‘Lessons learned’

Verslag van de zesde Rijksbrede IT-auditdag door EAP

EDP Audit Pool (EAP) organiseerde op 3 oktober in Den Haag de zesde Rijksbrede IT-auditdag. Het grootste deel van de IT-auditors werkzaam bij de rijksoverheid was aanwezig op deze dag.

Mw. drs. ing. N.D. Timmer en **drs. P.A. Doorduin RE** zijn als IT-auditor werkzaam bij EDP Audit Pool in Den Haag en maakten deel uit van de organisatie van dit symposium.

Leren is een belangrijk thema, zowel in de maatschappij als in het IT-audit vak. Vanouds hebben wij als beroepsgroep de verplichting om de ontwikkelingen te volgen en onszelf bij te scholen. Maar niet alleen op het terrein van de eigen kennisontwikkeling kunnen lessen geleerd worden.
De audits die wij uitvoeren, zorgen ook voor lessen voor de organisatie. Hoe gaat zij met deze lessen om?

Jeanot de Boer, directeur van EDP AUDIT POOL, opende de dag en heette de aanwezige IT-auditors welkom. Vervolgens gaf hij het woord aan de dagvoorzitter Ron Tolido die opende met het schetsen van het beeld dat hij van een IT-auditor heeft. Tolido ziet de IT-auditor als een serieus persoon, een beetje een zorgelijk type dat grote behoefte heeft aan structuur en analyse. Goede eigenschappen die hij zelf helaas minder bezit. Daarna gaf Ron een inleiding in het thema van de dag ‘Lessons Learned’. Geleerde lessen een lekker breed thema waar veel onder kan vallen. Daarbij onderstreepte hij het belang van blijven leren. Het blijven leren sluit goed aan op een van de doelstellingen van de Rijksbrede IT-auditdag, het delen van kennis.
Na de opening van de dag en de introductie in het thema volgden er twee plenaire lezingen.

Risico’s in theorie, lessen voor de praktijk

Gert van der Pijl (Erasmus School of Accounting & Assurance)

Gert van der Pijl begon zijn lezing met een korte introductie in het onderwerp Enterprise Risk Management. Maar wat is een risico, hoe schatten we het risico in en hoe waarderen we risico’s? Er bestaan standaard formules om het risico te bepalen, maar de mens kent beperkingen in het verwerken van variabelen. Ook speelt het persoonlijke risicoprofiel een grote rol in het bepalen van risico’s. Er zijn onderzoeken gedaan naar het inschatten van risico’s door accountants, hieruit blijkt dat binnen deze beroepsgroep verschillende risico-inschattingen gemaakt worden. Binnen het IT-audit vak is er nog geen onderzoek naar risico-inschatting gedaan. De vraag is hoe we op een goede manier met deze vragen kunnen omgaan. De conclusie van deze lezing was dat er een nadere explicitering binnen het vakgebied zal moeten plaatsvinden. Daarnaast moet er veel overleg plaatsvinden en, niet in de laatste plaats, moet er gerelativeerd worden.

Stemcomputers

Bart Jacobs (Radboud Universiteit te Nijmegen en Technische Universiteit van Eindhoven)

In juli 2006 is een actiegroep de discussie over de betrouwbaarheid van stemcomputers gestart. De actiegroep heeft een ‘oude’ stemmachine gekocht en omgebouwd tot schaakcomputer om te bewijzen dat deze machines niet alleen gebruikt kunnen worden voor de opslag van stemmen, maar ‘echte’ computers zijn met alle beveiligingsrisico’s van dien. Naar aanleiding van de discussie over de betrouwbaarheid van de stemmachines die gebruikt worden bij de Nederlandse verkiezingen is de ‘adviescommissie inrichting verkiezingsproces’ ingesteld. Bart Jacobs is lid van deze commissie. De grootste problemen bij het gebruik van stemcomputers zijn dat het voor de stemmer niet controleerbaar is of zijn stem juist is uitgebracht en dat een hertelling niet mogelijk is. Bart heeft een tipje van de sluier opgelicht over het uitgebrachte advies. In het advies wordt de stemmer centraal gesteld.

