ISACA Risk Event
NIS 2 Workshop

Gemma Jansen, 6 november 2024

Ronde 1 - Kennis:
NIS 2 Highlights; wat is de essentie en wat is de relatie met informatiebeveiliging

Break (10 min)

Ronde 2 - Kunde:
Voorbereiding voor de echte start met een assessment en een oefening

Ceo heeft eigen aansprakelijkheid cybersecurity niet op het netvlies

- Te veel bedrijven blijven tekortschieten als het gaat om de veiligheid van hun IT-systemen.
- De eisen op het gebied van cybersecurity worden daarom door Brussel fors aangescherpt.
- Bedrijfsbestuurders zijn zich te weinig bewust van hun eigen aansprakelijkheid op dit vlak.

Sandra Olsthoorn en Ardi Vleugels
Amsterdam

Bestuurders van bedrijven zijn zich onvoldoende bewust van de risico's die zij volgend jaar lopen. Europese regels die dan ingaan, maken hen expliciet verantwoordelijk voor het cyberbeleid van hun onderneming. Ze kunnen persoonlijk aansprakelijk worden gesteld als ze deze taak niet goed vervullen en kunnen in het uiterste geval zelfs tijdelijk uit hun functie worden gezet.

Daarvoor waarschuwt de Cyber Security Raad (CSR), die de overheid adviseert over digitale veiligheid. Tot nu toe lieten bestuurders cyberbeleid vaak over aan IT-afdelingen en was hun rol beperkt tot het goedkeuren van het gevraagde budget. In de nieuwe Europese regels, die voor veel bedrijven gaan gelden en die op dit moment naar Nederlandse wetgeving worden vertaald, moeten ze meer doen.

De CSR ziet dat veel bedrijven dit niet doorhebben. Zo moeten bestuurders maatregelen tegen cyberrisico's goedkeuren en toezien op uitvoering. Ook moeten ze meehelpen om de cybersecurity bij directe toeleveranciers te waarborgen.

Advocaat en hoogleraar Lokke Moerel, lid van de raad, noemt de regels revolutionair omdat bestuurders zo nadrukkelijk worden aangesproken op hun verantwoordelijkheden. 'Als je die negeert, zal sneller sprake zijn van een ernstig persoonlijk verwijt, waardoor persoonlijke aansprakelijkheid van bestuurders op de loer ligt. Dit strekt zich zelfs uit tot de commissarissen.'

In eerste instantie krijgt een nalatig bedrijf waarschuwingen en boetes, tot 2% van de jaaromzet. Als daarna voldoende verbetering uitblijft, kan een bestuurder persoonlijk gevolgen ondervinden. 'Die moet dus snel zijn kennis oppoetsen en controleren hoe het bedrijf er voorstaat', zegt Moerel.

Nu bedrijven digitaal sterk verbonden zijn, kan een zwakke achterdeur bij een kleine leverancier voor de hele keten gevolgen hebben. De nieuwe regels dwingen grote bedrijven daarom meer verantwoordelijkheid te nemen voor hun toeleveranciers. Ze moeten hen helpen, bijvoorbeeld door hun kennis te delen.

Wat betreft cyberveilig werken blijven juist kleinere bedrijven achter, zegt CSR-lid Claudia de Andrade, bij Havenbedrijf Rotterdam verantwoordelijk voor de IT. 'Naar schatting 60% van de grotere en 30% van de kleinere bedrijven is zich bewust van cyberrisico's.' Uit een uitvraag van cybersecuritybedrijf Cisco bleek vorige week dat maar 3% van alle bedrijven klaar is voor actuele cyberdreigingen.

'Wetgevers hebben gedacht: nou dan maken we van cybersecurity wel chefsache'

In Nederland gaan de regels per 2025 in, maar de inhoud is al grotendeels bekend en zal niet meer veranderen, denkt de raad. 'Om de invoeringsdatum te halen moet je nu beginnen', zegt Hester Somsen, directeur cybersecurity en statelijke dreigingen bij de NCTV. 'Regel je opleidingen, ga aan de slag met een risicoanalyse. Doe je dat niet, dan ben je kwetsbaar voor cyberaanvallen en uiteindelijk nalatig.'

Een deel van de regels, zoals een meldplicht bij cyberincidenten, geldt nu al voor zo'n duizend essentiële bedrijven, zoals in de telecom. Met de nieuwe wet zullen zo'n 10.000 bedrijven ermee te maken krijgen.

Moerel: 'Ook sectoren zoals de voedselproductie gaan straks voor het eerst onder een toezichthouder vallen voor hun cyberbeleid.' Dat besef is er niet bij iedereen: regelmatig ziet zij bedrijven die schrikken omdat ze nu pas ontdekken dat ook zij onder de regels gaan vallen. Met onlinetests kunnen bedrijven nagaan wat ze moeten doen.

Overheid en experts roepen al jaren op de bewaking tegen cyberaanvallen te verstevigen, maar veel bedrijven nemen een laconieke houding aan. Dat bestuurders nu expliciet verantwoordelijk worden, is een zwaar middel, maar daarom logisch, vindt Moerel. 'Wetgevers hebben gedacht: nou dan maken we het chefsache.'

