Van Vertrouwen in de Cloud naar Zekerheid in de Cloud

Security congres

Hilversum, 6 oktober 2021

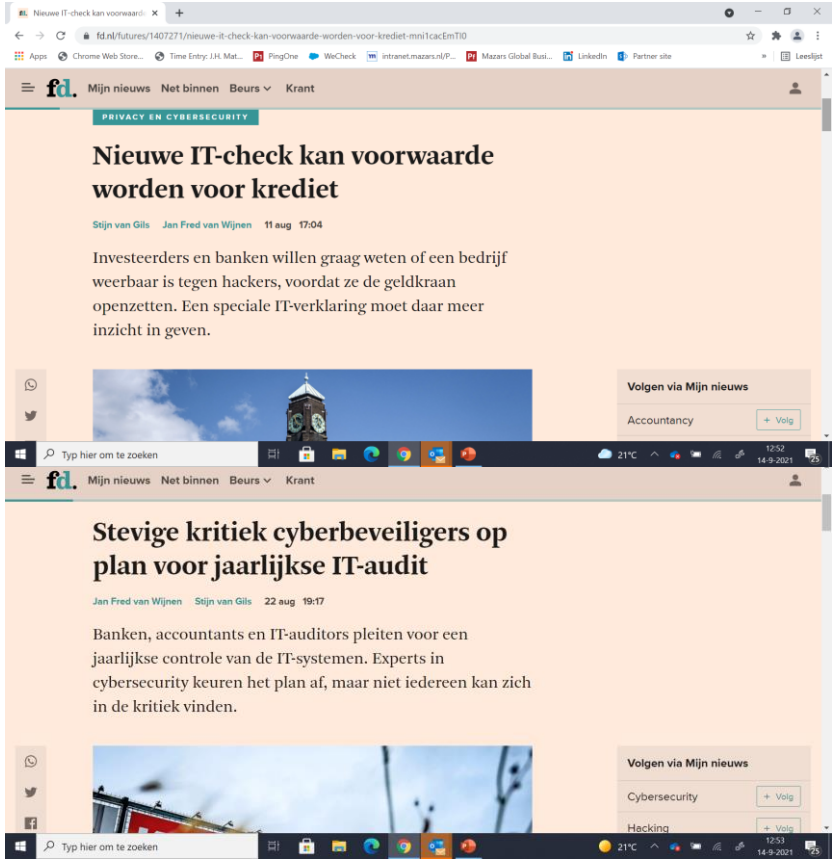
Jan Matto (Mazars / NOREA)

mazars

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Agenda

- 1) Setting the scene / aanleiding en achtergrond
- 2) Principes van de IT Auditverklaring
- 3) Vaktechnische onderwerpen en uitdagingen
- 4) Aanpak en projectgroep NOREA
- 5) Discussie



NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA IT Auditverklaring

DISCLAIMER:

De NOREA IT Auditverklaring is in ontwikkeling

NOREA IT Auditverklaring

1.1) Setting the scene / aanleiding en achtergrond

- Digitalisering is overall en daarmee een maatschappelijk relevant thema
- Raakt hele ecosysteem van een organisatie
- IT audit als integraal onderdeel jaarrekeningcontrole geeft een te beperkt beeld
- Focus van audit is traditioneel gericht op financiële processen en verantwoordingen
- Third Party Assurance (ISAE3000, 3402, SOC1,2,3) heeft een focus op uitbestede processen en is audit-to-audit

NOREA IT Auditverklaring

1.2) Setting the scene / aanleiding en achtergrond

➔ Diversiteit van stakeholders heeft belang bij zekerheid over digitalisering van een organisatie:

- RVC's, Toezichthouders, Aandeelhouders;
- Personeel, Cliënten, Individuen;
- (IT) service providers en onderaannemers;
- Keten- en netwerkpartners;
- Partijen met een breder maatschappelijk perspectief en economisch belang.