De stemmer geeft zijn stem via de stemcomputer, deze slaat de stem niet op maar print de stem uit. De stemmer kan dan zijn stem controleren en de stemmen kunnen automatisch geteld (en herteld) worden door het gebruik van Optical Character Recognition (OCR). Tot de implementatie van de stemprinter zal er gestemd worden via het vertrouwde papieren stemmen.

Na de plenaire sessies volgde een parallelle sessie van een viertal workshops. In deze workshops stonden ervaringen uit de praktijk centraal. De workshops werden begeleid door medewerkers van EDP AUDIT POOL en diverse gastsprekers.

Oracle Application Server als leerdoel

Ton Stevenhagen en John Zuidweg (beide EAP)

Oracle Application Server (OAS) is volop in ontwikkeling. Het is een verzamelnaam voor een architectuur die meer dekt dan de naam doet vermoeden. Tijdens deze workshop hebben Ton en John verteld over de geleerde lessen uit onderzoeken naar het Oracle Database Management Systeem en de relatie naar OAS gelegd. Zij hebben tevens voor de deelnemers een tipje van de sluier van OAS opgelicht, waarin de nieuwe architectuur van OAS is uitgelegd en aan de hand van eigen ervaring aangegeven welke risico's te onderkennen zijn. Tot slot hebben zij verteld op welke wijze een IT-audit uitgevoerd kan worden en wat de aandachtspunten hierbij zijn. Centraal in de workshop stonden de componenten identity management en webinterfaces, deze spelen een belangrijke rol bij het gebruik van OAS.

Succesvol een mijnenveld oversteken

Loubna Zarrou (EAP) en Roger Gerardts (OT2006)

Overheidsorganisaties zijn vanaf een bepaalde drempelwaarde verplicht een inkooptraject te laten verlopen via een Europese Aanbesteding. Europese Aanbestedingen kennen een eigen dynamiek door de vaak grote belangen die er spelen en de complexe omstandigheden en randvoorwaarden die de regelgeving met zich meebrengt. Roger is ingegaan op de uitdagingen die hij is tegengekomen bij Europese Aanbestedingen binnen de rijksoverheid. Daarnaast heeft hij toelichting gegeven welke rol de IT-auditor kan vervullen in de Europese aanbestedingstrajecten. Aan de hand van stellingen zijn de deelnemers uitgedaagd mee te denken over de mogelijke problemen, oplossingen en invulling van de rol van de IT-auditor bij een Europese Aanbesteding.

Het organisatiegeheugen van de overheid blijvend digitaal beschikbaar

Paul Scholte (V&W), Hugo Butter (ICTU) en Boudien Glashouwer (HEC)

Waar loop je tegenaan bij het digitaliseren van een archief? De sprekers zijn aan de hand van eigen ervaringen ingegaan op de geleerde lessen bij de ontmanteling van een ZBO. De belangrijkste leerpunten waren het van te voren vaststellen van de bewaarvraag en het de schoning. In dit project is men van 13 kilometer gestapelde A4 naar 350 meter gegaan en is de 15 terabyte aan gegevens 115 gigabyte geworden. Daarna hebben de sprekers ook een blik op de toekomst geworpen door een korte introductie op de baseline informatiehuishouding en de rol van de IT-auditor in de kwaliteit van de informatiehuishouding. De workshop is afgesloten met een lijst aandachtspunten voor de IT-auditor.

FileNet

Ron van 't Boveneind en Marcel de Bruijn (beide EAP)

Voor de digitalisering van de documentenhuishouding heeft een aantal departementen de krachten gebundeld en na een Europese Aanbesteding gekozen voor FileNet voor het beheren van digitale documenten. Maar wat is nu FileNet en wat kun je ermee? Ron en Marcel hebben een korte introductie gegeven in de 8 componenten van FileNet en hun mogelijkheden. Daarna hebben ze aan de hand van een succesvolle FileNet implementatie bij een departement, de geleerde lessen met het uitvoeren van een FileNet-audit gedeeld. Er zijn binnen FileNet veel mogelijkheden tot geprogrammeerde controles, logging en overzichten, maar de beschikbare kennis is schaars. De belangrijkste geleerde les is dat het inrichten van de workflow specialistenwerk is, waarbij een nauwe samenwerking tussen IT en organisatie van belang is.

Nieuwe technologie in spelen, spelen met nieuwe technologie

Tinus Jongert (TNO)

Aan het begin van de middag verzorgde Tinus Jongert een plenaire lezing. Omdat niet alleen IT-auditors continu leren, heeft Tinus verteld over de lessen die TNO heeft geleerd tijdens het uitvoeren van hun onderzoeken. Kennis ontwikkelen, integreren én toepassen: die combinatie onderscheidt TNO van andere kennisinstel-

business continuity planners

Groei mee met de vernieuwing

Dé onafhankelijke specialisten in Business Continuity Planning introduceren nieuwe integrale softwareondersteuning voor Business Continuity Planning en Business Continuity Management.

Wij zoeken:

IT auditors die zich willen specialiseren in Business Continuity Planning

Wij bieden:

Unieke, multidisciplinaire projecten bij toporganisaties binnen bedrijfsleven en overheid
Ruimte voor ontwikkeling binnen deze groeimarkt en in dit jonge vakgebied
Een vrije werkomgeving in een jonge organisatie
Uitstekende arbeidsvoorwaarden / winstdeling

Stuur een brief met motivatie en CV naar Business Continuity Planners, J.F.M.Roest RE RA, Spyridon Louisweg 93, 1034 WR, Amsterdam / info@businesscontinuityplanners.nl

---

"Operational Risk? Your way!"

Euroclear is the world's largest provider of domestic and cross-border settlement and related services for bond, equity and fund transactions. Market owned and market governed, the **Euroclear** group comprises Euroclear Bank, based in Brussels, as well as Euroclear France, Euroclear Nederland, Euroclear UK & Ireland and Euroclear Belgium, the central securities depositories of France, the Netherlands, the UK and Ireland and Belgium, respectively. Employing more than 2000 highly skilled professionals of 47 nationalities, **Euroclear** offers an international work environment. Offices are located in 9 different cities, with headquarters in Brussels.

For the Euroclear S.A. Risk Management Division we are looking for a

Risk Manager (Amsterdam)

Description: This position offers an excellent overview of the businesses of Euroclear. You will have the opportunity to improve Operational Risk Management, Security, and Business Continuity and drive real value into the company.

Tasks and responsibilities: • Advice Local Management on risk matters • Provide daily support to Business Managers like Self-Assessment process delivery, guardianship of Operational Risk databases for collection of incidents and issues, and support in crisis resolution and response to incident • Responsible for Operational Risk Management oversight and control • Perform impact analyses on Basel II • Maintain an overview of all issues relating to Security and Business Continuity • Prepare and maintain the company's Business Continuity Plans • Liaise between the Netherlands & Euroclear Group with regards to Operational Risk Management, Security and Business Continuity • Actively participate in various projects.

Profile: • A recognized degree in Business Economics or Accountancy, ideally complemented with a postgraduate degree in accounting or auditing (RA/RE/RO/CPA/CIA or equivalent) • Around 3 years relevant working experience • Good general knowledge of financial industry and risk or control-related issues • Good communication and social skills • Analytical skills, critical mind • General Risk Management experience • Experience with Basel II, Security Management and Business Continuity planning • Fluent in English en Dutch.