De strenge regels komen er niet voor niets: de risico's van cyberincidenten waren nooit eerder zo groot, stelt de CSR. Ransomware kan de bedrijfsvoering stilleggen en door spanningen in de wereld loopt de digitale dreiging fors op. Het aantal aanvallen neemt toe, mede door kunstmatige intelligentie. Moerel: 'Cyberincidenten staan in de top drie van grootste bedrijfsrisico's.'

Somsen wijst erop dat een cyberaanval op een bedrijf ook maatschappijontwrichtend kan zijn. 'Nederland heeft dat op die schaal nog niet gezien. Maar wij achten dat risico hier meer dan reëel.' Moerel: 'Zoals we er nu voorstaan, zijn we daar qua cyberweerbaarheid niet klaar voor.'

Relevante Europese wetgeving

Prevent

- **NIS 2** - Network and Information Security
- **DORA** – Digital Operational Resilience Act
- **Cybersecurity Act** - cybersecurity certification of ICT products, services and processes

- ***Cyber Resilience Act*** *– Product Security*
- ***Cyber Solidarity Act*** *- Cyber Emergency Mechanism & Cybersecurity Incident Review Mechanism*

Detect

- ***Cyber Solidarity Act*** *- European Cybersecurity Shield made up of Security Operation Centers – SOCs*

Respond

- ***Cyber Solidarity Act*** *- Cyber Emergency Mechanisms*

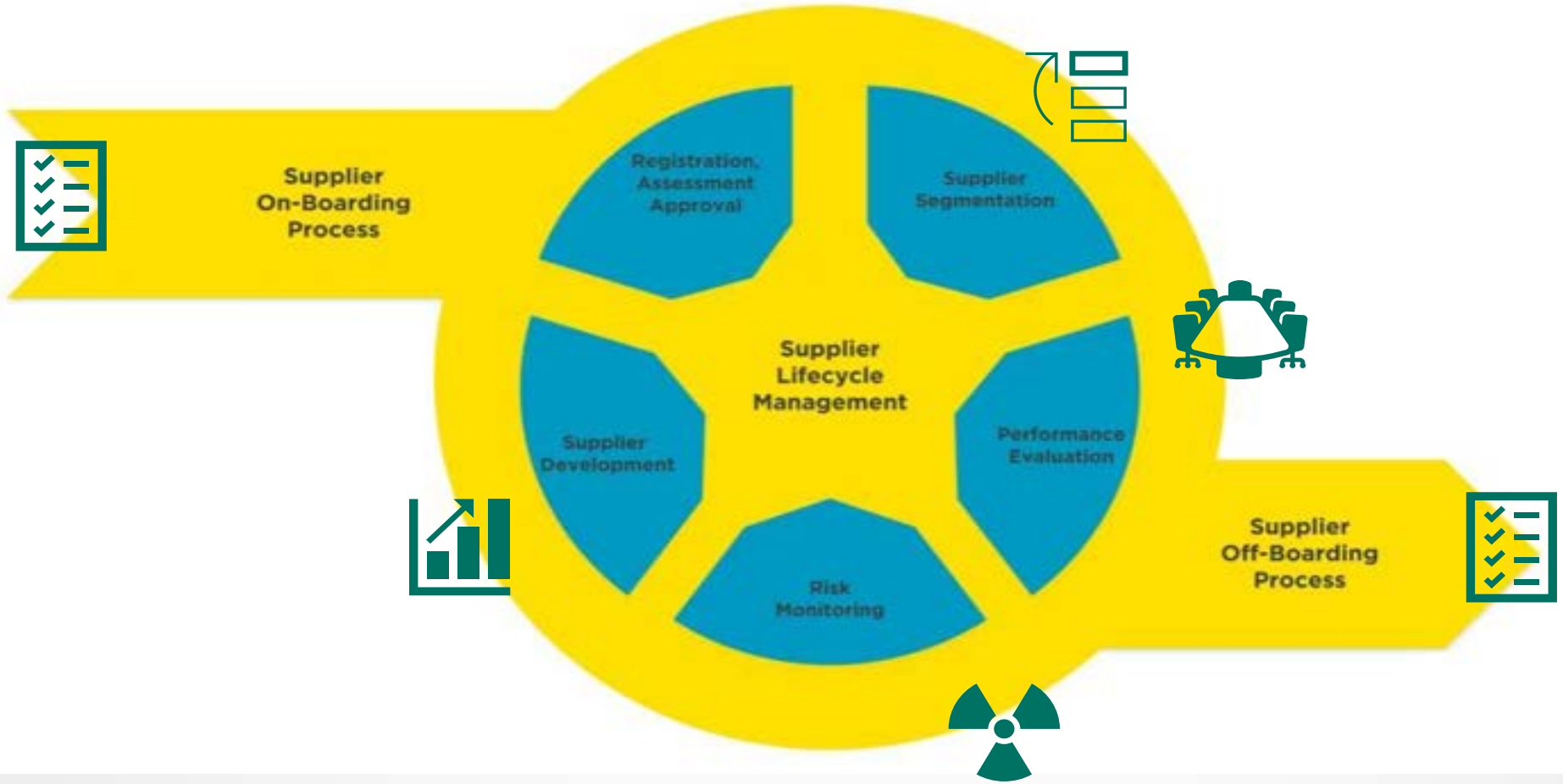
- Cyber Crisis Management
  - EU CyCLOne
  - CSIRT Network (NIS 2)

De NIS2 is vastgesteld door de Europese Unie en bedoeld om de cyberbeveiliging **en** de weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren.

