden;
- aspirant-leden.

De gewone leden van de NOREA zijn personen die afgestudeerd zijn aan een door de NOREA erkende universitaire opleiding en tevens voldoen aan de relevante ervaringseisen. Ook kunnen leden door het Bestuur worden toegelaten. Voor de toelating van gewone leden is een afzonderlijk reglement van toelating opgesteld.

Momenteel zijn door de NOREA een viertal universitaire postgraduate opleidingen IT-auditing formeel erkend. Het betreft de opleidingen aan de Amsterdam Business School-Universiteit van Amsterdam, de Vrije Universiteit Amsterdam Postgraduate School, de Erasmus School of Accounting & Assurance te Rotterdam en de TiasNimbas Business School te Tilburg. Hoewel er onderling verschillen zijn tussen de verschillende opleidingen is het curriculum van deze opleidingen toch van een zodanig niveau dat deze goed opgeleide Register EDP-auditors afleveren. Deze opleiding is zodanig dat na het met succes afronden van de opleiding de IT-auditing bij het voldoen aan ervaringseisen kan worden ingeschreven in het register van de Orde. Hij is dan gerechtigd de titel Register EDP-auditor te dragen.

Ereleden zijn personen die zich voor de Orde of voor het vakgebied ICT-auditing bijzonder verdienstelijk hebben gemaakt. Over de toelating tot erelid beslist de Algemene Vergadering op voordracht van het Bestuur. Tot op heden is hiervan spaarzaam gebruikgemaakt.

Geassocieerde leden zijn personen die geen gewoon lid en geen aspirant-lid van de NOREA zijn en die naar het oordeel van het Bestuur op enigerlei wijze verbonden zijn met het vakgebied ICT-auditing. Dit zijn veelal RE's, die voorheen gewoon lid waren en niet meer (fulltime) in het vakgebied werkzaam zijn.

De vierde categorie zijn de aspirant-leden. Dit zijn natuurlijke personen die meestal zullen studeren aan een door de NOREA erkende universitaire opleiding of daaraan afgestudeerden die nog niet hebben voldoen aan de gestelde ervaringseisen.

Door het Bestuur van de NOREA wordt een register bijgehouden waarin de namen van alle leden zijn vastgelegd. Het zijn alleen de gewone leden en de ereleden die het recht hebben van inschrijving in het register te doen blijken door achter hun naam te

vermelden Register EDP-auditor, dan wel de afkorting RE. Op alle leden zijn verder de statuten en alle op hen van toepassing zijnde reglementen relevant.

2.1.3 De organen van de Orde

Zoals hiervoor al is aangegeven worden binnen de NOREA een aantal organen onderscheiden. Deze organen zijn:
- het Bestuur;
- de Raad voor Beroepsethiek;
- de Raad van Tucht;
- de Raad van Beroep;
- de Raad van Advies.

Het *Bestuur* van NOREA heeft de dagelijkse leiding van de Orde. Het Bestuur wordt ondersteund door een directeur en een secretariaat en is verantwoordelijk voor het uitvoeren van de besluiten van de Algemene Vergadering en alle overige activiteiten in het belang van de NOREA en haar leden. Het bestuur benoemt de leden van alle commissies en studiegroepen met uitzondering van de Raden, die door de Algemene Ledenvergadering worden benoemd. Het bestuur is verder belast met de uitvoering van besluiten tot inschrijving in het register zoals genomen door de Commissie van Toelating, respectievelijk de Commissie van Beroep.

De *Raad voor Beroepsethiek* bewaakt de actualiteit van het Gedrags- en Beroepsregels Register EDP-auditors (Code of Ethics) en het Reglement van Tucht. De Raad doet zo nodig voorstellen voor aanpassing van de Code of Ethics aan de maatschappelijke ontwikkelingen en adviseert de Raad van Tucht. Daarnaast is het de taak van de Raad om de leden van NOREA te adviseren wanneer zij problemen bij de beroepsuitoefening ondervinden die op enigerlei wijze verband houden met het naleven van de Code of Ethics'. De werkzaamheden van de Raad en de benoeming van zijn leden zijn nader geregeld in het Reglement voor de Beroepsethiek.

De *Raad van Tucht* behandelt klachten die tegen registerleden of ereleden worden ingediend. Deze klachten kunnen echter alleen in behandeling genomen worden als het handelen van de betreffende RE in strijd is met de Code of Ethics *en* als voor de indiener van de klacht nadeel is ontstaan. Het Bestuur, iedere natuurlijke persoon en iedere rechtspersoon kan een dergelijke klacht indienen bij de Raad van Tucht. Nadere regelingen met betrekking tot taken, bevoegdheden, werkwijze, samenstelling en benoeming van zijn leden, worden opgenomen in een Reglement van Tucht.

De *Raad van Beroep* neemt bindende besluiten over bezwaarschriften. Hierbij kan het gaan om bezwaarschriften tegen het afwijzen van een aanvraag voor het gewone lidmaatschap. Het kan echter ook gaan om bezwaarschriften in verband met besluiten van de Orde over de erkenning van EDP-auditingopleidingen.

De *Raad van Advies* is ingesteld om de Algemene Vergadering en het Bestuur gevraagd en ongevraagd te adviseren over zaken die de beroepsuitoefening van de RE raken.

De Raad is samengesteld uit vertegenwoordigers van verschillende maatschappelijke groeperingen die voor de NOREA relevant zijn. Het doel hiervan is dat deze groeperingen betrokken worden bij het beleid en de taken van de NOREA. De Algemene Vergadering van de NOREA benoemt de leden van de Raad van Advies.

2.2 Regelgeving

- In het kader van de goede beroepsuitoefening door de RE's dienen alle RE's zich te houden aan de regels neergelegd in diverse besluiten van de Algemene Ledenvergadering, het bestuur en diverse commissies. Jurgen van der Vlugt heeft in 2010 in een artikel in *de IT-auditor* het huis van de NOREA-regelgeving beschreven. Dat ziet eruit zoals in figuur 2.2:

<table>
<tr><td colspan="5">A1 Statuten</td></tr>
<tr><td colspan="5">B1 Reglement Gedragscode 'Code of Ethics'</td></tr>
<tr><td colspan="5">B2 Reglement Beroepsbeoefening</td></tr>
<tr><td colspan="5">B3 Reglement KwaliteitsBeheersing NOREA</td></tr>
<tr><td colspan="5">B4 Reglement KwaliteitsOnderzoek NOREA</td></tr>
<tr><td rowspan="3">A2 Huishoudelijk reglement
A3 Reglement van toelating
A4 Reglement Beroepsethiek
A5 Reglement van Tucht
A6 Reglement van beroep
A7 Reglement PE
A8 Regeling Overstappers en herintreders</td><td>C1 Raamwerk Assurance-opdrachten
C2 Richtlijn Assurance Opdrachten
C3 Richtlijn 3402</td><td>D Audit
Assessment
Review
Quick Scan
Beoordeling
Analyse</td><td>E Advies

Invulling in ontwikkeling</td><td rowspan="3">F 'Niet actief'

(zoals 'in business' of gepensioneerd)

[Geen invulling; B2, B3 en B4 n.v.t.]</td></tr>
<tr><td colspan="3">G Uitvoeringsrichtlijnen
(Opdrachtaanvaarding en documentatie)</td></tr>
<tr><td colspan="3">H Handreikingen (ZekeRE Business, ZekeRE zorg DBC en AWBZ); studierapporten, Handboek en 'De IT – Auditor'</td></tr>
</table>

Figuur 2.2 *Het huis van de NOREA-regelgeving*

Boven in de hiërarchie **A1** staan de statuten die voor de Orde van toepassing zijn. In de statuten komen achtereenvolgens de volgende onderwerpen aan de orde:

- Algemene gegevens met betrekking tot de Orde:
  - naam en zetel;
  - verenigingsjaar;
  - middelen;
  - structuur.
- Leden van de Orde:
  - toelating;
  - einde lidmaatschap;

  - Register, lijsten van aspirant-leden en geassocieerde leden;
  - optreden als EDP-auditor;
  - rechten van de leden;
  - verplichtingen van de leden.
- Organen van de Orde:
  - Bestuur;
  - Algemene Vergadering;
  - Raad voor Beroepsethiek;
  - Raad van Tucht;
  - Raad van Beroep;
  - Raad van Advies;
  - EDP-auditingopleidingen;
  - Commissies.
- Overige onderwerpen met betrekking tot de Orde:
  - geldelijk beheer;
  - reglementen;
  - bijzondere besluiten.

Volgens de statuten van de NOREA kunnen reglementen worden vastgesteld over onderwerpen die de Algemene Vergadering wenselijk acht. Hierbij is in de statuten bepaald dat een bepaling in een reglement niet in strijd kan zijn met de statuten. Als dit wel het geval is dan is de bepaling nietig. Regelingen die de NOREA zelf betreffen zijn vastgelegd in een Huishoudelijk Reglement, dat door de Algemene Vergadering wordt vastgesteld en gewijzigd. De volgende reglementen zijn vastgesteld:
- A2 Huishoudelijk Reglement;
- A3 Algemeen Reglement Toelating;
- A4 Reglement Beroepsethiek NOREA;
- A5 Reglement van Tucht;
- A6 Reglement van Beroep;
- A7 Richtlijn Permanente Educatie;
- A8 Regeling Overstappers en Herintreders.

Naast statuten en reglementen kent NOREA richtlijnen, handreikingen en studies. Deze worden behandeld in hoofdstuk 3.

2.3 ISACA

De ISACA is in 1969 opgericht als een internationale vereniging van EDP-auditors (EDP Auditors Association – EDPAA). Het veranderde daarna haar naam in Information Systems Audit and Control Association (ISACA). Nu is de naam ISACA betekenisloos, omdat ISACA alle professionals die zich bezighouden met IT-governance verenigt. Governance komt uit het Grieks en betekent sturen. De definitie van IT-governance door het IT Governance Instituut luidt als volgt:

> IT-governance is de verantwoordelijkheid van de raad van bestuur en het uitvoerend management. Het is een integraal onderdeel van verantwoord ondernemingsbestuur en bestaat uit de leiding en organisatorische structuren en processen die ervoor zorgen dat de organisatie haar informatietechnologie onderhoudt en dienstbaar maakt de strategie en doelstellingen van de onderneming.

ISACA kent regionale en nationale afdelingen (Chapters). De vereniging is sinds 1986 actief in Nederland en stelt zich ten doel opleidingen met betrekking tot IT-governance te verzorgen en te stimuleren. Verder streeft de ISACA in samenwerking met andere partijen naar standaards op haar werkgebied. De ISACA is 'a not-for-profit foundation committed to expanding the knowledge base of the profession through a commitment to research'.
ISACA certificeert:

- Computer Information Systems Auditors (CISA);
- Certified Information Security Manager (CISM);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified in Risk and Information Systems Control (CRISC).

Figuur 2.3 *Het logo van de ISACA*

2.4 International Federation of Accountants (IFAC)

NOREA en ISACA zijn geassocieerd lid van de International Federation of Accountants, waardoor leden van beide organisaties moeten voldoen aan internationale regelgeving, in het bijzonder de eerdergenoemde Code of Ethics.

Index

A
aanbevelingen 38, 50
acceptatiecriteria 136
acceptatietest 152
accounting management 227
actieplan 196, 248
ActiveX 170
administratieve organisatie 16, 17
afhankelijkheidsanalyse 28
afhankelijkheids- en kwetsbaarheidsanalyse (A&K-analyse) 25
Agile systeemontwikkeling 157
Agile Systeemontwikkeling 132, 143
A&K-analyse (afhankelijkheids- en kwetsbaarheidsanalyse) 25
Algemeen Reglement Toelating 13
Algemene Vergadering 8
algoritme 225
applicatiebeheer 147
applicatiedimensionering 195
Applications Cycle Management 147
Application Services Library 116, 133
architectuurfase 5
aselecte getallen 57
ASL-bibliotheek 152
aspirant-leden 10
assertion based assurance-opdracht 90
assurance 1
asymmetrisch algoritme 226
attributen 55
attributieve steekproeven 54
auditbewijsmateriaal 2
auditcriteria 2
auditdossier 70
auditing 2
auditmethode 65
auditmiddelen 67
auditplan 66
auditrisk 66
auditsoftware 54, 72
authenticatie 238, 240
automatiseringsfunctie 161
automatiseringsplan 125
autorisatie 220, 238, 242

