NOREA
Inherent Risk en Cyber Security Assessment
versie 2.2 !

Webinar Kennisgroep Cybersecurity
17 september 2020

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Introductie

- Cybersecurity Assessment en Inherente Cyberrisico Analyse 2.1 in oktober 2019 gepubliceerd. Daarvan komt deze maand een update beschikbaar (versie 2.2) met een gecombineerde/integrale spreadsheet op basis van nieuwe/actuele standaarden en referenties (o.a. DNB *Good Practice*).

- Geschikt als basis voor managementrapportages en assessment-/auditactiviteiten en of communicatie over cyberrisico's met CISO's, Stakeholders etc.

- Link met Partnering Trust /Online Trust Coalitie, Business partners en value chain
  - Elkaar zekerheid geven over …info --- of inzicht geven in onderlinge risico's
  - Eerst zelf doen, dan delen

Introductie

- **Peter Kornelisse RE CISA CIPP/e**
  - Associate Partner bij EY | Technology Risk
  - Hoofddocent Auditing Cybersecurity bij TIAS
  - Lid NOREA kennisgroep Cyber Security
- **Marcel Woltjes RE CISA**
  - CISO bij Ministerie van OCW
  - Lid NOREA kennisgroep Cyber Security

- **NOREA**
- Kennisgroep Cybersecurity
- - Opgericht in 2010
- - 13 NOREA-leden
- - Doelen
  - - Verhogen awareness IT-auditors & opdrachtgevers
  - - Ondersteunen IT-auditor bij cybersecurity gerelateerde vragen

Begrijpen en sturen van cybersecurity-risico’s

Meerdere stakeholders hebben een rol bij het beheersen van cybersecurity-risico’s. Elk van deze stakeholders kan ook gebruik maken van de Inherent Risk en Cyber Security Assessment.

Stakeholders

IT-auditor

Security officer

Management

Risico-domeinen

Continuïteit

Enabler

Integriteit

Fraude

Privacy

Managementrapportage Cybersecurity

vs wachten op een cybersecurity-incident

1. Restrisico's voor de bedrijfsvoering op basis van bekende risico's
2. Ontwikkelende cybersecurity-dreigingslandschap
3. Compliance met cyber controls (interne en externe eisen)
4. Vooornaamste cybersecurity-incidenten
5. Voortgang van geplande cybersecurity-verbeteringen

Agenda

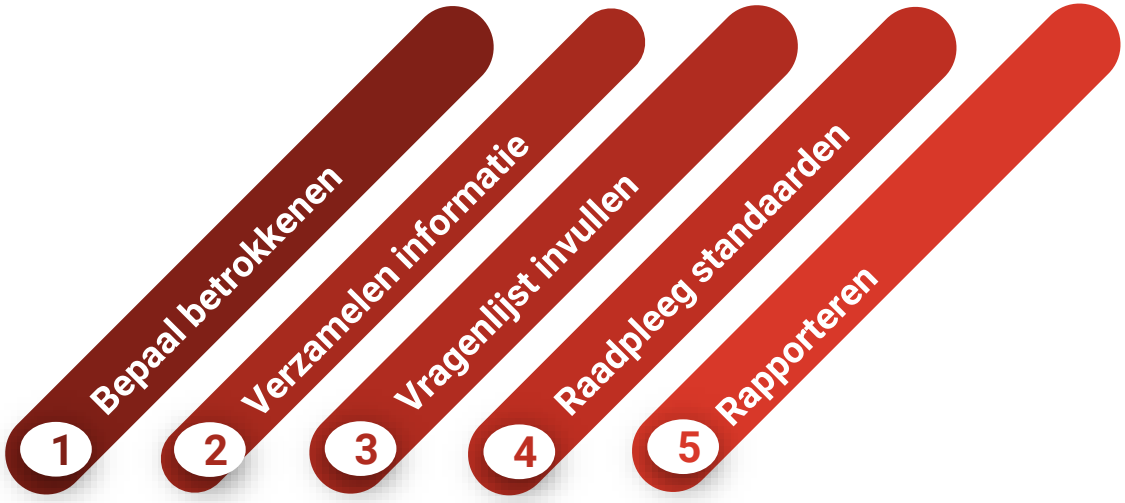
Inherent Cyber Risk en Cyber Security Assessment

- Wat kan ik er mee ?
- Wat is het en hoe werkt het ?