Contact: For questions regarding the application procedure please contact drs. L. Becka on 020-530 15 72 or Liza.Becka@Euroclear.com. For questions regarding the details of the position please contact drs. O.V. Nijland RE CISA on 06-5115 18 72 or Olivier.Nijland@Euroclear.com

www.euroclear.com

AMSTERDAM • BRUSSELS • FRANKFURT • HONG KONG • LONDON • NEW YORK • PARIS • SÃO PAULO • SINGAPORE • TOKYO

euroclear

The other face of finance

lingen. Doordat TNO kennisgebieden effectief met elkaar laat samenwerken, komen zij tot creatieve en praktijkgerichte innovaties: nieuwe producten, diensten en processen, op maat gesneden voor klanten bij bedrijfsleven en overheid. Tinus legt uit dat het werk van TNO daarom niet veel verschilt van IT-audit. Voor beide zijn kennis en een goede onderzoeksaanpak belangrijk om tot juiste conclusies te komen. Tinus legt aan de hand van een casus uit hoe TNO kennis gebruikt voor het continu verbeteren van oplossingen voor maatschappelijke problemen. Obesitas (overgewicht) is een steeds groter probleem bij Nederlandse kinderen. Volgens TNO komt dit vooral doordat kinderen steeds minder bewegen. De oorzaak hiervan is te vinden in de omgevingsdeterminanten (bijvoorbeeld computergebruik en de steeds onveiliger wordende woon- en speelomgeving). Hiervoor heeft TNO nieuwe speelconcepten ontwikkeld door gebruik te maken van innovatieve technologie. Dit speelgoed is getest door kinderen, zodat TNO hiervan kon leren en aanpassingen kon doen om de functionaliteit van het speelgoed te optimaliseren. Het resultaat zou volgens Tinus zijn dat kinderen meer zullen gaan bewegen. Hij merkt echter wel op dat een goede innovatie niet automatisch (blijvend) wordt gebruikt. Ook hier ligt weer een parallel met de IT-auditor, die ervoor moet zorgen dat de geleerde lessen uit een onderzoek blijvend gebruikt worden.

Na deze lezing volgde weer een parallelle sessie van vier workshops.

Basisregistraties: eens gegeven, altijd één gegeven

Ender Atalay, David Campbell en Jan Roodnat (allen EAP)

Om haar werk te doen, heeft de overheid gegevens nodig. Véél gegevens, vastgelegd in maar liefst 30.000 verschillende systemen. Dat moet anders. Minder versnipperd, eenvoudiger. Basisregistraties zijn hierop het antwoord van de elektronische overheid in de zoektocht naar een efficiëntere en betrouwbaardere informatievoorziening voor de diverse overheidsorganisaties. David en Ender gingen tijdens de workshop kort in op de betekenis en de impact van basisregistraties voor de IT-auditor. Daarna werd op er aan de hand van een quiz gediscussieerd over basisregistraties. Uit deze discussie werd duidelijk dat er nog veel werk ligt voor de IT-auditor. Basisregistraties voor de overheid worden in de toekomst weliswaar verplicht gesteld, maar strakke richtlijnen over basisregistraties, zoals afspraken over de kosten eigendom en verantwoordelijkheid, ontbreken nog.

VIR2007

Marcel Spruit (HEC en HHS), Kees van der Maarel en Chantal de Vette (beide EAP)

Het Voorschrift Informatiebeveiliging Rijksoverheid (VIR) stamt alweer uit 1994. Door de ontwikkeling werd het hoog tijd voor een nieuwe versie, het VIR 2007. Kees en Chantal gingen tijdens de workshop kort in op de verschillen tussen het oude en nieuwe VIR. Zij gaven aan dat in het nieuwe VIR gesproken wordt over het uitvoeren van een risicoanalyse (voorheen de A&K analyse) door het lijnmanagement. Aan de risicoafweging (lees: risicoanalyse) worden echter geen eisen gesteld, behalve dat deze expliciet is. Marcel Spruit nam de deelnemers vervolgens mee op reis naar de verschillende soorten tools voor risicomanagement die gangbaar zijn binnen de overheden in Europa. Hij gaf aan dat een A&K analyse nog steeds mag worden uitgevoerd, maar dat risicomanagement meer inhoud dan slechts het uitvoeren van deze analyse. Risicomanagement is naast risicoanalyse ook: 'maatregelen treffen', 'restrisico's accepteren' en 'communiceren en afstemmen' van deze keuzes in de informatiebeveiliging binnen de organisatie. De conclusie van zijn betoog was dat risicomanagement dus meer inhoudt dan risicoanalyse.