B
backoffice 150
back-upplan 196, 248
bedrijfs- en programmamanagement 173
bedrijfs- of programmamanagement 128
bedrijfsschadeverzekering 252
bedrijfszekerheid 99
beheersingsmaatregelen 21
beheersingsmaatregelen in de automatiseringsorganisatie 22
beheersingsmaatregelen in de gebruikersorganisatie 23
beheersingsmaatregelen in de toepassingsprogrammatuur 22
beheersingsmaatregelenmatrix 86
beheersomgeving 21
beheer van apparatuur 186
beheer van netwerken 187
beheer van systeemprogrammatuur 187
beleidsvorming 125
beschikbaarheidsbeheer 196, 204, 206, 208, 210
besluitvormingsproces 18, 22
bestaan 62
besturingsinformatie 19
besturingssystemen 212, 213
Bestuur 8, 11
bestuurlijke informatievoorziening 16, 17
betrouwbaarheid 52, 97
beveiliging 233
beveiligingsbeleid 103, 244
beveiligingscriteria 102, 234
beveiligingsincidenten 104
beveiligingsopleiding 104
beveiligingsplan 245
beveiligingsvoorzieningen 253
bewaring 183
bewijsstukken en overige vastleggingen 68
BPR (Business Proces Redesign) 145
brand 247
brandbestrijding 251
brandpreventie 250
brandsignalering 250
brand-, water- en stormverzekering 252
buizenpostsysteem 235
businesscase 136
businessmanagement 129
Business Proces Redesign (BPR) 145
business proces re-engineering 148

C
CAATT (Computer Assisted Audit Tools en Techniques) 70
CA (certificatieautoriteit) 237
calamiteitenbeheer 196, 204, 206, 208, 210

Capability Maturity Model 100, 101
capaciteitsbeheer 195, 204, 206, 208, 210
Capacity Management 106
CBP (College Bescherming Persoonsgegevens) 121
Central Computer & Telecommunications Agency (CCTA) 106
certificatieautoriteit (CA) 237
Change Management 137
checkpoint reports 139
cijferbeoordeling 161
CISA (Computer Information Systems Auditor) 14
Clark/Wilson-model 50, 100, 107, 109
classificatie en beheer van de bedrijfsmiddelen 103
CMDB (Configuration Management Database) 194
Code voor Informatiebeveiliging (CIB) 50, 100, 102
College Bescherming Persoonsgegevens (CBP) 121
Commissie Permanente Educatie 16
communicatieverbindingen 212
componentgeoriënteerde benadering 169
Computer-Aided Software Engineering 167
Computer Assisted Audit Tools en Techniques (CAATT's) 70
computer en netwerkbeheer 103
computerfraudeverzekering 252
Computer Information Systems Auditor (CISA) 14
conceptuele datamodel 167
configuratiebeheer 193, 206, 208, 210
configuratie-item 193
configuration management 226
Configuration Management Database (CMDB) 194
Configuration Management plan 137
connectiviteit 98
Constraint 155
continuïteit 97
controleerbaarheid 99
controletotalen 156
Control Objectives 104
Control Objectives for Information and related Technology (COBIT) 50, 100
conversie 155
coördinatiemechanisme 131
correctieve maatregelen 86
COSO-rapport 21
Cost Management 117

D
database 217
databasemanagementsystemen 212, 217
databasemanagementsystemen (DBMS) 216
databaseomgeving 216
datacommunicatie 224
Data Dictionary/Directory 218
Data Dictionary Directory System (DD/DS) 218
Data Division 169
datageoriënteerde benadering 166
DBMS (databasemanagementsystemen) 216
DD/DS (Data Dictionary Directory System) 218
deelwaarnemingen 52
defined level 102
degradatiemogelijkheid 99
dekkingsgraad bedrijfsprocessen 98
delegatie 131
Demand Management 106
deskundig 2
deskundigheid 37
deskundigheidsniveau 66
dienst 126
dienstniveaubeheer 191, 204, 206, 208, 210
direct-reportingopdracht 90
distributie en nabewerking 183
doelgroep 62
doelrealisatie 18
dossier 75
dossiervorming 75
dossiervorming en -beheer 36
Dynamic Systems Development Method 157