! *De focus ligt daarbij niet alleen op de eigen organisatie, maar hoe incidenten de samenleving en het functioneren van andere bedrijven/organisaties kunnen schaden of belemmeren.*

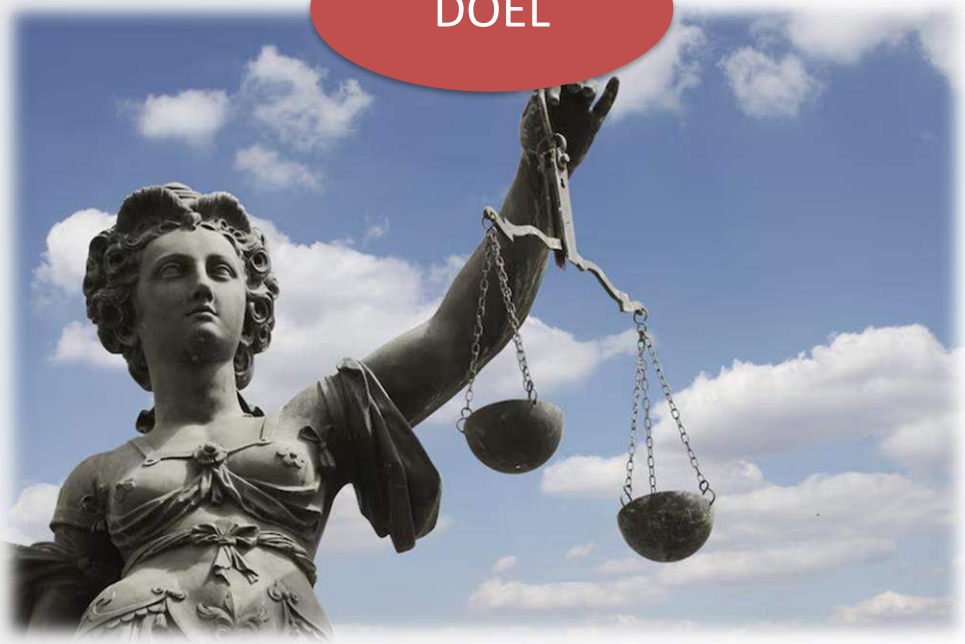
Scope: Kwantitatief

Scopeuitbreiding t.o.v. NIS 1: Kwalitatief



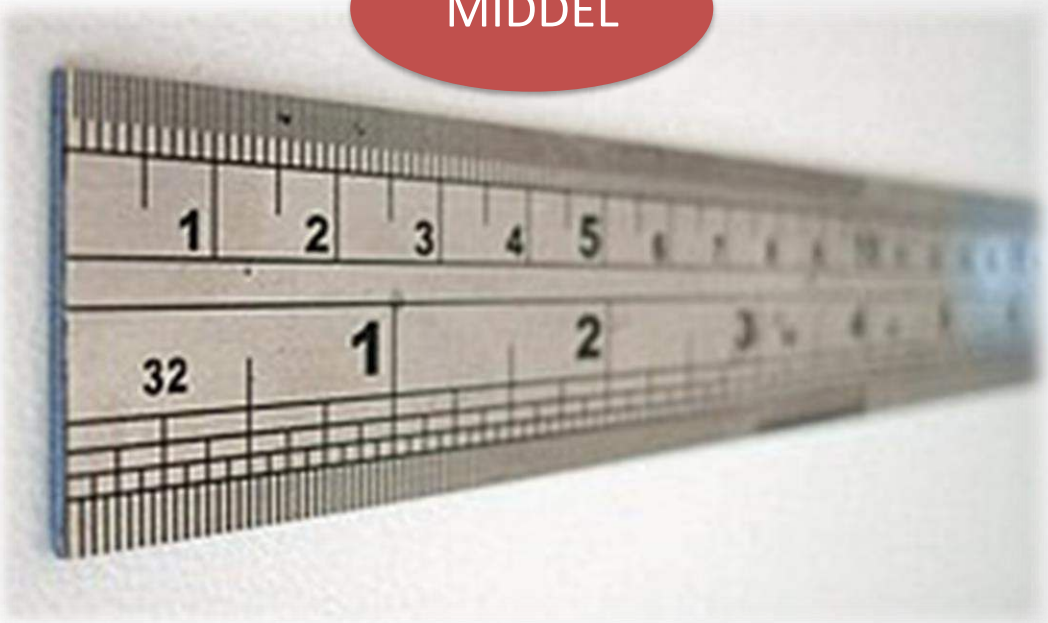
Verhouding: NIS 2 tot Cyberbeveiligingswet & ISO27001

DOEL



EU "first" & Member State "second"

MIDDEL



"ISO27001 promotes a holistic approach to information security"

Cyber & Niet-Cyber = ALL HAZARDS

NIS 2 DIRECTIVE

Overweging 30:

"identificatie van kritieke entiteiten, risico's, cyberdreigingen, en incidenten en niet-cyberrisico's, -dreigingen en –incidenten"

Turbulente tijden, onvoorziene effecten

Digitale risico's zijn dynamisch en worden beïnvloed door vele factoren die ook niet-digitaal kunnen zijn. <…> Om digitale risico's het hoofd te kunnen bieden, is het van belang een brede manier van risicobeheersing aan te nemen.