Governance en informatievoorziening

Rob Kramer en Paula Velthuys (beide Archiefinspectie)

Wanneer iemand aan een archief denkt, krijg je toch al snel associatie met oude papieren. Dat deze associatie niet juist is, maakten Rob en Paula tijdens deze workshop duidelijk. Overheidsinformatie zoals vastgelegd in archieven is in toenemende mate digitaal. Dat betekent dat de Erfgoedinspectie, die belast is met

ControllersMagazine

PRESENTEERT IN SAMENWERKING MET KENNISPARTNER **ORCHARD FINANCE CONSULTANTS**

ORCHARD FINANCE

CONGRES WERKKAPITAAL MANAGEMENT 2007

DONDERDAG 13 DECEMBER 2007 → NH CONFERENCE CENTRE LEEUWENHORST → NOORDWIJKERHOUT

DAGVOORZITTER **PETER VAN ZADELHOFF** PRESENTATOR BNR NIEUWSRADIO

PROGRAMMA

WERKKAPITAAL BELICHT VANUIT DIVERSE PERSPECTIEVEN, MET O.A.:

- Supply Chain Financing
- E-billing
- LEAN principes
- Purchase to Pay automatisering
- Decentraal werkkapitaalmanagement
- Trends in werkkapitaalfinanciering
- Outsourcing & Supply Chainmanagement
- Invloed incentivesystemen
- Automatische reconciliatie
- Securitisatie
- Creditmanagement
- Organisatie Supply Chain

PRAKTIJKCASES

- Zara
- Foot Locker
- Friesland Foods
- 3M
- De Meeuw Bouwsystemen
- Leaseplan
- TBI Holdings
- Sparck Hypotheken

KEY NOTE SPEAKERS

- **Jan Peter Kerstens,** CFO Endemol
- **Eelco Spaans,** COO Koninklijke Gazelle

- INSPIRERENDE EN LEERZAME BEST PRACTICES
- ONTMOET VAKGENOTEN
- FILEVRIJE TIJDEN
- 5 PE PUNTEN
- VROEGBOEKKORTING

MEER INFORMATIE EN AANMELDEN VIA

WWW.WERKKAPITAALMANAGEMENT.NL

Hoofdsponsor

LINDORFF
Confidence in Commerce and Credit

Sponsor

ING

Co-sponsors

AON trintech raising revenue · reducing risk BasWare anachron®

Reed Business

het toezicht op de archieven van de centrale overheid, meer kennis moet hebben van digitalisering en substitutie (het vervangen van originele bescheiden door reproducties). De archiefinspecteur voert dan op het gebied van de informatiehuishouding werk uit dat vergelijkbaar is met dat van de IT-auditor, maar vanuit een andere doelstelling. Daarom werd in de workshop stilgestaan bij het toenemende belang van de I(nformatie) functie ten opzichte van de F(inanciële) functie. In de financiële wereld is een goed systeem van verantwoording de normaalste zaak van de wereld. Dit is nog niet altijd zo in de wereld van de informatievoorziening. Gezien de ontwikkelingen in het informatielandschap is het bijna vanzelfsprekend dat overheidsinformatie ondergebracht moet worden in het systeem van verantwoording, audit en control. IT-auditors zullen steeds meer te maken krijgen met informatievoorziening, digitaliseringprojecten en substitutie.

Ontwikkeling IT-audits

Jeanot de Boer en Xander Bordeaux (beide EAP)

Op 1 januari 2008 bestaat EDP AUDIT POOL 20 jaar. Dat betekent 20 jaar ervaring met het uitvoeren van IT-audits. Sinds de oprichting van EAP in 1988 hebben verschillende discussies plaatsgevonden over de positie en het werkgebied van EAP binnen de Rijksoverheid. Parallel aan deze ontwikkelingen vinden ook veranderingen plaats binnen het auditgebied. Jeanot en Xander nemen de deelnemers van de workshop mee terug in de tijd aan de hand van de 'road to happyland' (Kor Mollema) toen IT-audit (EDP Audit) nog in de kinderschoenen stond. De discipline IT-auditing is ontstaan vanuit de financiële audit en had toen een 'in control' focus. IT-auditing is uitgegroeid van specialisatie van een accountant tot een vakgebied met eigen beroepsorganisatie waarbij het een volwaardige gesprekspartner met het management is geworden op strategisch niveau. Tijdens de workshop werd uitvoerig gediscussieerd over de huidige werkzaamheden waarbij duidelijk werd dat toch nog steeds veel audits ingestoken zijn vanuit de financiële hoek. Ook passeren nieuwe ontwikkelingen als integrated en strategy based auditing de revue waarbij de in het publiek aanwezige Ronald Paans en Gert van der Pijl ook hun visie gaven. Via stellingen nodigden Jeanot en Xander de deelnemers uit om te reageren op de toegevoegde waarde van de IT-auditor. Allen waren het er natuurlijk over eens dat de IT-auditor toegevoegde waarde heeft voor het management, maar wel vanuit verschillende visies en met verschillende argumenten.

Forumdiscussie

Ronald Paans en Gert van der Pijl blikten terug op de Rijksbrede IT-auditdag. Zij hebben veel gehoord, maar konden vanwege de tijd niet alles behandelen. Eerst stonden zij stil bij de risico-inschatting van IT-auditors. Gert heeft aan het begin van de dag verteld dat risico's erg moeilijk in te schatten zijn. Ronald bevestigt dit en illustreert dit met voorbeeld: hij heeft eens de kerstdagen doorgebracht met een matrix van 5600 velden voor een SOX-audit. Hierin stonden de deelrisico's vermeld, maar het totaalrisico was niet de optelsom van alle deelrisico's. De vraag is dan ook hoe een IT-auditor dan het totaalrisico bepaalt? Dit is niet slechts het toepassen van de formule R = P * I (het risico is de kans dat iets optreedt maal de impact die het heeft als het optreedt). Door de veelheid aan beheersmaatregelen en risico's en de complexiteit, is het voor de IT-auditor zeer moeilijk om een totaalrisico in te schatten.

Ook digitalisering kreeg de aandacht. Een belangrijk aandachtspunt bij digitalisering is de (digitale) duurzaamheid. Volledige archieven worden opgeslagen op één of meerdere dvd's, maar wat is de uiterste houdbaarheidsdatum van een dvd? Een dvd kan na vijf jaar niet meer leesbaar zijn. Leg de dvd in de zon en de levensduur wordt aanzienlijk verkort. En waarom zou men dvd's gebruiken als een microfiche een levensduur van 150 jaar heeft? De conclusie hierbij was dat nadenken over de duurzaamheid van opslag erg belangrijk is en dat nieuwe technologieën niet altijd beter zijn.

Tot slot

Na de forumdiscussie rondde dagvoorzitter Ron Tolido de dag af met een korte samenvatting. Hij gaf aan dat het voor hem ook een leerzame dag is geweest. Hij kon met een nieuwe woordenschat weer terug naar huis, alwaar hij indruk kon maken met woorden als obesotene sfeer (van obesitas) en omgevingsdeterminanten. Ook het inschatten van risico's blijft een moeilijk punt. De IT-auditor moet dus blijven leren en de geleerde lessen daarna in praktijk brengen.

Voor meer informatie en alle presentaties, zie www.eap.nl