IT-Auditorsdag 2014

De ISACA/NOREA IT-Auditorsdag van 25 september 2014 stond in het teken van:

Governance, Risk & Compliance in Europees Perspectief.

In toenemende mate zijn IT-auditors betrokken bij GRC-activiteiten en processen, die sterk worden beïnvloed door Europese wet- en regelgeving als Solvency II, Basel III en de introductie van het Europees bankentoezicht. De impact van de Europese Privacy-verordening en de Cybersecurity Strategie wordt merkbaar, o.a. in de gezamenlijke initiatieven ter bestrijding van Cybercrime.

In diverse presentaties werd ingegaan op deze ontwikkelingen en stilgestaan bij het belang van Data-analyse en Datakwaliteit. Ook werd ingegaan op de betekenis van COBIT 5 voor Risk & Compliance.

Dagvoorzitter was **Job Stierman,** oud-bestuurslid van ISACA.

De presentaties werden verzorgd door:

- **Albert Kisjes** RE en **Ruben Moorlag** (Agilos, Center of experts 4 GRC 2) over trends en ontwikkelingen op basis van 13 (eerder gepubliceerde) GRC Survey rapporten.
  Daaronder waren onderzoeken van leveranciers, van de Big 4 en van meer onafhankelijke partijen, zoals OCEG, Open Compliance and Ethics Group, (zie www.oceg.org) die zich inmiddels ook bezighouden met performance management, risk management, governance and assurance. Ruben Moorlag heeft zich als Master in Bestuurskunde (TU Delft) bezig gehouden met dit vergelijkend onderzoek, o.a. begeleid door Albert Kisjes. Enkele conclusies waren: we moeten het discipline overstijgende GRC onderzoek niet motiveren vanuit angst (voor non-compliancy bijvoorbeeld), maar eerder vanuit Performance (verbeterkansen). Verder is afstemming van de terminologie, semantiek en taal nodig; er wordt nog teveel in silo's gedacht (er zijn nog weinig voorbeelden van ICF's, Integrated Control Frameworks).

- **Freddy Dezeure** (Head of Computer Emergency Respons Team EU) over praktijkervaringen met cybercrime.
  Freddy Dezeure is hoofd van het CERT-EU dat sinds juni 2011 (ingesteld door Neelie Kroes) bestaat. Hij ging in op Advanced Persistence Threats (APT's) en Pass to Hash (PtH) risico's en de noodzaak tot samenwerking tussen landen, maar ook tussen bedrijven. Ze publiceren ook interessante Whitepapers: zie cert.europe.eu.

- **Evert Koning** RE RA (DNB) over ontwikkelingen inzake Europees bankentoezicht.
  Evert Koning deelde als bestuurslid van NOREA mee dat op de website het Visie 2020 document van de commissie Donkers (onder leiding van oud-voorzitter Hans Donkers) te vinden is. Kern daarvan is dat het Audit beroep breder is geworden, behalve IT Audit ook IT Governance, en dat NOREA als Beroeps-organisatie meer samenwerking wil zoeken en aangaan.

Als Hoofd van het Expertisecentrum IT van de DNB ging hij vervolgens in op de organisatieveranderingen binnen DNB (en ECB, Europese Centrale Bank).
Er zijn Frameworks ontwikkeld (SSM, SRM, DGS) die een nieuw stelsel van Bankentoezicht introduceren, zie het filmpje van 3 minuten op https://www.ecb.europa.eu/ssm/html/index.nl.html. De ECB begint in november 2014 met haar nieuwe toezichthoudende taken. Er zijn in de EU 130 banken aangeduid als significant, daaronder 7 in Nederland, waarvan er 3 in feite onderdeel zijn van een moederorganisatie buiten Nederland.

Nieuw is ook dat er ook onsite diepte onderzoek gedaan kan gaan worden, verder zijn er nieuwe 'reporting frameworks' ontwikkeld. Vanuit de ECB Frankfurt zullen er vanuit 4 Directoraten-Generaal met zo'n 800 medewerkers toezichthoudende taken worden uitgevoerd. Er zal gewerkt worden met zogenaamde JST's (Joint Strategy Team's) die bepalen wat er onderzocht gaat worden, waarna het onderzoek plaatsvindt door een onafhankelijk team onder leiding van een HoM (Head of Mission). Er lopen onderhandelingen om ook via het Right to Execute en het Right to Audit in de keuken van leveranciers te mogen kijken (SAAS).