A. Essentiële bedrijven

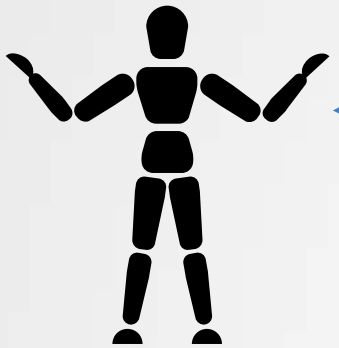
- Organisaties die volgens de CER-richtlijn zijn aangewezen als kritieke entiteit. Automatisch een essentiële entiteit volgens de NIS2-richtlijn.
- Grote organisaties die actief zijn in een van de zeer kritieke sectoren.
  - minimaal 250 werknemers of;
  - een jaaromzet van meer dan € 50 miljoen en een balanstotaal van meer dan € 43 miljoen.

B. Belangrijke bedrijven

- Middelgrote organisaties die actief zijn in een van de zeer kritieke sectoren
- Middelgrote en grote organisaties die actief zijn een van de kritieke sectoren
  - minimaal 50 werknemers of;
  - een jaaromzet en balanstotaal van meer dan 10 miljoen euro.

Wie bepaalt of jouw organisatie past in deze criteria?

“Evalueer zelf of uw organisatie onder de NIS2-richtlijn valt.”



?

NIS2?

JA

NEE

NOG NIET…

SCOPE UITBREIDING LIGT IN DE LIJN DER VERWACHTING

https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

Scope NIS 2

Scope Informatiebeveiliging

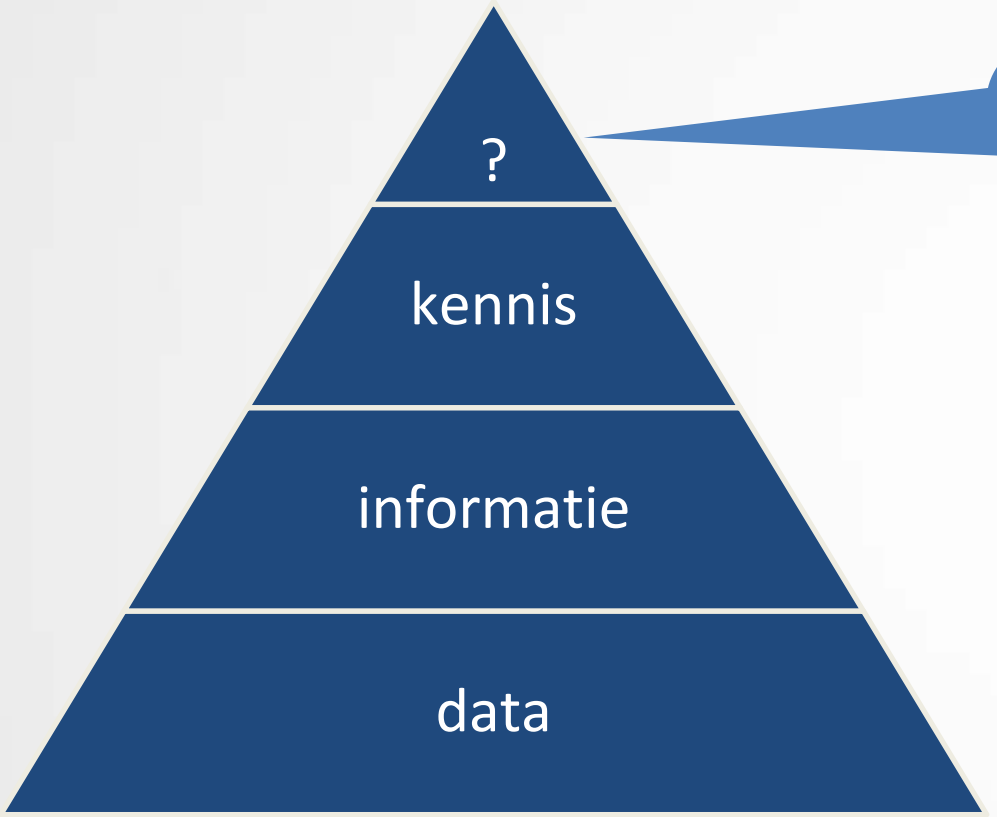
DE KROONJUWELEN VAN DE ORGANISATIE MOETEN PASSEND BESCHERMD WORDEN

Aantoonbaar in control:
Integraal Risico Management

Aantoonbaar in control:
Informatie Risico Management
(Informatiebeveiliging)

=> Conform eisen ISO27001 plus……

Opleiding (artikel 20.2)



Voorziet een e-learning zoals: “wat te doen als je in een phishingmail trapt” hierin?

*Management moeten handvatten krijgen om vervolgens “**wijze**” afwegingen te kunnen maken in het belang van de ketenweerbaarheid als onderdeel van de zorgplicht.*

Invulling van de handhaving

Sectoraal toezicht

Aantoonbaar “in control”

Hoge boetes

Persoonlijke aansprakelijkheid

Break!


Done

Hoe staat je organisatie ervoor op Informatiebeveiliging & op de NIS 2 “focus” processen?