➔ Overheid en toezichthouders reageren vanwege juist dat bredere maatschappelijke en economische belang van digitalisering met meer regelgeving rond Digitalisering
(Zoals: AI-Directive, NIS-1 NIS-2, Sectorale wet- en regelgeving, GDPR, ePrivacy, et cetera)

NOREA IT Auditverklaring

2.1) Principes IT auditverklaring

- Directie spreekt relevante **digitale bedrijfsdoelstellingen** uit
  - Denk aan een soort "**digitale omgevingsimpactassessment**" en **stakeholderanalyse**
  - Er is wel een **base line aan minimale topics** die in scope moeten zijn.

- Directie doet een **managementbewering** over de opvolging en realisatie van de **digitale bedrijfsdoelstellingen**

- De IT Auditor toetst de managementbewering
- en toetst of er **passende maatregelen** zijn getroffen, én of deze **doelstellingen bereikt zijn of kunnen worden**

NOREA IT Auditverklaring

2.2) Principes IT auditverklaring

➔ Parallelen zijn te trekken met sustainability reporting (Vergelijk framework van GRI, Global Reporting Initiative)

➔ IT Auditverklaring sluit aan op de IT auditwerkzaamheden ihkv de jaarrekeningcontrole

➔ IT Auditverklaring is geen vervanging van ISAE3402, SOC1,2,3. (third party assurance)

➔ IT Auditverklaring kan wel steunen op deze al verrichte auditwerkzaamheden

➔ Bestaande IT standaarden en normen worden zoveel als mogelijk hergebruikt

NOREA IT Auditverklaring

2.3) Principes IT auditverklaring / Topics minimaal in scope (voorlopig):

➢ (Cyber)security	IT omgeving, data, anticiperen op te verwachten ontwikkelingen, ketenanalyse
➢ IT Continuity	Eigen functioneren organisatie, en impact omgeving, ketenanalyse, licentiebeheer, contractmanagement
➢ Incident management	Verslag van incidenten, incident response en toekomst gerichte maatregelen
➢ Change	IT gerelateerde wijzigingen, innovatief vermogen, stappen in digtale transformatie aansluitend op bedrijfsdoelstellingen, realisatie van IT projecten
➢ Data governance & ethics	Data Governance, impact stakeholders, Omgang met AI/ML, ….
➢ Compliance & Eco -systeem	Voldoen aan wet- en regelgeving, maatschappelijk verantwoord ondernemen, (digitale footprint, privacybescherming, et cetera)

NOREA IT Auditverklaring

3.1) Vaktechnische onderwerpen en uitdagingen

- Uitspraak over verleden én uitspraak overtoekomst (behalen van doelstellingen)
- Hanteren van een groei- of volwassenheidsmodel in de tijd gezien
- Uitspraak met redelijke mate van zekerheid of beperkte mate van zekerheid
- Scope: hele organisatie of deel organisatie
- Te hanteren auditstandaard,
- Inhoud verslag en inhoud verklaring

NOREA IT Auditverklaring

3.2) Vaktechnische onderwerpen en uitdagingen

Gefaseerde benadering IT audit:

- Pre auditfase (doelstellingenfase, understanding the entity (Auditee & IT Auditor)
- Eerst nulmeting en verbeteringen signaleren (door IT Auditor)
- Verbeteringen doorvoeren (door Audittee)
- Audit uitvoeren leidend tot een uitgebreide IT management letter
- Audit uitvoeren leidend tot verklaring (eventueel met IT management letter)

NOREA IT Auditverklaring

4) Aanpak en Projectgroep

- Commissie beroepsreglementering NOREA
- Vertegenwoordigd zijn onder andere alle 6 de OOB kantoren (EY, PWC, KPMG, Deloitte, BDO, Mazars)
- Consultatieronde directoraten vaktechniek OOB kantoren
- Onderzoeksenquete is onderhanden: https://www.norea.nl/onderzoek-t.b.v.-'it-auditverklaring'-norea
- Overleg met: NBA, GRI (Global Reporting Initiative), toezichthouders, overheden, grote ondernemingen, beursfondsen, commissarissen.
- DOEL: Eerste verklaringen af te geven over 2022

Bedankt

Voor meer informatie kun je contact opnemen met:

mazars
Jan Matto
06 535 78 232
jan.matto@mazars.nl

14 september 2021

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS