Third Party Assurance Reports

Kritische blik op het gebruik van Third Party Assurance rapporten

Voorstellen

- Jan Joost Bierhoff
- Internal Audit Heineken Nederland
- EDP Audit opleiding aan VU afgerond in zomer 2008
- EDP Interesse
  - Third party assurance
  - Identity & Access Management
- Persoonlijke interesse
  - Golf surfen
  - Amsterdam

Scriptie

- *How will an IT auditor be able to form a sound opinion of outsourced IT processes and related controls, based on IT assurance reports*
- Frank Herruer – Deloitte Enterprise Risk Services
- Tjakko de Boer – Itegrity
- Robert Boon – Deloitte Enterprise Risk Services
- Interviews bij:
  - Deloitte
  - Noordbeek
  - KPMG
  - ITegrity
  - PWC

Postkantoren BV	Getronics	
UWV	Interpolis	
ABN/AMRO	Translink	
Belastingdienst	KPN	
EDP Audit pool	Ahold	

Complexe situatie

- Complex IT landschap
- Vele verschillende derde partijen
- … soms zelfs subservices
- Vele verschillende rapportage middelen, o.a.:
  - Contracten
  - SLA i.c.m. SLR
  - TPM rapporten
  - SAS-70 rapporten

Ideale situatie

- Volledig overzicht
  - Overzicht van alle derde partijen
  - Overzicht alle risico's
  - Overzicht alle beheersmaatregelen
  - Overzicht bijbehorende taken/eigenaarschap/verantwoordelijkheden
    - Welke partij doet wat?
    - Dekt contract dit ook af?
  - 100% eenduidige, rapportage hierover

Mijn mening

- Moeilijk om oordeel te geven in ons huidige werkveld

Initiatie

- "*Expectation Management*"
  - Waarom vragen we een dergelijk rapport op
  - Waar liggen taken, verantwoordelijkheden en eigenaarschap
- Kennis van TPAR
- IT auditor moet betrokken zijn
  - 'Tolk' en begeleider bij gehele proces
  - Zekerstellen dat aansluiting aanwezig is bij ontvangen
- 1:1 vragen …
- … anders 1:N aansluiting van document bij eigen organisatie zeker stellen

Scope

- Alle uitbestede locaties, processen, applicaties en systemen in scope?

Control Standards

- *Risk based*
  - Vraag zekerheid over geidentificeerde risico's
- Principle based
  - Lever doelstellingen aan i.p.v. eigen gedetaileerde controle maatregelen "over de schutting te gooien"
  - Vraag eigen externe auditor om eventuele "*mapping"* te doen

- *"Bridge the gap"* indien document reeds aanwezig
  - Vergelijk doelstellingen en controle maatregelen met standaard raport van service organisatie met eigen set

Uitvoering en rapportage

- Zorg voor vertrouwen
  - In document (zie Initiatie)
  - In de uitvoerende IT auditor/instelling
- Streef naar een generiek TPAR
  - Zelfde mate van zekerheid
  - Zelfde steekproef grootte
  - Zelfde lay-out
  - Standaard normenkader
- Indien nodig, ... vul de generieke TPAR aan met een extra TPAR
  - Indien extra zekerheid noodzakelijk
  - Indien extra steekproef in aantallen of scope applicaties

Kritsiche blik IT auditor

- Wees kritisch op lokaal management!
- Wees kritisch op lokaal IT management!
  - Vraag naar overzicht van alle derde partijen
  - Vraag naar risico's die bij derde partijen liggen
  - Vraag naar een aansluitend overzicht contracten, SLA, SLR en TPAR
  - Vraag naar overzicht van taken, verantwoordelijkheden en eigenaarschap rondom deze risico's, kortom … wie doet wat!
- Wees kritisch op bevindingen van collega RE's, durf de discussie over bevindingen aan te gaan!
- Wees kritisch op subservices!
- Wees kritisch op vakgroepen!