Maak een assessment op management- abstractieniveau met behulp van de tabellen

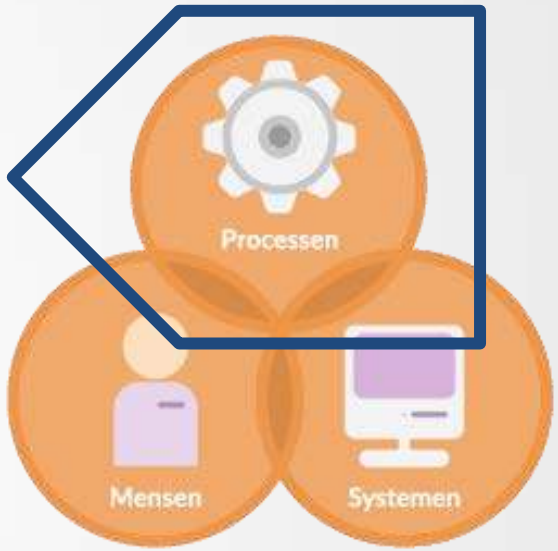
Legenda:

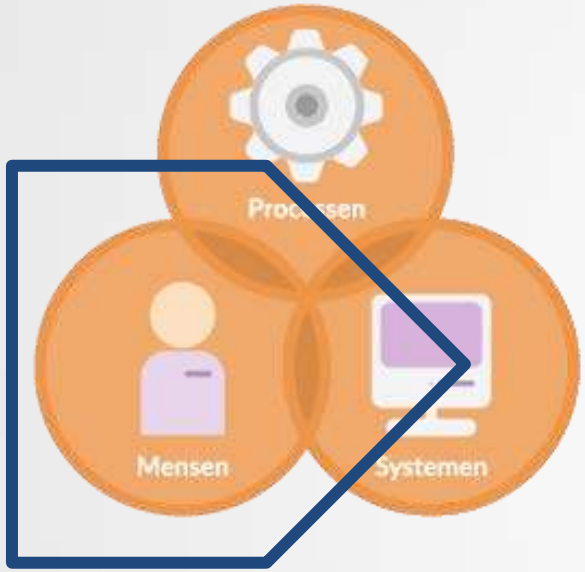
√ = goed

≈ = er is “iets” waar op gebouwd kan worden

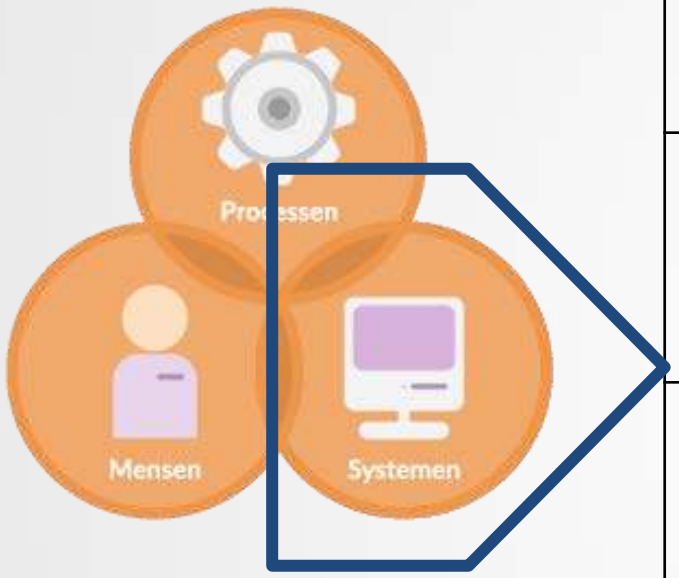
X = niet

Checklist	√	≈	X
Borging informatiebeveiliging in alle organisatie processen die data/informatie gebruiken als continu proces.			
Passende werking van de informatiebeveiligingsprocessen zelf om de organisatie te kunnen faciliteren met preventie, toetsing en incidentmanagement.			
Structurele borging zowel aan het begin (elk proces/project), als tijdens werking als bij afronding, of in geval van projecten bij de oplevering.			
Volgorde van prioriteit wordt altijd bepaald door de risico inschatting op het juiste niveau.			
De afdeling Informatiebeveiliging faciliteert de organisatie bij het realiseren van deze doelstellingen door, onder meer, risico analyses uit te voeren op de processen, organisatorische maatregelen (ook wel “controls”) te bepalen en een besluit tot risico acceptatie te faciliteren met advies voor de Directie.			





Checklist	√	≈	X
Medewerkers kennen hun rol en verantwoordelijkheden (Awareness)			
Medewerkers gedragen zich passend op basis van hun verantwoordelijkheden (Security Behaviour)			
De samenwerking is op Operationeel, Tactisch en Strategisch niveau passend geborgd als continu proces (Governance)			
De afdeling Informatiebeveiliging faciliteert de organisatie bij het realiseren van deze doelstellingen door, onder meer, awareness & behaviour activiteiten door middel van opleiding, communicatie, campagnes.			



Checklist	√	≈	X
De systemen zijn ondersteunend aan processen en security is hierbij als hygiëne aspect aantoonbaar geborgd.			
De systemen en bijbehorende userinterfaces zijn ingericht op basis van maximaal gebruiksgemak in een veilige omgeving => Een veilige omgeving moet prettiger werken dan een onveilige omgeving.			
De afdeling Informatiebeveiliging faciliteert de organisatie bij het realiseren van deze doelstellingen door het uitvoeren van risicoanalyses, het afstemmen van de te nemen technische maatregelen (controls) en het laten uitvoeren van periodieke toetsingen zoals audits en penetratietesten door een ethisch hacker.			

Checklist	√	≈	X
Integraal Risk Management			
Business Continuity Management			
Supply Chain Management			
Crisis Management Organisatie			
Basis Information Security op orde			
NIS 2 Information Security extra vereisten: • Meldplicht • Informatie uitwisseling • Opleiding Management			


DETAIL
TIJD
STRATEGISCH
1 - 3 jaar
TACTISCH
maand - kwartaal
OPERATIONEEL
dag - week

1760-1840

1936 -
heden

18e eeuw | 19e eeuw | 20e eeuw | 21e eeuw

1798
1e Ministerie van
Financiën

2022
Staatssecretaris Koninkrijksrelaties
& Digitalisering

Iedereen heeft ermee te maken.

Veel mensen snappen het belang wel maar de inhoud niet.

Het is een hygiëne proces.

Puzzelen met cijfers en risico's.

The devil is in the detail!

- Hoe is het nu georganiseerd?
- Hoe zou het moeten zijn?

STELLING:
ZONDER PASSENDE GOVERNANCE EN HELDERE AFSPRAKEN OVER DE VERANTWOORDELIJKHEDEN KRIJG JE NOOIT GOEDLOPEND PROCES

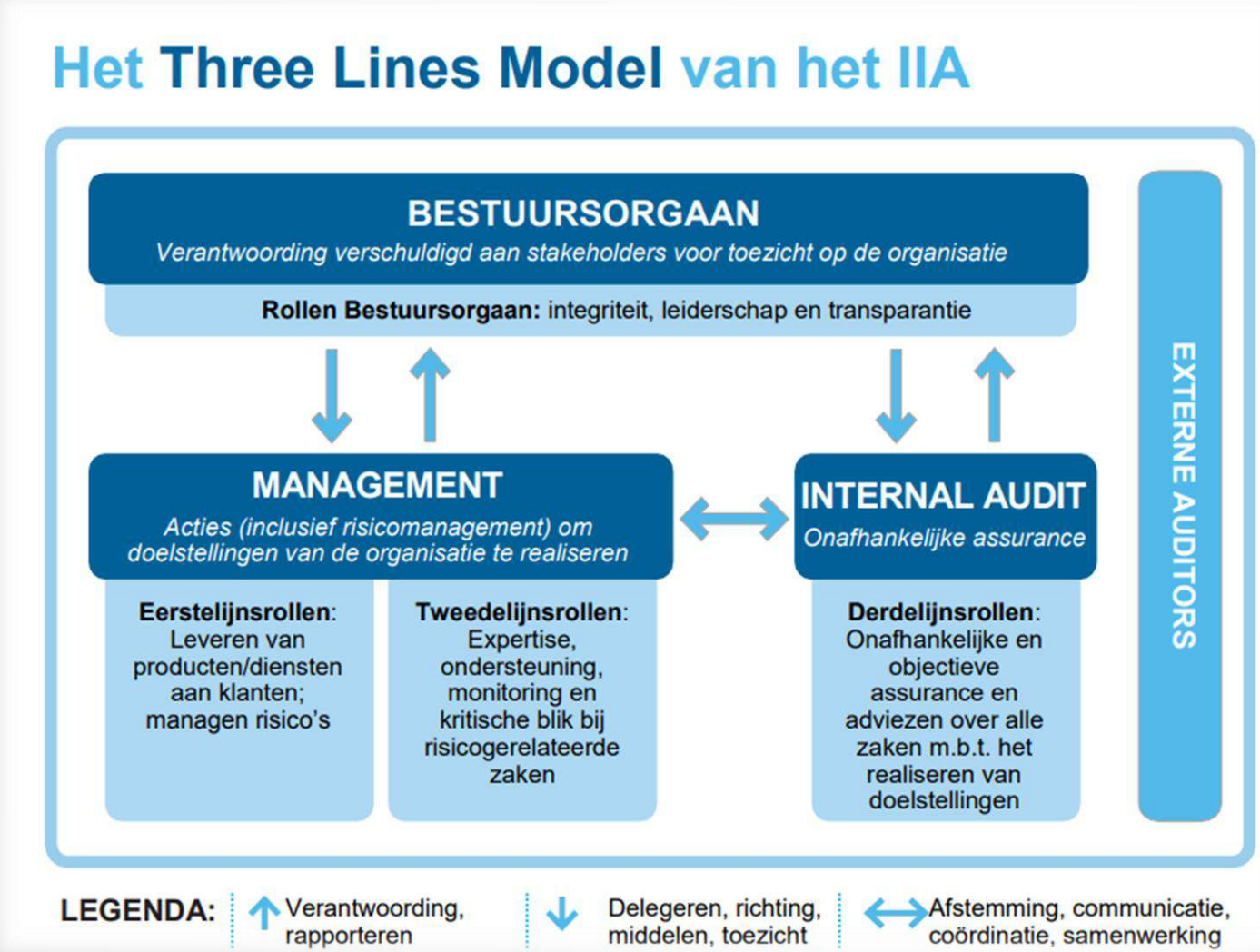
"Organizations are human undertakings, operating in an increasingly uncertain, complex, interconnected, and volatile world.

They often have multiple stakeholders with diverse, changeable, and sometimes competing interests.

Stakeholders entrust organizational oversight to a governing body, which in turn delegates resources and authority to management to take appropriate actions, including managing risk.

For these reasons and more, organizations need effective structures and processes to enable the achievement of objectives, while supporting strong governance and risk management."

Bron: Instituut van Internal Auditors


Het Three Lines Model van het IIA
BESTUURSORGAAN
Verantwoording verschuldigd aan stakeholders voor toezicht op de organisatie
Rollen Bestuursorgaan: integriteit, leiderschap en transparantie
MANAGEMENT
Acties (inclusief risicomanagement) om doelstellingen van de organisatie te realiseren
Eerstelijnsrollen: Leveren van producten/diensten aan klanten; managen risico's
Tweedelijnsrollen: Expertise, ondersteuning, monitoring en kritische blik bij risicogerelateerde zaken
INTERNAL AUDIT
Onafhankelijke assurance
Derdelijnsrollen: Onafhankelijke en objectieve assurance en adviezen over alle zaken m.b.t. het realiseren van doelstellingen
EXTERNE AUDITORS
LEGENDA:
Verantwoording, rapporteren
Delegeren, richting, middelen, toezicht
Afstemming, communicatie, coördinatie, samenwerking

Managementvertaling: 3 Lines

1ste lijn	2de lijn	3de lijn
• Verantwoordelijk voor uitvoering • Risico eigenaar van het primaire proces • Bevat alle business units en de ondersteunende diensten zoals onder meer ICT, HRM, Inkoop, Juridische Zaken, Finance.	• Vertaalt de wettelijke en de door de organisatie gekozen kaders naar de 1e lijn • Adviseert, faciliteert modellen, tools, formats • Organiseert, controleert en rapporteert aan het hoogste bestuursorgaan op basis van de geïdentificeerde risico's.	• "Is er niet van" • Controleert de 2e en 1e lijn • Rapporteert onafhankelijk aan het hoogste bestuursorgaan

	1ste lijn	2de lijn	3de lijn
	• Verantwoordelijk voor uitvoering • Risico eigenaar van het primaire proces • Bevat alle business units en de ondersteunende diensten zoals onder meer ICT, HRM, Inkoop, Juridische Zaken, Finance.	• Vertaalt de kaders naar de 1e lijn • Adviseert, faciliteert modellen, tools, formats • Organiseert, controleert en rapporteert aan het hoogste bestuursorgaan op basis van de geïdentificeerde risico's.	• "Is er niet van" • Controleert de 2e en 1e lijn • Rapporteert onafhankelijk aan het hoogste bestuursorgaan
Operationeel			
Tactisch			
Strategisch			

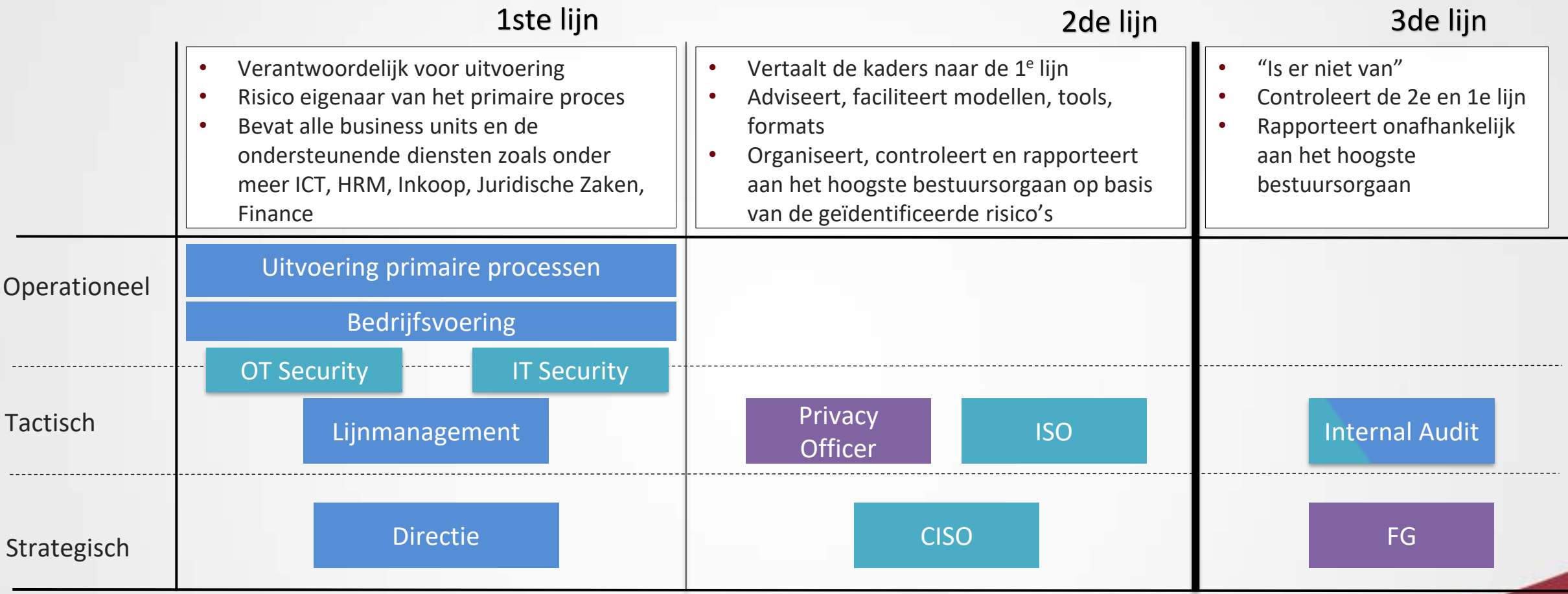
Hoe liggen de rollen & verantwoordelijkheden? Plot de rollen –zoals het zou moeten zijn- in het 3 Lines/OTS-model

Plot de volgende rollen in het model

- Directie (C-level)
- Lijnmanagement
- Uitvoeringsafdelingen/business units
- Bedrijfsvoering/Ondersteunende processen
- IT Security (TSO) - OT Security (OTSO)
- Interne Audit
- CISO
- ISO
- Privacy Officer
- Functionaris Gegevensbescherming

En indien hierboven niet benoemd: je eigen rol

3 Lines & OTS i.r.t. Privacy en InfoSec



3 Lines & OTS i.r.t. CMO, BCM en Supply Chain

	1ste lijn	2de lijn	3de lijn
	• Verantwoordelijk voor uitvoering • Risico eigenaar van het primaire proces • Bevat alle business units en de ondersteunende diensten zoals onder meer ICT, HRM, Inkoop, Juridische Zaken, Finance	• Vertaalt de kaders naar de 1ste lijn • Adviseert, faciliteert modellen, tools, formats • Organiseert, controleert en rapporteert aan het hoogste bestuursorgaan op basis van de geïdentificeerde risico's	• "Is er niet van" • Controleert de 2e en 1e lijn • Rapporteert onafhankelijk aan het hoogste bestuursorgaan
Operationeel	Uitvoering primaire processen Bedrijfsvoering		
Tactisch	Lijnmanagement		
Strategisch	Directie		

"NIS 2 is here to stay"

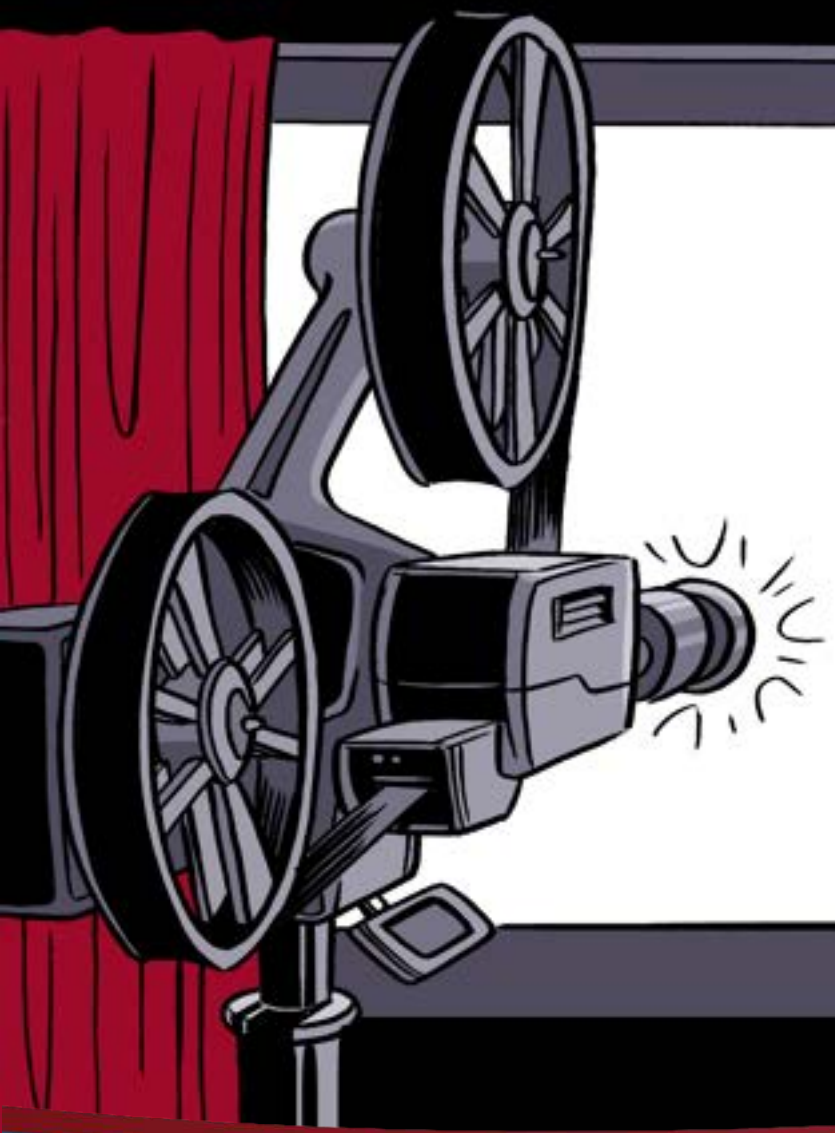
De meeste organisaties zijn nog niet "NIS 2 proof", *en we snappen ook waarom*

Organisatieverandering lukt alleen met de juiste "Tone at the Top", *zeker bij hygiëne processen*

Je hebt nu wat handvatten over waar je moet beginnen en welke organisatorische keuzes er gemaakt moeten worden *(toch?)*

Tip: "80 is prachtig" en hou het proportioneel

https://www.omdenken.nl/



The End

Dank voor jullie aandacht en nog veel plezier op het event ☺