Privacy gerelateerde assurance rapportage

Themadag Privacy

22 november 2017

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Topics

- Waarom een assurance–rapportages van een IT auditor
- Leerpunten uit het verleden
- Wat is beschikbaar
- Gebruik SOC 2© format
- Hoe verder?

Waarom een assurance-rapportages van een IT auditor

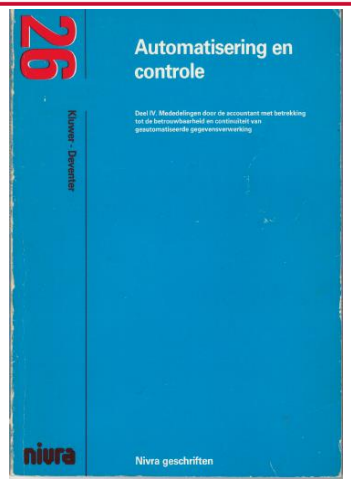
- Werkt op basis van IFAC standaarden
- Door NBA erkend als “andere professional” *)
- Geeft meer dan een certificaat, de IT auditor rapporteert
- Privacy beheersing is ‘proces en infrastructuur op orde’, het domein van de IT auditor
- Ervaren beroepsgroep:
  - Privacy Audit proof
  - Alles over data-lekken

<u>de</u> leverancier van inzicht en zekerheid

*) NBA Nadere Voorschriften accountskantoren - assurance

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

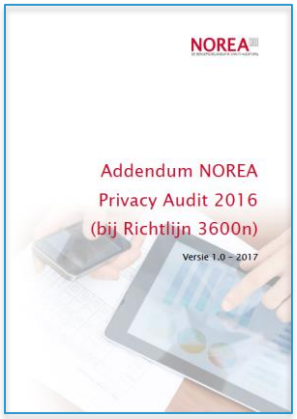
Leerpunten



- TPM / TPA, wie kent hem niet?
  - (Basis is NIVRA (NBA) geschrift 26 uit 1982)

Probleem, het is niet wat het lijkt.

- SAS 70
  - Amerikaanse standaard die niet meer bestaat
- ISO certificaat (27018:2014)
  - Geeft geen inzicht
- Privacy Proof / richtlijn 3600n (2006)



NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Wat zijn beschikbare rapportage-standaarden

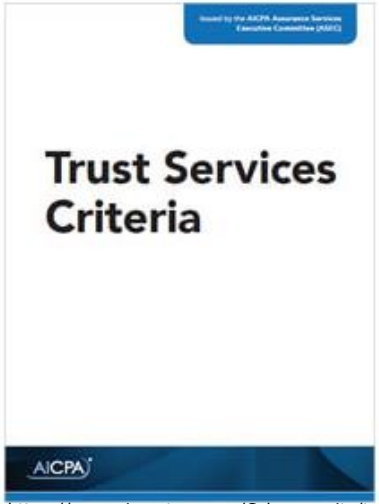
- Richtlijn 3000 (A & D)
  - ASSURANCE-OPDRACHTEN DOOR IT-AUDITORS
- Richtlijn 3402
  - ASSURANCE-RAPPORTEN BETREFFENDE INTERNE BEHEERSINGSMAATREGELEN BIJ EEN SERVICEORGANISATIE
- Richtlijn 4401
  - OPDRACHTEN TOT HET VERRICHTEN VAN OVEREENGEKOMEN SPECIFIEKE WERKZAAMHEDEN MET BETREKKING TOT INFORMATIETECHNOLOGIE

Bron:
https://pixabay.com/nl/driehoek-waarschuwing-blauw-36068/

ATTENTIE PUNT voor de audit professionals
3000 en 3402 zijn per 1 januari 2017 vernieuwd

SOC 2© format

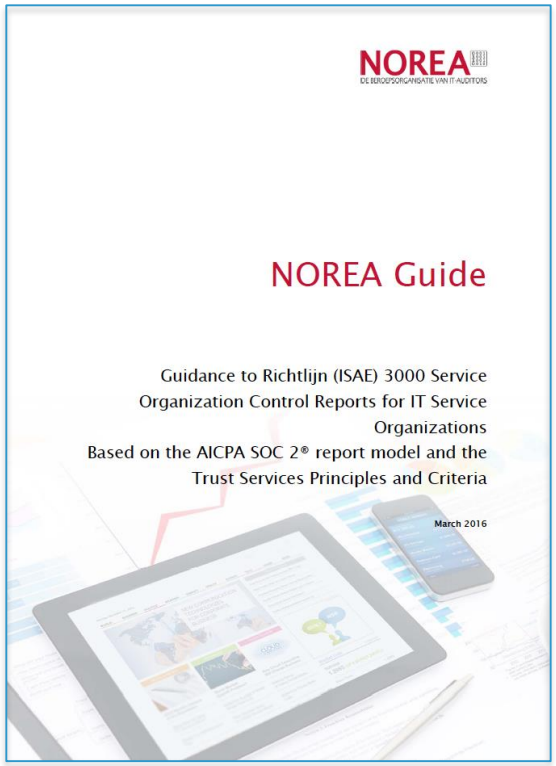
- SOC 2© (AICPA)
  - Reporting on Controls Relevant to:
    Security, Availability, Processing Integrity, Confidentiality, or Privacy
  - Vast rapportage model
  - Voor–gedefinieerde normen set: Trust Service Principles and Criteria
  - ~~Service Organization Control~~ –> System and Organizational Controls
  - Update TSP 2017 is beschikbaar (incl.US privacy regulations)



https://www.aicpastore.com/Cybersecurity/trust-services-criteria/PRDOVR~PC-TSPC13/PC-TSPC13.jsp

In deze vorm in Nederland **niet bruikbaar**!

Handreiking Service Organisatie Control (SOC) Rapporten



1. Introduction
2. ISAE 3000 / Service Organization Control
3. Conducting an ISAE 3000 / Service Organization Control Engagement
4. Use of ISAE 3000 / Service Organization Control Report
5. Principles and Criteria
6. ISAE 3000 / Service Organization Control versus other standards
7. Annex
    a. Management Statement
    b. Assurance report ISAE 3000
    c. Extract trust services principles and criteria
    d. Key references to guidelines, professional standards, articles and brochures
    e. List of contributors

Hoe verder?

Professie

- Ontwikkel rapport format
- Ontwikkel universele normenset (criteria)

Markt

- Vraag om een assurance–rapport
- Vraag om rapportage formaat
- Vraag om toepassing van een universele norm

https://pixabay.com/nl/zakenman-zakenvrouw-teamgeest-2753324/

Bedankt

Voor meer informatie kun je contact opnemen met:

Han Boer
Han@hanboer.nl / 06 537 454 37

22 november 2017

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS