NOREA-Plaza: aanvang 16.30 uur

Netwerk NOREA ZZP-leden medewerkers kleine IT-auditorganisaties

[20-5-2021]

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Agenda

- Opening en welkom door Winfried Nanninga, bestuurslid NOREA
- Audit of advies over Informatiebeveiliging en/of IT–beheersing, hoe/waar te beginnen? Door Peter Kornelisse (EY)
- Permanente Educatie, blik op toekomstige ontwikkelingen en ambities door Alex Klaassen, voorzitter Commissie Permanente Educatie
- Hoe kan ik me voorbereiden op kwaliteitsonderzoek en wat wordt onderzocht? Door Jaap Boukens, Voorzitter College Kwaliteitsonderzoek (CKO) NOREA
- Virtuele borrel: Round–Table en/of Break–Out sessies

Werkgroep Cybersecurity

ZZP-bijeenkomst NOREA 20 mei 2021

20 mei 2021

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA | Belang van cybersecurity

Van een organisatie mag worden verwacht dat zij cybersecurity heeft geregeld, op drie niveaus:

1. **Risicogebaseerde keuzen voor cybersecurity door een organisatie**
2. **Cybersecurity-weerbaarheid van een organisatie**
3. **Beveiliging van producten en diensten**

NOREA | Belang van cybersecurity

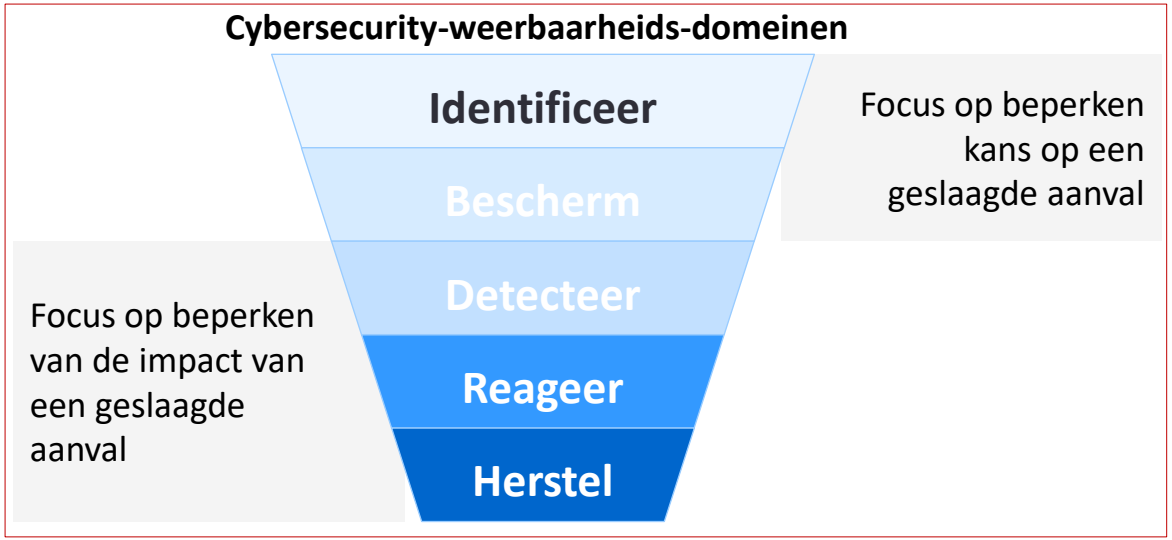
Van een organisatie mag worden verwacht dat zij cybersecurity heeft geregeld, op drie niveaus:

1. **Risicogebaseerde keuzen voor cybersecurity door een organisatie**
2. Cybersecurity-weerbaarheid van een organisatie
3. Beveiliging van producten en diensten

NOREA | Belang van cybersecurity

Van een organisatie mag worden verwacht dat zij cybersecurity heeft geregeld, op drie niveaus:

1. Risicogebaseerde keuzen voor cybersecurity door een organisatie
2. **Cybersecurity-weerbaarheid van een organisatie**
3. Beveiliging van producten en diensten