E
e-commerce 236
effectiviteit 97
efficiency 97
eigen waarnemingen 69
eilandautomatisering 143
eis 96
encapsulation 169
encryptie 225
encryptiesoftware 25
End User Development 160
energievoorziening 247, 251
engineering 126
Enterprise Resource Planning 143
entiteitenrelatiemodel 167
entiteitintegriteit 219
Erasmus Universiteit 7
ereleden 10
ERP-systemen 144
evaluatiemethode 59
exclusiviteit 99
extern model 167
Extreme Programming 157

F
facturen 69
faseplan 139
fasetolerantie 140
fault management 226

Financial Management 106
financieel beheer 197, 204, 206, 208, 210
financiële verantwoordingen 69
flexibiliteit 98
framework internal control 21
frontoffice 150
functie- en taakbeschrijvingen 69
functiepuntanalyse 117
functiescheiding 23
functioneel applicatiebeheer 119, 186
functionele systeemtest 152
fysieke beheersingsmaatregelen 23
fysieke beveiliging 247
fysieke beveiliging en omgeving 103

G
geassocieerde leden 10
gebruikersfase 5
gebruikersidentificatie 238
gebruikersinterface 144
gebruikersmanagement 129
gebruikersvriendelijkheid 98
gefaseerde conversie 156
gegevensbankbeheer 185
gegevensbeheer 185
gegevensdefinitie 219
gegevenseigenaar 119
gegevens- en informatiebeheer 119
gegevensentiteit 167
gegevensonafhankelijkheid 167
geïntegreerde informatiesystemen 143
geprogrammeerde controle 22, 155
geschiktheid infrastructuur 98
gestructureerde educatie 16
gewone leden 10

H
herbruikbaarheid 98
herstelbaarheid 99
hiërarchische datamodel 168
Huishoudelijk Reglement 13
hulpprogrammatuur 212
HyperText Markup Language 170

I
I-CASE-tools 167
ICT-auditgrondslagen 36
ICT-auditing 1
ICT-auditobject 4
ICT-auditorganisatie 40
ICT-development strategy 123
ICT-portfoliomanagement 123
identificatie 238
identificatiesysteem 238
impactanalyse 148
implementatie- en conversiefase 155
incidentenbeheer 198, 206, 208, 210
informatieanalyse 145
informatiebeveiliging 6, 100, 102, 233
informatieplan 128
informatieverzorgingssysteem 179
Information Systems Audit and Control Foundation (ISACF) 104
Information Technology Infrastructure Library (ITIL) 50, 100, 190
inherente risico 82
initial level 101
inlichtingen van gecontroleerde 67
integriteitsbewaking 217, 219
Integrity Verification Procedures 108
Internal Control – Integrated Framework, Treadway Commission 21
Internal Control Report 122
International Standard on Assurance-opdrachten (ISAE) nr. 3402 110
interne kwaliteitsaudits 41
inventarisatie 70
investeringsbeoordeling 137
IP-adressen 236
ISACF (Information Systems Audit and Control Foundation) 104
ISO-normen 2, 50
issue log 139
ITIL (Information Technology Infrastructure Library) 50, 190

J
JavaScript 170
juistheid 99

K
Katholieke Universiteit Brabant 7
kernmodule 166
kwaliteit 96
kwaliteitsbeheersing 131
kwaliteitsmanagementsystemen 95
kwaliteitsmanager 131
kwaliteitstoetsing 131
kwaliteitstolerantie 137
kwaliteitsverantwoordelijken 137
kwetsbaarheidsanalyse 31

L
leerpuntenrapport 141
levensfase 46
leveranciersmanagement 129
Life Cycle Management 123
lijncontrole 70
Limperg Instituut 79
linking-pinprincipe 131
logging 55
Lower-CASE-tools 167

M
maatwerksysteem 132
managed level 102
materialiteit 66, 74, 112
maturity levels 101
Microsoft Office 162
MoSCoW-principe 145
mutatieverslagen 69

N
netwerkbesturingssystemen 212
netwerk datamodel 168
NOREA (Nederlandse Orde van Register EDP-auditors) 3, 7, 50

O
objecten 2
objectgeoriënteerde benadering 166
onafhankelijkheid 2, 35
onderhoudbaarheid 98
ondersteuning besluitvorming 98
onderzoek en verandering 127
onderzoeksobject 2
onderzoeksperiode 47
ongestructureerde educatie 16
onpartijdig 2
onpartijdigheid 35
ontdekkingsrisico 51
ontdekkingsrisico in enge zin 52
ontwikkeling en onderhoud van systemen 103
oordeel 2
oordeelsvorming 75, 80
opdrachtaanvaarding 36
opdrachtnemer 130
Open Office 162
opensourcesoftware 161
operating 183
opslagapparatuur 212
optimizing level 102
opzet 62
ORE (Orde van Register EDP-auditors) 7
organisatie- en bedrijfsbeschrijvingen 69
organisatiekunde 18
organisatie van de beveiliging 103
organisatie van de informatieverzorging 17
organisatie van de informatievoorziening 17
organisatorische beheersingsmaatregelen 23
Organization Cycle Management 147
OSI Management Framework 226
outsourcing 63
overdraagbaarheid 75, 77
overstapconversie 156

P
parallelle conversie 156
performance management 227
permanente dossier 76
pilot-studyconversie 156
PKI (Public Key Infrastructure) 237
Planning and Control 117
planning en werkvoorbereiding 183
Planning & Organization 104
populatie 55
portabiliteit 98
postdoctorale opleiding EDP-auditing 7
post-project review 141
preventieve maatregelen 85
PRINCE2 (Projects in Controlled Environments) 133
privacyauditors 122
probleembeheer 200, 207, 209, 210
Procedure Division 169
procedurele beheersingsmaatregelen 24
proceduretests 70
proces 5
proces van normconcretisering 61
product 5, 126
product-based planning 142
product breakdown structure 142
product description 142
productencryptie 225
product flow diagram 142
productiesysteem 158
productietest 152
productontwikkeling 127
productontwikkelingstraject 127
programmamanagement 120
programmanagement 129
programmatuurbeheer en distributie 198, 206, 208, 210
project 125
projectachtergrond 136
projectbeheersing 137
projectbestuur 128, 129
projectbrief 136
projectdefinitie 136
projectidee 136
projectinitiatie 136
projectinitiatiedocument 137
projectleiding 173
projectmanagement 128
projectproducten 137
projectsoorten 126
projectvoorstel 136
prototyping 158
proxyfirewall 236
Public Key Infrastructure (PKI) 237

Q
Quality Management 118
quality review 140

R
Raad van Advies 8, 11
Raad van Beroep 11
Raad van Tucht 11
Raad voor Beroepsethiek 8, 11
raamwerk interne beheersing 21
Rapid Application Development 159
rapportage 36
rapportering 238
rationaliteitsaxioma's 80
realisatiefase 151
reconstructieplan 248
recoveryplan 196
redundantie 217
referentiële integriteit 219
registratie 183
Reglement Beroepsbeoefening Register EDP-auditors 38
Reglement Beroepsethiek NOREA 13
Reglement van Tucht 13
relationele datamodel 168
repeatable level 102
repressieve maatregelen 86
reviewbaarheid 75
richtlijnen 38, 50
Richtlijn Permanente Educatie 16
risicoanalyse 21, 22, 80, 136, 142
risicoanalytische aanpak 51
risicomatrix 85
risicomijder 52, 81
risiconeutraal 81
risicoprofiel 139
risicozoeker 52, 81
risk log 140
robuustheid 99
Rule 155

S
samenwerkingsverband 20
Sarbanes-Oxley Act 122
scope 66
scrum 157
SEC 122
security management 226
selectiemethode 57
Service Catalogue Management 106
Service Delivery Set 190
Service Level Agreement (SLA) 191, 203
Service Level Management 106, 118
Service Portfolio Management 106
Service Support Set 190
sleutel 225
sleutelbeheer 229
smartcards 240
SQL-statements 222
standaarddeviatie 60
standaardprogrammatuur 143
stateful inspection firewall 237
statistische steekproef 52
steekproefomvang 56
storingsbronnen in de directe omgeving 247
structuur 5
stuurgroep 129, 173
submodule 166
substitutie-encryptie 225
symmetrisch algoritme 226
systeemarchitectuur 143
systeembeheer 144, 181
systeemeigenaar 119
systeemintegratie 143
systeemontwikkeling 126, 127, 132
systeemontwikkelingsproject 127
systeemtest 164
systematische selectiemethode 57
Systems Development Life Cycle 153

T
teamleiding 173
teammanagement 128
teammanager 130
teamplan 139
technisch applicatiebeheer 186
technische beheersingsmaatregelen 24
technische infrastructuur 181
technische systeemtest 152
template 71
testbaarheid 98
testdoel 165
testen 164
testen van eenheden 164
testomgeving 165
testorganisatie 165
tijdigheid 99
toegangsbeveiliging 6, 103, 238
toegankelijkheid 75, 77
toetsingsnormen 49
toezicht 103
tolerantie 51, 66
tolerantiegrens 139
toleranties 141
top level reviews 23
totstandkomingsproces 203
Transformation Procedures 108
transpositie-encryptie 225
Trigger 155

U
uitvoeringsnormen 49
uitwijkmogelijkheid 99
Upper-CASE-tools 167
user-id 238

V
variabele steekproef 54, 59
veranderingsmanagement 143
verantwoordelijkheidsgebied 31

verantwoordingsinformatie 20
versiebeheer 165
verwerkingsapparatuur 212
verwervingsfase 5
verwijzigingsgegevens 77
verzekering tegen de kosten van reconstructie 252
verzekering tegen de kosten van uitwijken 252
viruscontrole 104
volledigheid 75, 77, 99
Voorschrift informatiebeveiliging Rijksdienst 1994 25
voortgangsrapport 139
vragenlijsten 58
Vrije Universiteit 7

W
wachtwoordsysteem 240
wateroverlast 247
webgeoriënteerde benadering 166
wettelijke normen 50
wijzigingenbeheer 128, 200, 207, 209, 210
work package 138

Z
zuinigheid 98

In *Inleiding ict-auditing* beschrijven Jan van Praat en Hans Suerink het volledige werkveld van de ict-auditor: waar moet hij rekening mee houden, wat zijn de belangrijke beroepsregels, hoe gaat de dossiervorming en hoe geeft hij assurance? Ook komt aan de orde hoe ICT opgesplitst kan worden in onderzoeksobjecten.

De zesde druk kent de vertrouwde indeling in twee delen. In het eerste deel worden het vakgebied ict-auditing en het auditproces nader uitgewerkt. In het tweede deel wordt ict-auditing geconcretiseerd: de auditingobjecten worden met grote diepgang beschreven. Enkele voorbeelden van de vele inhoudelijke uitbreidingen zijn de actualisering van de beroepsregels, de normen (zoals COBIT, Prince2, ISAE3402 en ITIL) en de relevante beroepsorganisaties.

Inleiding ict-auditing is in de eerste plaats een studieboek voor studenten in het hoger onderwijs. Verder is het boek een uitstekende inleiding voor de specifieke ict-audit-opleiding aan zowel hbo als universiteit. Tot slot dient *Inleiding ict-auditing* in de bibliotheek te staan van elke organisatie die gebruikmaakt van diensten van ict-auditors.

Over de auteurs

Jan van Praat heeft vanuit vier van de vijf grote accountantsorganisaties, de rijksoverheid en twee universiteiten zijn bijdrage aan het vakgebied geleverd. Jan is nu CFO van het Nederlands Forensisch Instituut.

Hans Suerink is ict-audit-partner geweest bij een groot accountantskantoor en is nu verbonden aan 2 Control B.V. Hij is lid van de Raad van Beroep van NOREA en was gedurende meer dan tien jaar voorzitter van de Commissie Vaktechniek van NOREA.

ISBN 978 90 395 2712 2
NUR 123 / 982

ACADEMIC SERVICE

9 789039 527122

www.academicservice.nl