Inherent Risk en Cyber Security Assessment

Wat kan ik er mee

- Inzicht in cyberrisico's van organisatie
- Creëren van bewustwording
- Praktische stappen



Cyber Security Assessment

Wat is het en hoe werkt het ?

Inherent Cyber Risico

ICR CSA Acties

Belang beheersing

- Bepaling inherent cyberrisico (ICR)
  - Situatie zonder beheersmaatregelen
  - Eenvoudig toe te passen
  - Uitkomst cyber risicoprofiel: Hoog / Medium / Laag
  - Indicatie voor prioritering maatregelen

- *Koppeling met NBA LIO, Cyber Health check, NIST, Cobit*
- *Gebaseerd op model FFIEC (Toezichthouder US)*

Inherent Cyber Risico

Belang beheersing

ICR → CSA → Acties

- 24 vragen, verdeeld over categorieën
  - **Vitaal**
  - **Organisatiekarakteristieken**
  - **Technologie & derde partijen**
  - **Online aangeboden producten en diensten**
  - **Externe cyberdreigingen**

Inherent Cyber Risico

ICR CSA Acties

Belang beheersing

- Per vraag een score: hoog, midden of laag risico
- Voorbeeld:

	Vraag:	Risico-inschatting:			Uw inschatting: 1 (Hoog), 2 (Midden) of 3 (Laag)
		1 = Hoog	2 = Midden	3 = Laag	
rde	Hebben derde partijen toegang tot de interne systemen van uw organisatie?	1 of meer derde partijen met toegang tot interne systemen	NVT	Geen derde partijen, individuen met toegang tot interne systemen	1