- **Ger Roeleven** RA (DNB) over Data Quality
  Na de pauze gaat de collega van Evert Koning bij de DNB, Ger Roeleven, nader in op de intensivering van het Data onderzoek door de DNB en ECB. Waar Basel I nog vooral Principle Based was, Basel II in de periode van 2007-2013 vooral Risk based was, zal in Basel III (generatie 3) het onderzoek niet alleen data/gegevensgericht zijn, maar ook systeemgericht. Behalve Opzet en bestaan ligt het accent ook veel meer op Werking (in Audit terminologie). Bovendien zal veel meer detail worden gevraagd (tot wel 4 maal zoveel data als voorheen). De rapportage zal plaatsvinden in Dashboards, ook de aanlevering van data zal worden gemoderniseerd (XBRL), zodat de checks in 10 werkdagen kunnen plaatsvinden door de ECB.

- mr. **Maurits Westerik** (Partner Bird&Bird LLP) over EU-Cybersecurity Strategie
  Maurits Westerik ging nader in op de komende te verwachten wet- en regelgeving vanuit Europa. Nu de EU commissie met een directoraat ENISA en via Publiek-Private Samenwerking (PPS) de Cybersecurity strategie lijnen uitzet, is de verwachting dat er straks een NIS Directive komt (NIS= Network and Information Security). Die zal waarschijnlijk gaan inhouden dat er een Meldplicht komt voor Security Incidenten, waarna je (verplichte) hulp krijgt, het incident wordt gedeeld (via een zogenaamd NIS Platform, met andere landen en de lokale 'NCSC's). Als je het niet doet, volgen er boetes, maar ook aansprakelijkheid op basis van 'due care' (= zorgplicht). Mogelijk zelfs aangeduid als 'onrechtmatige daad' volgens art.162, dus als hoofdelijke bestuurlijke aansprakelijkheid!
  Via amendementen is de werksfeer momenteel beperkt, hij geldt niet voor burgers, niet voor MKB bedrijven, wel voor 'significante' private en publieke partijen.

- **Andreas Weller** (EBA=European Bank Authority) over regelgeving inzake Europees Bankentoezicht
  De EBA zetelt in Londen (niet in Frankfurt) en ziet ook toe op niet-EU banken (bijvoorbeeld Zweden).
  Er is een EU Single Rulebook ontwikkeld gebaseerd op CRD generatie IV(CRD=concentratie risico management), aangevuld met regels voor IT assets. Daarnaast ontwikkelde de EBA de SREP guidelines, richtlijnen voor review en evaluatie. En tot slot hebben ze de ITS ontwikkeld (ITS= Implementing Technical Standards, using XBRL for reporting).

- prof. **Wim van Grembergen** (Universiteit van Antwerpen) over de betekenis van COBIT 5 voor Risk & Compliance.
  Wim van Grimbergen ging nader in op het onderscheid tussen Governance en Management, tussen 'ensure dat' zaken gebeuren op basis van (bestuurlijke) aansprakelijkheid en anderzijds daadwerkelijk het regelen en (toezien op) de uitvoering van zaken (verantwoordelijk zijn als management voor). Ook maakte hij erg duidelijk dat COBIT5 een aantal ISO standaarden heeft geadopteerd. Zoals ISO 31000, Risk Management, ISO38500, Corporate Governance en ook ISO15504, het Maturiteits model. COBIT5 is heel bewust omschreven als model voor Enterprise Governance for Information Processing. Het is niet alleen relevant en bruikbaar voor Corporate organisaties (bedrijfsleven) maar ook voor Public Enterprises. Bovendien gaat het over Governance en dat is meer dan dar waar het in COBIT4 nog vooral Management guidelines betrof.

Tot slot: de verzorging van de lunch, buffet, koffie, drankjes en dergelijke was als vanouds weer zeer goed verzorgd voor de ruim 200 deelnemers aan IT Auditors dag van NOREA en ISACA.