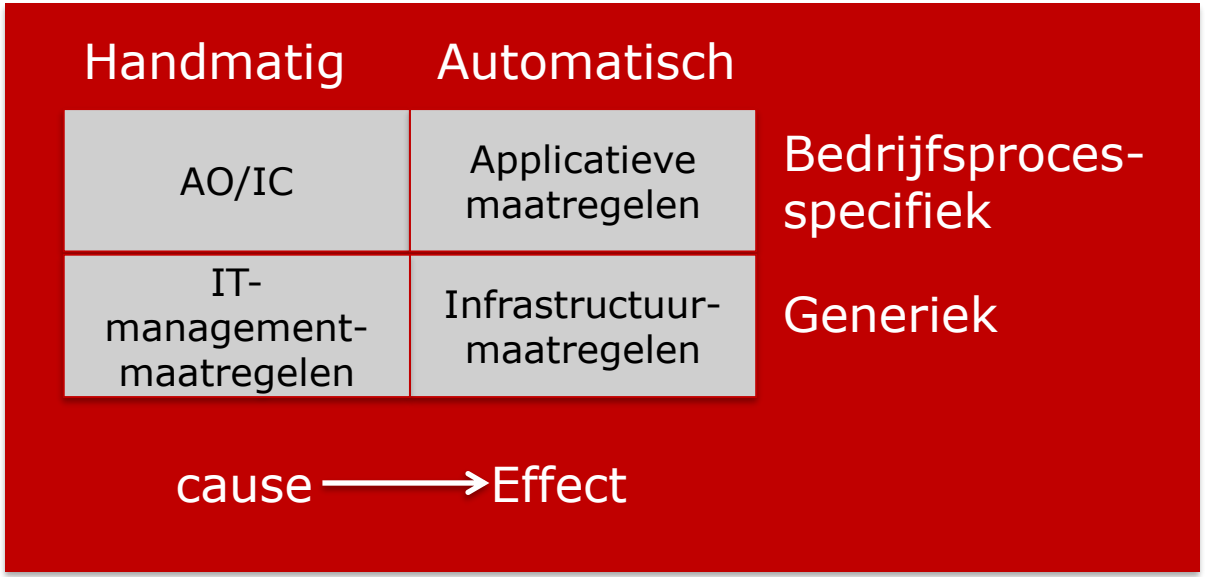


100 % beveiliging bestaan niet. Derhalve zal een organisatie voorbereid moeten zijn op een geslaagde aanval

NOREA | Belang van cybersecurity

Van een organisatie mag worden verwacht dat zij cybersecurity heeft geregeld, op drie niveaus:

1. Risicogebaseerde keuzen voor cybersecurity door een organisatie
2. Cybersecurity-weerbaarheid van een organisatie
3. **Beveiliging van producten en diensten**



NOREA | Belang van cybersecurity

Nederland is een voorloper met digitalisering. Hierbij is cyber-security van cruciaal belang, opdat digitalisering beheerst en veilig kan plaatsvinden.
Denk hierbij ook aan de toenemende keten-afhankelijkheid van organisaties en burgers, evenals het borgen van bescherming van persoonsgegevens. Goede cybersecurity is ook een enabler voor organisaties en haar producten en diensten.

De toenemende digitalisering resulteert in een toenemende gevoeligheid van organisaties voor:

- Vertrouwelijkheid, i.e. persoonsgegevens, intellectueel eigendom;
- Continuïteit, niet alleen van administratieve processen, maar ook productieprocessen, en digitale diensten aan klanten;
- Integriteit van gegevens, zoals die van financiële rapportages.

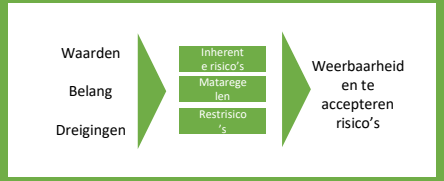
Dit vraagt ook in toenemende mate om zekerheid over de beveiliging van digitale oplossingen. IT-auditors kunnen deze zekerheid bieden.