Inherent Cyber Risico

Belang beheersing

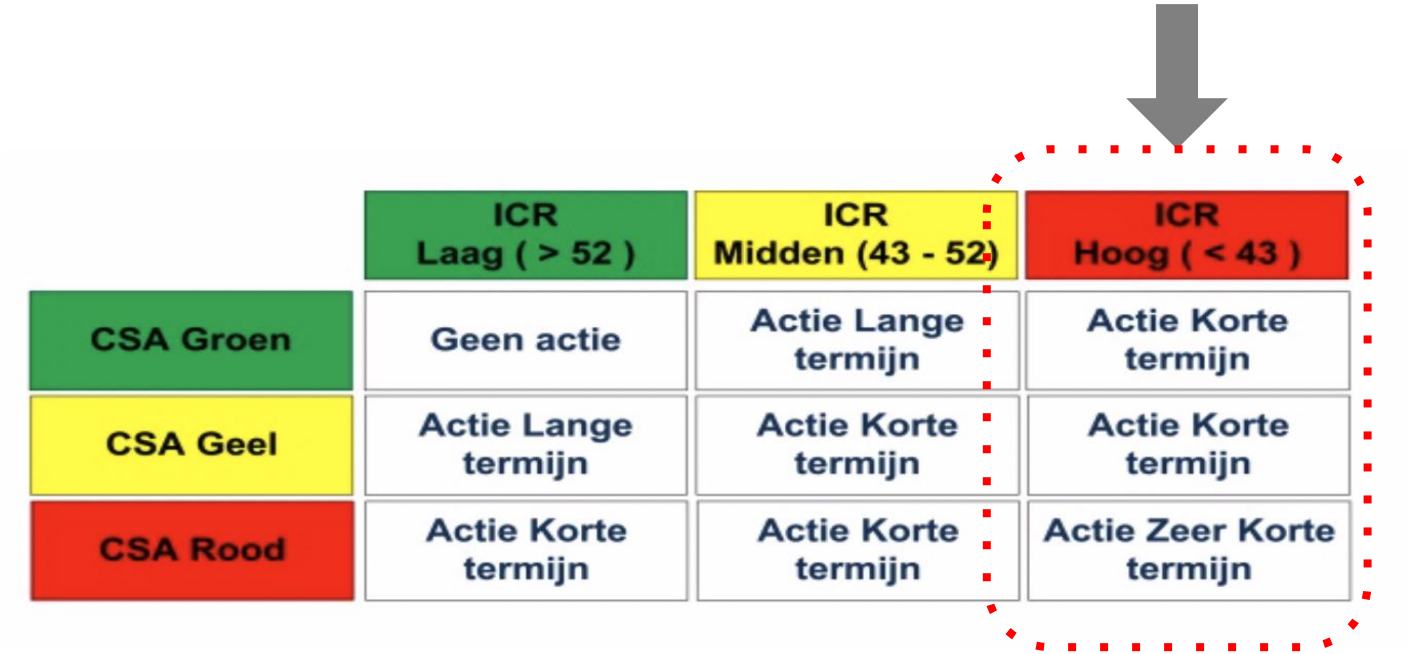
ICR → CSA → Acties

- Na invullen ICR volgt een samenvattende score: Hoog, Medium of Laag
- Helpt met prioriteren benodigde beheersmaatregelen binnen de CSA

Inherent Cyber Risico

Tussenresultaat belang beheersing

ICR → CSA → Acties



	ICR Laag (> 52)	ICR Midden (43 - 52)	ICR Hoog (< 43)
CSA Groen	Geen actie	Actie Lange termijn	Actie Korte termijn
CSA Geel	Actie Lange termijn	Actie Korte termijn	Actie Korte termijn
CSA Rood	Actie Korte termijn	Actie Korte termijn	Actie Zeer Korte termijn

Cyber Security Assessment
Invullen vragenlijst

ICR CSA Acties

- Aandachtsgebieden

  - Organisatie & governance
  - Gedrag & cultuur
  - Wet- & regelgeving
  - Waardeketen
  - Inzicht in technologie landschap
  - Detectie
  - Reactie

Cyber Security Assessment
Invullen vragenlijst

ICR CSA Acties

Reactie			Selecteer score (Ja of Nee)
1	Kan de organisatie snel acteren richting de diverse stakeholders in geval van een cyberdreiging?		Nee
2	Is een specifiek proces ingericht voor de afhandeling van cybersecurity incidenten?		Nee
3	Is een CSIRT of vergelijkbaar orgaan ingericht en aangesloten op de reguliere crisisorganisatie?		Ja
4	Maakt de organisatie voor de afhandeling van incidenten onderscheid o.b.v. bijvoorbeeld impact van een incident?		Nee
5	Vinden periodiek trainingen / testen plaats om cyberincidenten effectief af te handelen?		Ja
6	Zijn leveranciers en afnemers onderdeel van het responseproces en zijn zij daarvan op de hoogte?		Ja
7	Zijn leveranciers en afnemers betrokken bij de trainingen / testen voor cyberincidenten?		Nee
		Totaal score	4

Cyber Security Assessment
Invullen CSA - deelscore

ICR → CSA → Acties

Reactie		Selecteer score (Ja of Nee)
1	Kan de organisatie snel acteren richting de diverse stakeholders in geval van een cyberdreiging?	Nee
2	Is een specifiek proces ingericht voor de afhandeling van cybersecurity incidenten?	Nee
3	Is een CSIRT of vergelijkbaar orgaan ingericht en aangesloten op de reguliere crisisorganisatie?	Ja
4	Maakt de organisatie voor de afhandeling van incidenten onderscheid o.b.v. bijvoorbeeld impact van een incident?	Ja
5	Vinden periodiek trainingen / testen plaats om cyberincidenten effectief af te handelen?	Nee
6	Zijn leveranciers en afnemers onderdeel van het responseproces en zijn zij daarvan op de hoogte?	Nee
7	Zijn leveranciers en afnemers betrokken bij de trainingen / testen voor cyberincidenten?	Nee
	Totaal score	3

7	Reactie	3	U lijkt uw risico's t.a.v. reactie niet te kennen en te beheersen. De normen van ISF – SoGP, ISF – CRF, ISACA Cybercrime Audit/ Assurance Program en NIST bieden hier handvatten voor.
	Overall cyber risico score (1 – 10)	6	

Cyber Security Assessment
Score totaalscore CSA

ICR CSA Acties

	Categorie:	Score:	Waardevolle standaarden:
1	Organisatie & Governance	4	U lijkt uw risico's t.a.v. governance en organisatie niet te kennen en te beheersen. De normen van ISF – CRF, ISACA Cybercrime Audit/ Assurance Program, PAS 555 en NIST bieden hier handvatten voor.
2	Gedrag & Cultuur	8	U lijkt zicht te hebben op uw gedrag en cultuur risico's en de beheersing daarvan.
3	Waardeketen (stakeholders) versus risico's	8	U lijkt zicht te hebben op uw waardeketen en stakeholders risico's en de beheersing daarvan.
4	Inzicht in technologielandschap	6	U lijkt uw risico's t.a.v. technologielandschap niet volledig te kennen en te beheersen. De normen van ISF – SoGP, SANS – CSCfECD, ISACA Cybercrime Audit/ Assurance Program, NIST en ISO/IEC 27032 bieden hier handvatten voor.
5	Wet- en regelgeving	8	U lijkt zicht te hebben op uw wet- en regelgeving risico's en de beheersing daarvan.
6	Detectie	5	U lijkt uw risico's t.a.v. detectie niet volledig te kennen en te beheersen. De normen van ISF – SoGP, ISF – CRF, SANS – CSCfECD, ISACA Cybercrime Audit/ Assurance Program, NIST en ISO/IEC 27032 bieden hier handvatten voor.
7	Reactie	3	U lijkt uw risico's t.a.v. reactie niet te kennen en te beheersen. De normen van ISF – SoGP, ISF – CRF, ISACA Cybercrime Audit/ Assurance Program en NIST bieden hier handvatten voor.
	Overall cyber risico score (1 – 10)	6	

Acties

Uitbrengen rapportage

	Categorie:	Score:	Waardevolle standaarden:
1	Organisatie & Governance	4	U lijkt uw risico's t.a.v. governance en organisatie niet te kennen en te beheersen. De normen van ISF – CRF, ISACA Cybercrime Audit/ Assurance Program, PAS 555 en NIST bieden hier handvatten voor.
2	Gedrag & Cultuur	8	U lijkt zicht te hebben op uw gedrag en cultuur risico's en de beheersing daarvan.
3	Waardeketen (stakeholders) versus risico's	8	U lijkt zicht te hebben op uw waardeketen en stakeholders risico's en de beheersing daarvan.

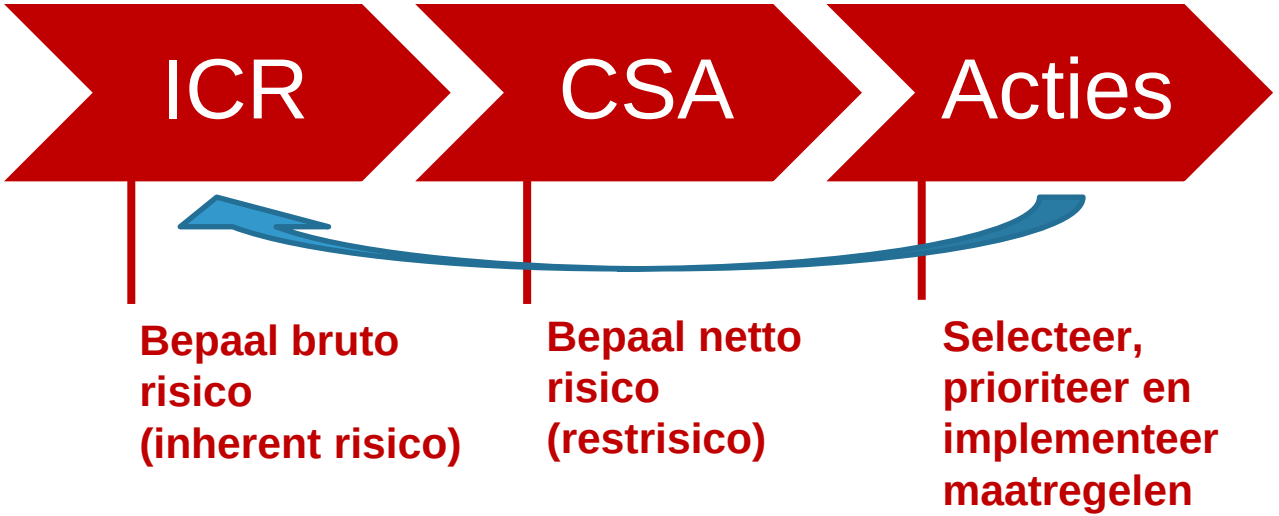
Acties

Raadplegen relevante standaarden

Basisselectie vanuit CSA 1.0 aangevuld, met o.a. DNB Good Practice, 58 controls

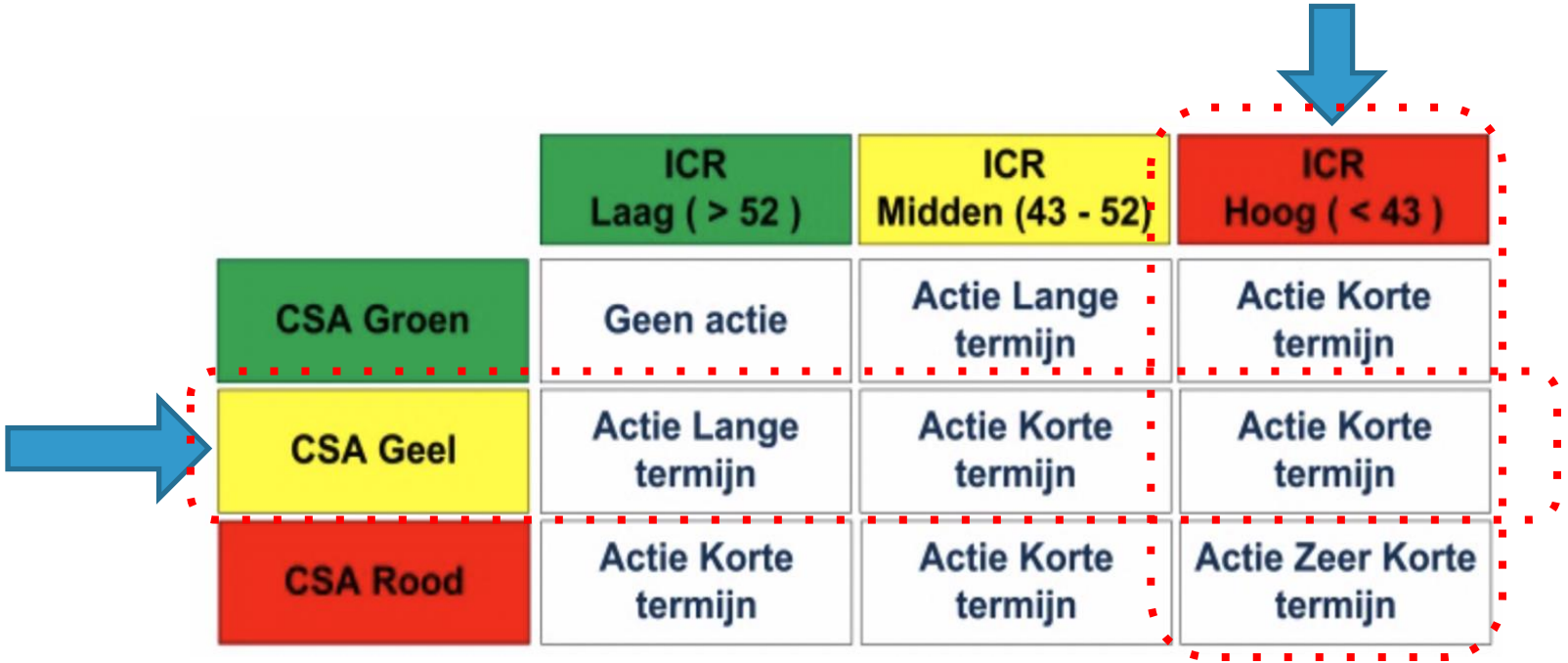
Organisatie	Standaard
Information Security Forum (ISF)	Standard of Good Practice (SoGP)
SANS Institute	Critical Controls for Effective Cyber Defense (CCfECD)
Information Systems Audit and Control Association (ISACA)	Cybercrime Audit / Assurance Program
British Standards Institute (BSI)	PAS555, Cyber Security Risk, Governance and Management
National Institute of Standards and Technology (NIST)	Cyber Security Framework
International Standards Organisation (ISO)	ISO 27032 Guidelines for Cyber Security

`Cyber security assessment 2.0



Acties

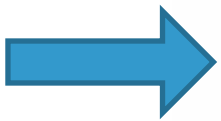
Combineren ICR en CSA



	ICR Laag (> 52)	ICR Midden (43 - 52)	ICR Hoog (< 43)
CSA Groen	Geen actie	Actie Lange termijn	Actie Korte termijn
CSA Geel	Actie Lange termijn	Actie Korte termijn	Actie Korte termijn
CSA Rood	Actie Korte termijn	Actie Korte termijn	Actie Zeer Korte termijn

Acties
` *Prioriteitstelling*

Definitie acties:



Geen actie: Voer na een jaar opnieuw een ICR en CSA uit.
Actie Lange termijn: Stel belangrijke verbeteringen vast, implementeer deze binnen 1 jaar. Voer na een jaar opnieuw een ICR en CSA uit.
Actie Korte termijn: Start een project om belangrijke verbeterpunten te implementeren binnen 6 maanden. Voer na 6 maanden opnieuw een ICR en CSA uit.
Actie Zeer Korte termijn: Start een project en/of programma om belangrijke verbeteringen te implementeren en bewaak de voortgang.

Acties

Selecteer en implementeer maatregelen

Links en verwijzingen

Links:	Standaarden:
http://www.nist.gov/cyberframework/	NIST – Cybersecurity Framework, Version 1.0, Framework for Improving Critical Infrastructure Cybersecurity
http://www.sans.org/critical-security-controls/	SANS Top 20
http://www.iso.org/iso/catalogue_detail?csnumber=44375	BS ISO27032:2012 Information technology – Security techniques – Guidelines for cybersecurity,
http://www.itgovernance.co.uk/shop/p-1356-pas-555-2013-cyber-security-risk-governance-and-management.aspx	BSI PAS555 2013 Cyber Security Risk Governance and Management Specification
https://www.isaca.org/bookstore/Pages/Product-Detail.aspx?Product_code=96WCSP	ISACA – Cyber security policy framework

Prikkelende vragen

- Hoe vaak heb je afstemming tussen security en business
  - Week – maand – kwartaal – jaar

- Welke metingen zelf of ontvang je voor rapporteren
  - Beveiligingsbewustzijn
  - Toegangsbeheer
  - Technologie

- Heb je de afgelopen 6 maanden een oefening crisisbeheersing cybersecurity gehouden?
  - Ja | nee

- Wanneer krijg jij een ‘Maastricht’je
  - Maand | Kwartaal | Jaar | 2 jaar

Samenvattend

- Tooling voor uitgebreide risicoanalyse proces Cybersecurity
- Communicatietool voor bespreken met directie en het verhogen awareness
- Eenvoudig uitbreidbaar (specifiek te maken)
- Goede aansluiting met NBA LIO, ISO27000, NIST CSF, DNB IB/Cyber, …

Toekomst

- Actualiseren onderliggende normenkaders
- Uitbreiden vragenlijsten
  - ICR
  - CSA

Meer informatie

norea@norea.nl
www.norea.nl/handreikingen/

drs. ir. M.P.P. (Marcel) Baveco RE CISA CISSP
drs. R.R. (Rob) Bouman RE RA
drs. D.P. (Dennis) van Heijst RE
ing. J.G.M. (Johan) Hofhuis RI EMITA RE
dr. ing. J.H.M. (Jürgen) van Grinsven RE
ir. J.W. (Jan) de Heer RE
ing. R.H.J. Kok RE CISSP
ir. P (Peter) Kornelisse RE CISA CIPP/e
ing. M. (Mark) van der Krift RE
M.J.B. (Marcel) van Leeuwen RE
C.A. (Amer) Ramkoeber MSc EMITA RE
mr. W. B. (Wouter Bas) van der Vegt RE
ing. M.S. (Marcel) Woltjes RE
ing. J. (Jean) Zweers RE CISA CISSP

© NOREA

Relatie met andere standaarden

Cybersecurity health check

- Vragenlijst gebaseerd op fasering in NIST
- Gericht op MKB
- Gaat over beheersing
- Gebruik ICR helpt om meer health check specifieker te maken

NBA LIO

- NBA-LIO linkt door ISO27000, DNB 2017, ….
- Beide modellen kunnen gebruikt worden als instrument voor self-assessment
- NBA-LIO model vanuit diverse controle-doelstellingen relevant voor cyber security