IT B@SE(D)

THE FUTURE OF (IN) CONTROL, AUDIT AND ASSURANCE

DERDE, GEHEEL HERZIENE DRUK

ESTHER VAN GRUNSVEN | GIDEON FOLKERS | BRENDA WESTRA

PENTAGAN BOOKS

Andere boeken van Brenda Westra en Esther van Grunsven zijn onder andere:

- Compendium Accountancy (diverse delen)
- Auditing Essentials
- Kern van Knechel
- Succesvol studeren voor LAC (diverse delen)
- Succesvol studeren voor BIV/AO (diverse delen)

---

eerste druk, juni 2013
tweede druk, januari 2017
derde, herziene druk: oktober 2019 (geheel herziene versie 2019)

CIP-GEGEVENS KONINKLIJKE BIBLIOTHEEK DEN HAAG

Esther van Grunsven, Gideon Folkers, Brenda Westra
ISBN 978-90-830146-2-3 NUR 786

Trefw.: IT audit, IT, CAATT's, auditing, accountantscontrole

Voor meer info: info@pentaganbooks.nl
www.pentaganbooks.nl

Voorwoord

Smartphones, tablets en laptops zijn niet meer weg te denken uit het dagelijks leven. Tegenwoordig kun je betalen met je smartphone, op internet alles kopen wanneer je maar wilt en als je contact opneemt met een onderneming, heb je tegenwoordig al snel een gesprek met de chatbot.

De Informatietechnologie (IT) heeft en krijgt steeds meer impact op het bedrijfsleven. De technologische vooruitgang zorgt voor een overgang van 'document-uitwisseling' naar 'data-uitwisseling'. Binnen alle branches is dit zichtbaar. Denk bijvoorbeeld aan de wijze van communicatie met de gezondheidszorg, de scholen, de banken, de verzekeringsmaatschappijen waar tegenwoordig alles digitaal wordt afgehandeld.

De technologische ontwikkelingen zorgen ervoor dat 'het werk' van onder andere de administratie, de controller, de accountant ofwel alle financiële professionals ingrijpend aan het veranderen is. Aan de ene kant levert het voordelen op. Zo kunnen er grote 'efficiencyslagen' worden gemaakt. Aan de andere kant krijgen we te maken met (samenhangende) IT risico's, zoals de 'inefficiënties' die kunnen optreden. Denk aan een pinstoring bij de supermarkt of bij het tankstation, aan phishing mails en als kers op de taart de computer hacks oftewel computercriminaliteit. Bij de laatste wordt er vaak gebruikgemaakt van de zwakste schakel van de IT en dat is nog steeds de mens.

Op dit moment loopt 'de integratie' van de IT (soms of vaak) achter, zowel bij ondernemingen als bij de accountantsorganisaties. Het wringt dan met name op het punt van de concrete toepassingen die de IT biedt en het kapitaal dat is benodigd om hierin te investeren. Maar één ding is zeker, iedere onderneming wordt een IT onderneming.

Hoe stel ik vast dat de General Controls van voldoende niveau zijn? Begrijp ik de werking van de Application Controls? Is het mogelijk om gebruik te maken van Data Analyse? Wat is Process Mining? Hoe is het nu gewaarborgd dat de mensen in de onderneming zich houden aan de werkafspraken met betrekking tot de IT? Heb ik het overzicht van

alle relevante technologische ontwikkelingen die een rol (kunnen gaan) spelen voor mijn functioneren?

Waar moet ik nu beginnen...?

Op al deze vragen wil dit boek een antwoord geven en je bovenal aanmoedigen om als 'mens' en als 'financiële professional', de technologische ontwikkelingen te volgen. Je gaat dan ook onderkennen dat je over de (basis)kennis van het algoritmisch denken moet beschikken. Maak de vergelijking met de scheidsrechter op het voetbalveld. Als hij het speelveld niet kan overzien, hoe kan hij dan nagaan of de spelregels worden overtreden?

We wensen iedereen veel plezier met dit boek! Dat het een uitdaging voor ons allemaal mag worden om de IT optimaal, ethisch en veilig te kunnen (gaan) inzetten.

Esther en Gideon

Dankwoord

Bijzondere dank aan een vriend op afstand. Telkens gaf hij aan dat ik nog dieper en kritischer de IT omgeving moest analyseren. Hierdoor ben ik meerdere malen van de ene in de andere verwondering gevallen en was het vaak hersenkraken. Dank daarvoor!

Daarnaast dank aan mijn motivatie- en krachtbron, die ervoor zorgt dat ik nooit opgeef.

Gideon Folkers, dank voor de vragen en de suggesties.

Eva de Hilster, veel dank voor het meedenken en de prachtige opmaak van het boek.

Als laatste mijn vader, mijn beste vriend. Dank voor je morele support en dat je altijd aan mijn zijde staat.

Esther

'De subjectiviteit van het individu is inderdaad ons uitgangspunt. Niet omdat wij deel uitmaken van de bourgeoisie, maar omdat we een leer willen die op waarheid is gegrond en niet een verzameling mooie theorieën, hoopvol maar zonder reële waarde.'

J.P. Sartre, 1967

Inhoud

Afkortingen

3LoD	Three lines of defence
ACF	Assurance Control Framework
ACL	Audit Command Language
ACM	Applications Cycle Management
AFM	Autoriteit Financiële Markten
AI	Artificial Intelligence
AIaaS	Artificial Intelligence as a Service
AO/IB	Administratieve Organisatie en de hierin opgenomen maatregelen van Interne Beheersing
AP	Autoriteit Persoonsgegevens
API	Application Program Interfaces
ASL	Application Service Library
AVG	Algemene Verordening Gegevensbescherming
BCP	Business Continuity Planning
BI	Business Intelligence
BIM	Business Informatie Management
BiSL	Business information Services Library
BIV	Bestuurlijke Informatie Voorziening
BPaaS	Business Process as a Service
BSC	Balance Score Card
CA	Continuous Assurance
CAATT	Computer Assisted Audit Tools and Techniques
CAu	Continuous Auditing
CFO	Chief Financial Officer
CIO	Chief Information Officer
CM	Continuous Monitoring
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSP	Certification Service Provider

CSR	Corporate Social Responsibility
CTF	ControleTechnische Functiescheiding
DSD	Data Structure Diagram
EDP	Electronic Data Processing
ELT	Extract, Load, Transform
ERD	Entity Relationships Diagram
ERP	Enterprise Resource Planning
ETL	Extract, Transform, Load
FEM	Faculteit Economie en Management
GDPR	General Data Protection Regulation
HRM	Human Resource Management
IaaS	Infrastructure as a Service
ICF	Internal Control Framework
ICT	Informatie- en Communicatietechnologie
IDEA	Interactive Data Extraction and Analysis
IIOT	Industrial Internet of Things
IOT	Internet of Things
IR	Integrated Reporting
ISA	International Standards on Auditing
ISO	International Organization for Standardization
IT	Informatie Technologie
ITIL	Information Technology Infrastructure Library
KI	Kunstmatige Intelligentie
KSF	Kritische Succes Factoren
KvK	Kamer van Koophandel
LAAI	Logging, Autorisatie, Authenticatie, Identificatie
LOR	Letter of Representation
MIS	Management Informatie Systeem
MKB	Midden en Klein Bedrijf
ML	Machine Learning
MLaaS	Machine Learning as a Service
NBA	Nederlandse Beroepsorganisatie van Accountants
NOREA	Nederlandse Orde van Register EDP-Auditors

NoSQL	Not only Structured Query Language
NV COS	Nadere Voorschriften Controle- en Overige Standaarden
O/S	Operating System
OCM	Organization Cycle Management
OOB	Organisatie van Openbaar Belang
OT	Operational Technology
PaaS	Platform as a Service
PCF	Privacy Control Framework
PhD	Doctor of Philosophy
PI	Prestatie Indicatoren
PKI	Public Key Infrastructure
RA	Robotic Accounting
RDBMS	Relationele DataBase Management Systeem
RPA	Robotic Process Automation
RSG	Referentie Grootboek Schema
RvB	Raad van Bestuur
RvC	Raad van Commissarissen
SaaS	Software as a Service
SBR	Standard Business Reporting
SLA	Service Level Agreement
SOX	Sarbanes-Oxley
SQL	Structured Query Language
TOGAF	The Open Group Architecture Framework
WCC (III)	Wet Computer Criminaliteit
WMD	Wet Meldplicht Datalekken
XBRL	eXtensible Business Reporting Language

Leeswijzer

Het beste is om de hoofdstukken volgordelijk te lezen. Dit vanwege de opbouw van de hoofdstukken en de begrippen die worden gehanteerd. De kapstok (groei) modellen IT 1 en IT 2, die in hoofdstuk 1 worden gepresenteerd, lijken mogelijk op het eerste gezicht abstract en zijn misschien in eerste instantie moeilijk te volgen. Maar gaandeweg worden beide modellen concreter en op het einde van het boek hebben zij geen geheimen meer voor je. Daarnaast is er bewust gekozen om te werken met voetnoten. Vanzelfsprekend ter verantwoording van de gebruikte bronnen, de afbeeldingen en toelichting of de uitleg van gehanteerde begrippen. Belangrijker is evenwel dat zij een hulpmiddel kunnen zijn op het moment dat je je verder wilt verdiepen in bepaalde onderwerpen. Soms worden op het einde van het hoofdstuk expliciet websites genoemd, die voor jou van belang (kunnen) zijn.

HOOFDSTUK 1

IT base (d), (back to) the 'Future' of (in) Control, Audit & Assurance

De technologische vooruitgang heeft een grote impact op onze samenleving. Zo worden de burgers, de consumenten, de werknemers 'gedwongen' steeds meer zelf via het internet te regelen en neemt het aanbod van de digitale dienstverlening, die tijd en plaats onafhankelijk is, hand over hand toe. Denk bijvoorbeeld aan de diverse betalingsmogelijkheden, die als paddenstoelen uit de grond schieten en aan alle 'apps' om je huis 'slimmer' te maken. Tegenwoordig is het vreemd als je thuis geen computer hebt staan en je niet beschikt over een smartphone. Een stroomuitval in Nederland en/of een wereldwijde internet storing is desastreus.

IT is de afkorting voor Informatietechnologie, ook Informatie- en Communicatie Technologie (ICT) genoemd. Het is een vakgebied dat zich bezighoudt met informatiesystemen, telecommunicatie en computers. Hieronder valt het hele scala van 'ontwikkelen' en 'beheren' van systemen, netwerken, databanken en websites evenals onderhoud van de computers en de programmatuur en het schrijven van de software.

Waar komen al die IT ontwikkelingen vandaan? Wat betekenen die voor de financiële professional. Waar staan we vandaag de dag en waar gaan wij naar toe?

1.1 IT in historisch, huidig en toekomstig perspectief, in vogelvlucht

1.1.1 Historisch perspectief

Geschiedkundig gezien, heeft de mens altijd gezocht naar hulpmiddelen om berekeningen te kunnen maken. Je kunt concluderen dat 'de mens' eigenlijk de eerste computer op aarde was op het moment dat zij of hij het sterrenstelsel ging analyseren. Alles wordt, in eerste aanleg, met het 'mensenhoofd' berekend en ontworpen. Denk aan de eerste

landkaarten die in het begin van de 19e eeuw door middel van cartografie[1] werden opgesteld. Fascinerend!

Al in 1833 komt er een eerste ontwerp voor een machine[2] die aan de hand van ponskaarten wiskundige berekeningen kan uitvoeren. Een belangrijk detail voor alle dames onder ons: Augusta Ada Byron[3] raakt geïnspireerd en bevlogen door dit ontwerp en wordt de grondlegster van het allereerste computerprogramma. Begin jaren 50 van de vorige eeuw worden de eerste computers in gebruik genomen. In die tijd zijn er al zorgen in hoeverre dit 'elektronische brein' de mens zou kunnen gaan verdringen. Eind jaren 80 komen de computers overal in beeld. De 'typekamers' verdwijnen en alle medewerkers binnen een onderneming krijgen de beschikking over een eigen computer. In diezelfde periode doet ook de homecomputer zijn intrede. Maar pas met de komst van het internet (in Nederland vanaf 1996) neemt het thuisgebruik van computers een enorme vlucht. Zonder deze ontwikkelingen, zouden wij nu geen internet, tablets of mobiele telefoons hebben. Tegenwoordig bestaat er al een generatie, die zich niet meer een leven zonder mobiele (smart) telefoon kan voorstellen.

De ontwikkelingen in de IT gaan razendsnel. Zo kennen we de 'Wet van Moore'. Hij voorspelt al in 1965 dat de vooruitgang in de IT elk jaar zou verdubbelen en hij heeft gelijk gekregen. De rekenkracht van de computers blijft alsmaar toenemen[4] en de opslagcapaciteit voor gegevens (data) begint oneindig te lijken.

1.1.2 Huidig perspectief

In de jaren 90 komen de eerste Enterprise Resource Planning (ERP) pakketten op de markt en worden er concrete stappen gezet om de bedrijfsprocessen te automatiseren. In eerste aanleg zijn de ERP pakketten bedoeld voor grote ondernemingen. Tegenwoordig zien we dat er voor middelgrote en kleine ondernemingen tevens ERP oplossingen zijn.

Binnen een ERP pakket is er sprake van één centrale database waar alle bedrijfsprocessen, zoals verkoop, inkoop, productie, salarisadministratie en financiële administratie met

1 Onthoud alvast dat de kunst van de cartografie kan worden vergeleken met Process Mining.
2 Charles Babbage (1791-1871) ontwerper van de eerste geautomatiseerde programmeerbare, mechanische rekenmachine, de voorloper van de elektronische computer.
3 Augusta Ada Byron (1815-1852).
4 De verwachting (volgens IBM) is dat de commerciële quantum computers over vijf jaar beschikbaar zijn.