Van een organisatie mag worden verwacht dat zij cybersecurity heeft geregeld, op drie niveaus:

1. Risicogebaseerde keuzen voor cybersecurity door een organisatie

Een organisatie wil haar doelstellingen bereiken. Tegelijkertijd wil zij haar risico's beheersen, waaronder die tegen cyber-gerelateerde dreigingen. Dit vraagt om continue risicogebaseerde verbeteringen. Van een organisatie wordt dan ook verwacht dat de leiding zich bewust is van, en kiest voor, een passende mate van cybersecurity.
Een passende mate van cybersecurity wordt bepaald door de gevoeligheid van een organisatie betreffende de te beschermen waarden, op basis van en de mogelijke impact van cyber-dreigingen en de kans dat deze dreigingen daadwerkelijk optreden, evenals haar risicobereidheid.
Hierbij is het tevens van belang bewust te zijn van relevante wet- en regelgeving, zoals die betreffende de bescherming van persoonsgegevens (Algemene Verordening Gegevensbescherming), en de Wet Beveiliging Netwerk- en Informatiesystemen voor digitale dienstverleners en essentiële diensten in diverse sectoren.

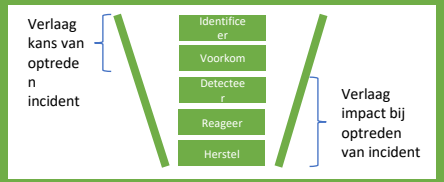
Voorbeelden zijn de cybersecurity risk assessment van NOREA en de audit op basis van de SOC (Service Organisation Controls) for Cybersecurity van ISACA.



2. Cybersecurity-weerbaarheid van een organisatie

Een organisatie beschermt zich, in een mate die past bij haar vastgestelde risicobereidheid, tegen cyber-dreigingen.
Wij beseffen echter dat 100% beveiliging niet bestaat. Van een organisatie mag dan ook redelijkerwijs worden verwacht dat niet alleen beveiligingsincidenten zo veel als mogelijk worden voorkomen, maar ook dat incidenten die toch plaatsvinden, snel worden gedetecteerd en adequaat worden opgevolgd.
Als onderdeel van cybersecurity-weerbaarheid is het voor een organisatie van belang te beseffen in welke organisatieketen(s) zij zich bevindt, en de afhankelijkheid daarvan regelmatig in kaart te brengen en te onderzoeken.

Voorbeelden betreffen audits tegen normen van de Baseline Informatiebeveiliging Overheid (BIO) voor de overheid, Informatiebeveiliging voor de zorg op basis van NEN7510, en het studierapport Algemene beheersing van IT-diensten van NOREA. Ook worden audits uitgevoerd om de volwassenheid van cybersecurity-weerbaarheid te meten.

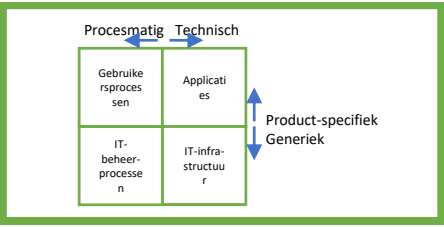


3. Beveiliging van producten en diensten

Met de toenemende digitalisering worden steeds meer diensten gebouwd, zowel op het Web als in Apps. Ook groeit naast IT (Informatie-Technologie) het gebruik van OT (Operationele Technologie) voor de aansturing van producten zoals elektrische auto's, sluizen en fabrieken.

Voor elk product en elke dienst is het veelal van belang een totaalbeeld van de beveiliging te hebben. Hiertoe dienen de relevante objecten waaruit het product of de dienst bestaat te zijn onderkend, en dienen hieraan ook de relevante eisen te worden gesteld. Dit betreft zowel procesmatige als technische aspecten, en product-specifieke en generieke aspecten.

Een voorbeeld van audits naar producten en diensten betreft de beoordeling van een website die gebruik maken van DigiD.



Ontwikkelingen en ambities C'cie Permanente Educatie

ZZP-bijeenkomst NOREA 20 mei 2021

[20 mei 2021]

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Agenda

- Strategie NOREA en Educatie
- Ambities Commissie – > portefeuilles & organisatie

Elementen uit de Strategie 2021 – 2025

Verstevigen kwaliteit van ons vak

De beginselen van een RE zijn deskundigheid, objectiviteit en onafhankelijkheid, waarbij kennis, opleiding en kwaliteit essentieel zijn. De door de RE geleverde dienst of product moet daarom altijd, bij 100% van de opdrachten, op het hoge niveau liggen.

Website als kennisplatform

- Toegankelijkheid website verbeteren voor derden
- Basisvindplaats van kennis voor leden
- Actualiseren/herijken content

Ontwikkelen en delen van kennis intensiveren

- Website als kennisplatform inrichten om ontwikkeling en deling van kennis tussen leden en andere professionals te stimuleren
- Bevorderen kennisdeling via o.a. webinars, trainingen, themabijeenkomsten

Intensiveren samenwerking met universiteiten

- Frequent in gesprek met de IT-audit opleidingen en andere universitaire opleidingen
- Afstudeeronderwerpen aandragen en afstudeerders kunnen zitting nemen in Taskforces

Opleiding en permanente educatie

- Frequent in gesprek en uitbreiden samenwerken met universiteiten met als doel vergroten bekendheid RE, kennisontwikkeling en relevantie voor maatschappij
- Periodiek actualiseren eindtermen
- Verplicht toetsen op specifieke onderwerpen (kennistoetsen en CKO-onderzoeken)

Elementen uit de Strategie 2021 – 2025

Verstevigen kwaliteit van ons vak

De beginselen van een RE zijn deskundigheid, objectiviteit en onafhankelijkheid, waarbij kennis, opleiding en kwaliteit essentieel zijn. De door de RE geleverde dienst of product moet daarom altijd, bij 100% van de opdrachten, op het hoge niveau liggen.

Website als kennisplatform

- Toegankelijkheid website verbeteren voor derden
- Basisvindplaats van kennis voor leden
- Actualiseren/herijken content

Ontwikkelen en delen van kennis intensiveren

- Website als kennisplatform inrichten om ontwikkeling en deling van kennis tussen leden en andere professionals te stimuleren
- Bevorderen kennisdeling via o.a. webinars, trainingen, themabijeenkomsten

Intensiveren samenwerking met universiteiten

- Frequent in gesprek met de IT-audit opleidingen en andere universitaire opleidingen
- Afstudeeronderwerpen aandragen en afstudeerders kunnen zitting nemen in Taskforces

Opleiding en permanente educatie

- Frequent in gesprek en uitbreiden samenwerken met universiteiten met als doel vergroten bekendheid RE, kennisontwikkeling en relevantie voor maatschappij
- Periodiek actualiseren eindtermen
- Verplicht toetsen op specifieke onderwerpen (kennistoetsen en CKO-onderzoeken)

Educatie heeft een nadrukkelijk (meer) strategische lading gekregen

Ambities en Organisatie

- Strategie is vertaald naar ‘portefeuilles’.
- Portefeuilles zijn ‘toebedeeld’ aan de leden van de c’cie.
- Elke ‘portefeuille–houder’ heeft een activiteitenplanning gemaakt en een tijdslijn.
- Elke maand een ‘plenaire bijeenkomst’ om voortgang en inhoud met elkaar te delen.
- Portefeuilles zijn:
  - PE–Model; een zo goed mogelijk model voor de toekomst.
  - Verplichte toetsen; Wie doet hierin wat en wat gaan we hoe aanbieden.
  - Website als kennisplatform; sterkere faciliterende rol NOREA.
  - Samenwerking met Universiteiten; Binding en samenwerking niet alleen tbv kennis, ook..
  - Webinars & Themabijeenkomsten; Meer digitaal!
  - Communicatie naar leden; Inbedding van communicatie over bovenstaande naar leden.

Bedankt

Voor meer informatie kun je contact opnemen met:

[Alexander Klaassen]
[0615946142]
[alex.klaassen@newdayriskservices.nl]

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Hoe kan ik me voorbereiden op kwaliteitsonderzoek en wat wordt onderzocht?

Jaap Boukens
Voorzitter College Kwaliteitsonderzoek (CKO) NOREA

Norea Reglement Kwaliteitsbeheersing

Art 5. Vereisten:

De IT-auditorganisatie dient een zodanig systeem van kwaliteitsbeheersing op te zetten dat een redelijke mate van zekerheid wordt geboden, dat de organisatie en haar personeel voldoen aan de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen en dat de door de organisatie of haar voor opdrachten verantwoordelijke professional afgegeven rapporten onder de gegeven omstandigheden voldoen aan de reglementen, richtlijnen en handreikingen die door NOREA zijn uitgevaardigd.

Art 6. Het kwaliteitsbeheersingssysteem van de IT–auditorganisatie dient gedragslijnen en procedures te bevatten gericht op de volgende aspecten:

a. Verantwoordelijkheid van de leiding voor kwaliteit binnen de auditorganisatie.

b. Ethische normen.

c. Aanvaarden en voortzetten van de relatie met opdrachtgevers en van specifieke opdrachten.

d. Personeelsbeleid.

e. Uitvoering van de opdrachten.

f. Het monitoren.

Hoe kan ik me voorbereiden op het kwaliteitsonderzoek?

Kennisnemen van Handreikingen, Richtlijnen en Studies op de website van Norea

Richtlijn:	Door Norea uitgevaardigde regels over de toepassing van fundamentele beginselen voor de beroepsuitoefening met een dwingend karakter.
Handreiking:	Door Norea uitgevaardigde richtinggevende beschrijvingen van methoden, technieken of normen waarvan de afwijking moet worden gemotiveerd en gedocumenteerd
Studie:	De uitingen van Norea over vaktechnische onderwerpen, niet zijnde richtlijnen of handreikingen

Hoe kan ik me voorbereiden op het kwaliteitsonderzoek?

Kennisnemen en uitwerken/invullen van:

NOREA model handboek Kwaliteitsbeheersing

Download van www.norea.nl: 2020 Model Handboek kwaliteitsbeheersing KITA's vs 2.0.docx

Hoe kan ik me voorbereiden op het kwaliteitsonderzoek?

NOREA model handboek Kwaliteitsbeheersing bevat o.a.:

7.1	Klantacceptatie
7.2	Opdrachtaanvaarding en –bevestiging
7.3	Uitvoering van de opdracht
7.4	Kwaliteitsbewaking uitvoering
7.5	Opdrachtgerichte kwaliteitsbeoordeling
7.6	Dossiervorming en documentatie
7.7	Rapportage en (verplichte formulering inzake) oordelen
7.8	Monitoren en verbeteren kwaliteitsbeheersingssysteem

Hoe kan ik me voorbereiden op het kwaliteitsonderzoek?

Handreiking Opdrachtgerichte Kwaliteitsbeoordeling (OKB)

Criterium RKBN	De aard van de opdracht, alsmede de mate waarin het openbaar belang daarbij betrokken is	Het signaleren van ongebruikelijke omstandigheden of risico's ten aanzien van een opdracht of groep opdrachten	De omstandigheid dat wet- of regelgeving een opdrachtgerichte kwaliteitsbeoordeling voorschrijft.
Voorbeelden	Assurance-opdrachten	Opdrachten met een fee groter dan xxx	Er is thans geen specifieke wet- en regelgeving die een opdrachtgerichte kwaliteitsbeoordeling voorschrijft.
	Rapporten voor brede verspreidingskring	Opdrachten waarbij een externe deskundige wordt ingeschakeld	
	Opdrachten voor beursgenoteerde ondernemingen	Opdrachten buiten de landsgrenzen	
	Opdrachten voor financiële instellingen		

Wat wordt onderzocht?

Onder andere:

1. Het self–assessment
2. Het handboek kwaliteitsbeheersing
3. Enkele opdrachten om vast te stellen dat aan de kwaliteitseisen wordt voldaan.

Twee soorten negatieve bevindingen:

1. Aanbeveling
2. Aanwijzing

Aanwijzingen leiden tot een negatief oordeel over het kwaliteitssysteem.

Gecontroleerde moet verbetermaatregelen voorstellen en aantonen dat deze zijn geïmplementeerd. Daarna volgt een heronderzoek.

Bedankt

Voor meer informatie kun je contact opnemen met:

[NOREA]
[020–3010380]
[norea@norea.nl]

[datum]

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS