Duurzaamheid en de verschillende manieren waarop dit impact heeft op de speelvelden van ERM, beheersmaatregelen (controls) en audit

Van compliance naar waarde creatie

Paul Weel - Randstad

Diana Maissan - Kiwa

The Institute of Internal Auditors Netherlands

IIA CONGRES 2026 PRIDE & PREJUDICE

4 & 5 JUNI AFAS THEATER LEUSDEN

Ontspan en haal diep adem

Belangrijke PSA

We delen hier geen wetenschappelijk onderbouwde inzichten

we delen ONS inzicht en kijken uit naar jullie reflectie!

We stellen ons even voor

Paul Weel
Randstad
Director Risk & Audit

Diana Maissan
Kiwa (part of SHV)
CSRD Program Manager

Openingsvraag

Stelling:

‘mijn organisatie werkt aan ESG implementatie en ik als auditor / risk professional ben hier (volledig) bij betrokken’

Raise your hand when asked:

1- niet gestart/gestart, maar niet betrokken

2- gestart, maar voornamelijk betrokken voor CSRD/Netzero elementen.

3- gestart en volledig betrokken

The Institute of Internal Auditors Netherlands

IIA CONGRES 2026 PRIDE & PREJUDICE 4 & 5 JUNI AFAS THEATER LEUSDEN

Even stapje terug: wat is ESG / Sustainability ook alweer?

Wat we zien van ESG / Sustainability

ESG vision and mission statement

Travel policy

Scaling up and down

ESG report

Lease car policy

DMA

ESRS

Talent attraction and retention

HSE policy

Sustainability website

HSE targets and rates

limited assurance

Training portal

CSDDD

policies related to Code of Conduct, anti-bribery and corruption

CSR Performance Ladder

Safety measures

Diversity and inclusion in HR policy

Speak Up line

Sustainability officer

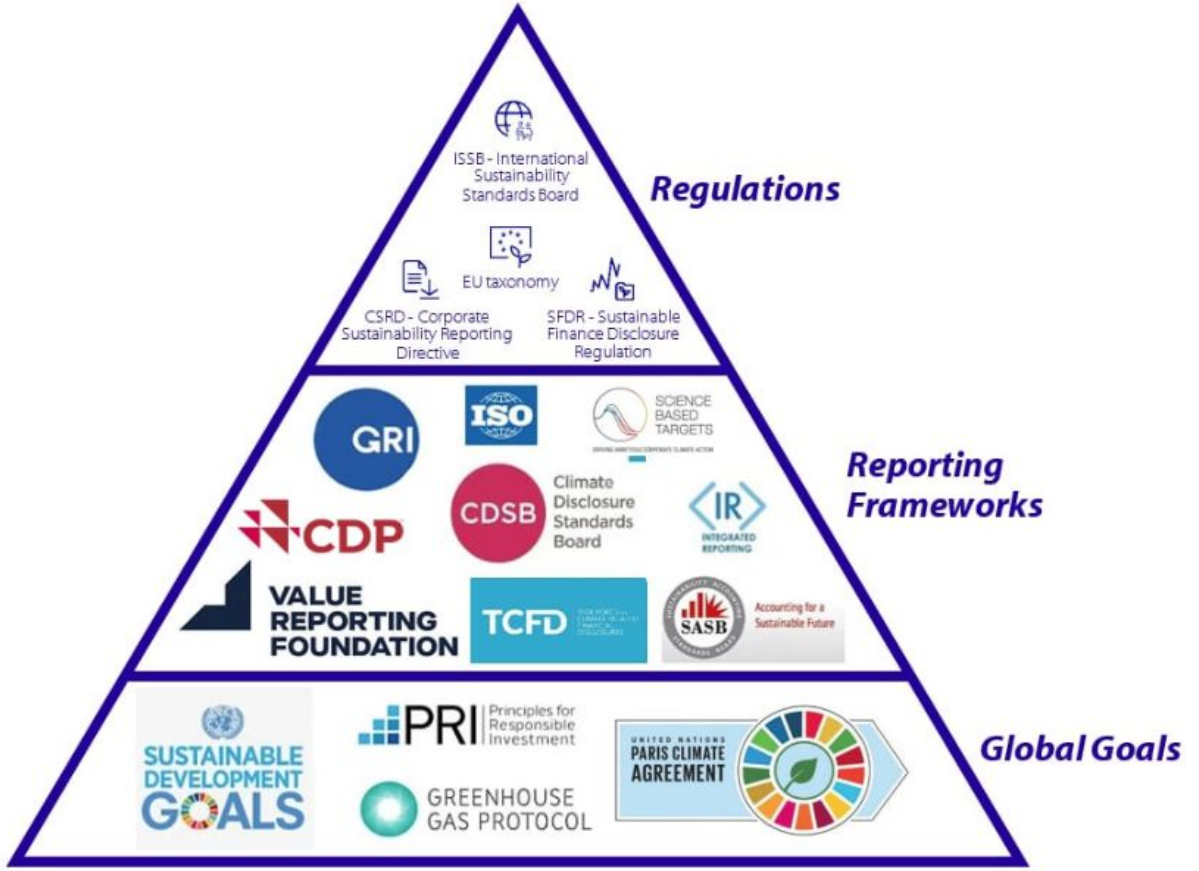
Global job framework

Greenwashing

Local supplier policies

De inmiddels beroemde alfabet soep

De brei van vele regels en wetgeving



Lekker Diana & Paul

Vertel ons eens iets dat we nog niet wisten!

Ok

Hoe relevant is die zogeheten alfabet-soep nu echt?

Wat is de impact op/van ERM, interne beheersmaatregelen en audit?

Ons antwoord in 3 delen

- Typische “types” in ESG/Sustainability
- Maturity denken als houvast
- De keuze die risk management, controls en audit KAN en/of MOET maken

Typeringen in ESG/sustainability

We doen dit omdat…

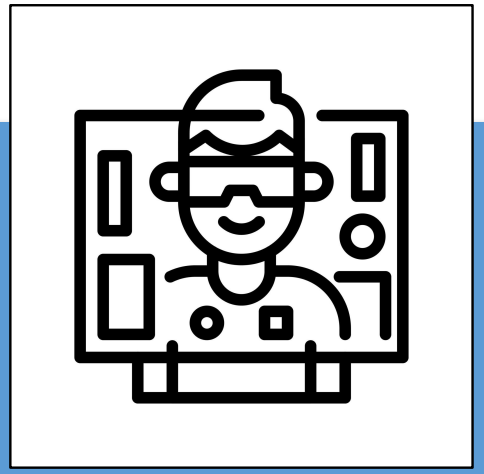
het moet van de **wetgever** (b.v. CSRD)

we het belangrijk vinden vanuit de **kern van ons bedrijf**

het moet om onze **reputatie** te beschermen (bv onder druk van **activisten**)

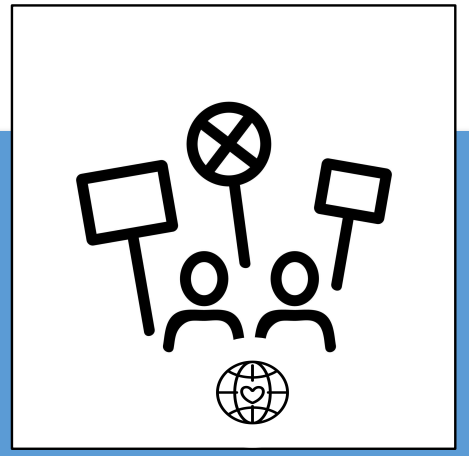
CSRD and Sustainability related legislation may be new, but the earth isn't. And if we don't take action we will extinct ourselves, not just the earth

Sustainability ‘archetypes’



De compliance administrateur

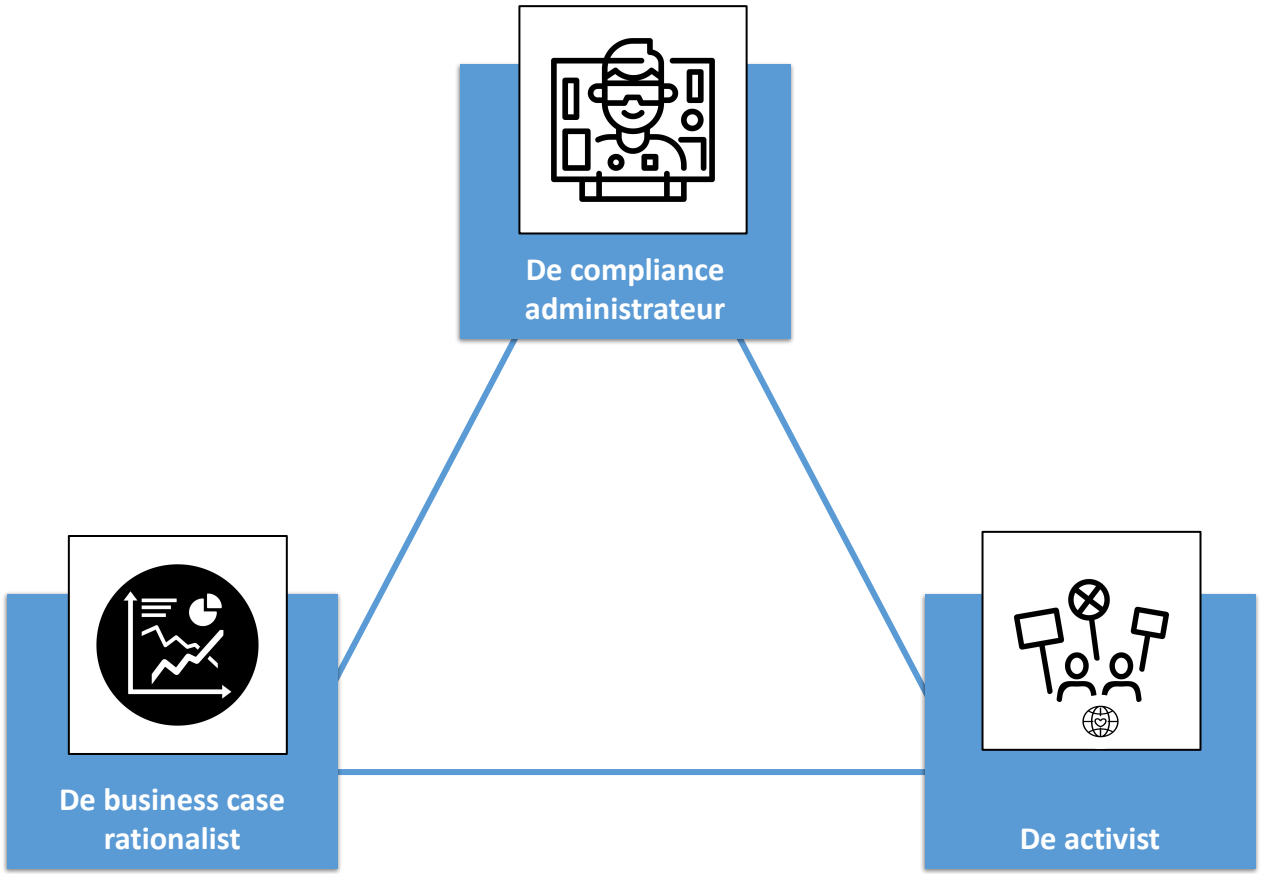
De business case rationalist



De activist

Note: dit is een stereotypering om als voorbeeld voor de discussie te dienen

Sustainability ‘archetypes’ in de mix

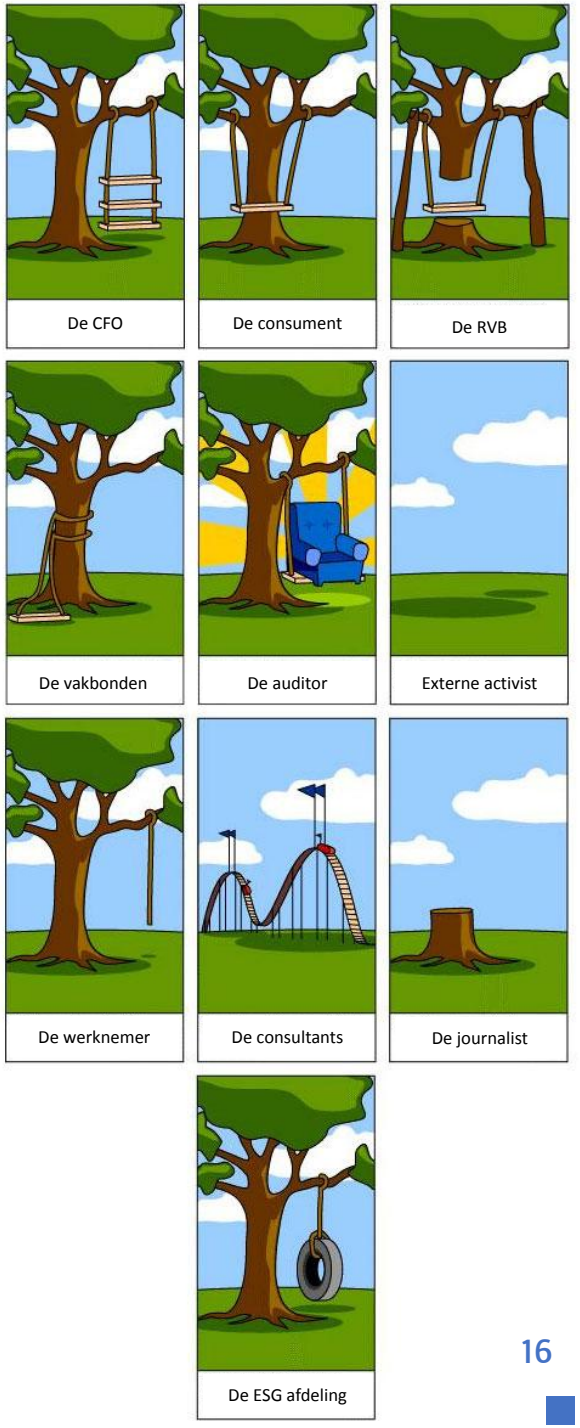


Senior stakeholders dragen ‘archetypes mix’ met zich

Belangen, ervaringen en wereldbeelden zijn persoonlijk, de mentale CV

Stakeholder triggerpoints

- compliance of business?
- business models of AO/IC?
- financieel resultaat of opbrengsten?
- De wereld beter maken of het bedrijf succesvol maken?



Waar zitten de “allergieën”

En lijkt daarom het spanningsveld in leven gehouden te worden

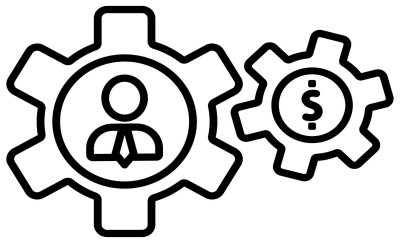
CEO / COO

CFO

verdienmodel voor consultants

Compliance

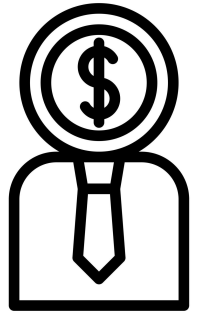
Must do



Is idealistisch

Gericht op welk probleem?

Gezien als een “slow down” voor groei en weinig toegevoegde waarde voor busines



Kost alleen maar geld

een hype

Is voor bomenknuffelaars – waar is de data

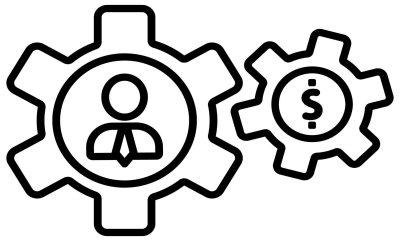
Prioriteit voor jaarverslag

Waar zit de mogelijke connect

Op basis waarvan er met management een gesprek op gang gebracht kan worden

CEO / COO

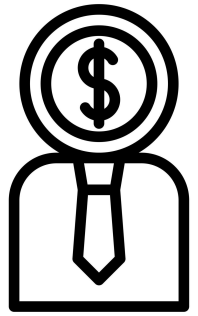
Compliance als guidance in plaats van “must do”



ESG als key success factor ook naar je klanten

ESG is gelinkt aan de business strategie en geeft belangrijke inzichten voor business growth

CFO



Meetbare data leidt tot inzicht in oorzaken van financiële cijfers

Data leidt tot mogelijkheden voor kosten reductie

ESG op geïnformeerde manier oppakken kan ook inhouden GEEN actie te nemen

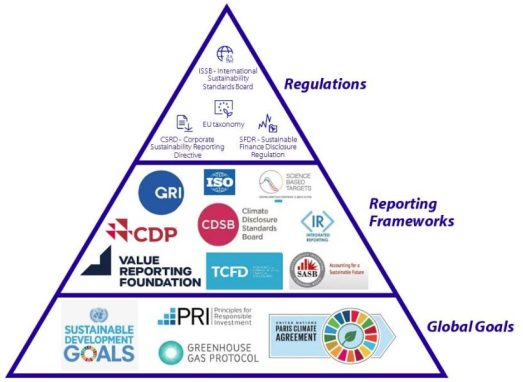
De harde praktijk

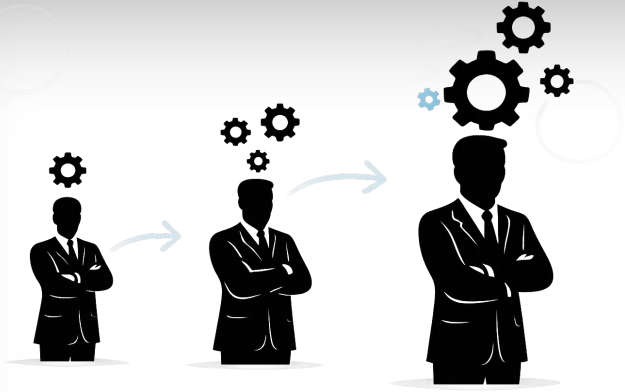
Wat zien we nu gebeuren: mede veroorzaakt door de soep aan wetgeving en rapportageverplichtingen

ESG als data en compliance exercitie

Onzichtbare strategische waarde / verankering

Risico van beperkte focus





ESRS lering en voortschrijdend inzicht

EN (not least)

Omnibus

it made management think…… how to move forward?

Dit leidde tot....

Het gelijk van de compliance 'push' vs market en company strategy 'pull/push'

kaarten op tafel in prioriteiten

'let's now make sure we bring down the workload'

wat ons brengt op maturity denken als houvast

Maturity denken als houvast

change is a process, not an event

Ten eerste: organisatorische volwassenheid in ESG

Ten tweede: de stappen van de Internal Auditor

Mentaliteitsverandering auditors

Auditors moeten voorbij de data en regels kijken naar waar waarde gecreëerd kan worden door intenties en samenhang te onderzoeken.

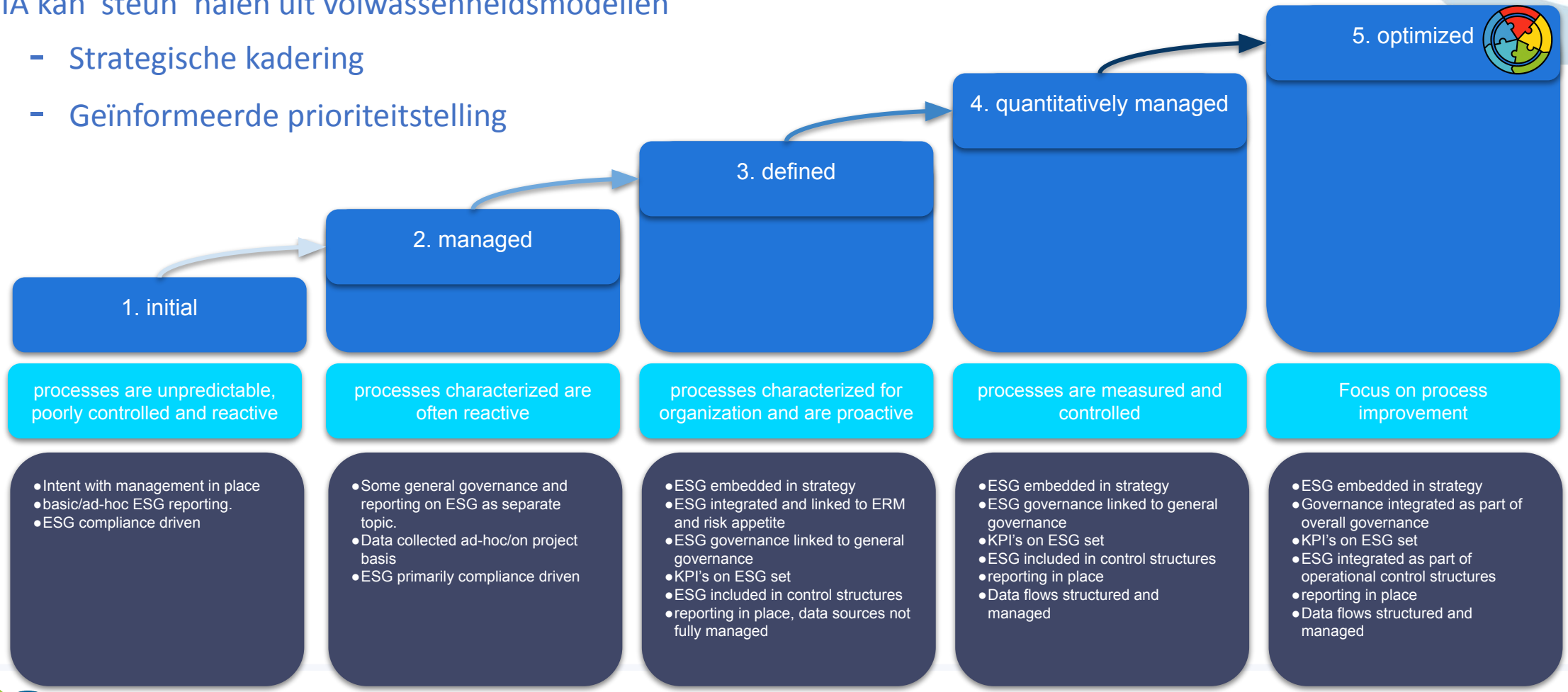
CSRD als middel, niet doel

CSRD creëert ruimte voor gesprekken over waarde creatie, impact en lange termijn bestendigheid

OK, en dan, hoe verder?

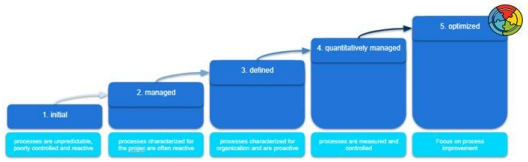
IA kan ‘steun’ halen uit volwassenheidsmodellen

- Strategische kadering
- Geïnformeerde prioriteitstelling



ESG definition

Doelstellingen kunnen / moeten variëren



Huidig maturity level	To move up…
1	Borgen regulatory compliance
2	Zorgen dat compliance kosteneffectief is en targets aansluiten bij bestaande business modellen en doelstellingen.
3	Ambities heroverwegen en integreren in lange termijn strategie, business modellen en interne governance
4	Optimalisatie van structuren door integratie en automatisering (incl. AI). Governance integratie
5	Nirvana: geen noodzaak meer voor aparte ESG afdelingen of chief sustainability officer, het is nu echt volledig geïntegreerd => in stand houden is de uitdaging

!! Essentiële vraag voor management: Welk volwassenheidsniveau wilt u naar toe? !!

Blijf ontspannen en blijf diep ademhalen

Dus… hoe gaat de IA/RM/IC afdeling(en) dit effectief inzetten

De keuze die risk management, controls en audit KAN en/of MOET maken

De shift

Kortgezegd: minder ESRS compliance meer ‘business balance’

Traditionele compliance auditor:	De ‘traditionele auditor’ richt zich op controle en rapportage volgens vastgestelde normen en regels.
Rol van critical friend:	De critical friend daagt uit, stelt kritische vragen en ondersteunt bij het verbeteren van processen.
Andere vaardigheden vereist:	Strategisch denken, communicatie en stakeholdermanagement zijn essentieel voor de modern auditor.

Wat doet de business en wat heeft de business nodig?

Wat suggesties voor gesprekken

die gevoerd kunnen/moeten worden

Balans tussen bottom only vs top down

Huidige audits focussen nog veel op KPI's, control uitvoering en reporting.

- Welke KPI's zijn echt nuttig?
- Welke targets worden gebruikt (context)?
- Vergeleken met peers: doet het bedrijf het beter of slechter?
- En dan toch: is de data volledig en juist (genoeg)?

Verleg de audit focus:

Audit richt zich vaak alleen op KPI's, controls en reporting, zonder de diepere waarom-vraag te stellen.

- Wat is de strategische relevantie?
- Welke elementen buiten compliance frameworks om bekeken zijn relevant?
- Hoe loopt de lijn van policy naar operatie (inclusief targets)?

Challenge de governance en responsibilities:

Gezien bovenstaande is het niet altijd even logisch waar de bewijslast / finance / data vandaan komt:

- Waarom zit de gemiddelde Sustainability Reporting specialist binnen Finance?
- Waarom wordt gemiddeld genomen de CSRD audit het meest besproken met Finance / CFO?
- Hoe vaak wordt de COO / CEO betrokken in dit gesprek?

Voorkom polarisatie (silo's) -> integreer

Wat zien we in de praktijk nog veel gebeuren:

- ESRS based audits -> ophalen / valideren van data
- Valideren van alleen het data process en controls
- Ondersteund bij Double materiality assessments?
- Internal control structuren versterkt => CSRD based of anders….?
- Management gesteund om tot een VOR aftekening te komen?

Maar hebben we ook…..

- De Governance omtrent ESG gechallenged?
- DMA en ERM geintegreerd?
- ESG controls geintegreerd in het internal control framework en de assessments?
- De logische lijn van strategie naar Policies naar Targets naar KPI's naar operations geaudit?
- Operationele embedding in business processen geborgd?
- Data en onderliggende structuren geanalyseerd op efficiëntie?

Uiteindelijk komt het neer op: voorkom verkokering van werkvelden! - > De beroemde silo's

Voorbeelden uit onze praktijk

The Institute of Internal Auditors Netherlands

IIA CONGRES 2026 PRIDE & PREJUDICE
4 & 5 JUNI AFAS THEATER LEUSDEN

kiwa

creating
trust
driving
progress

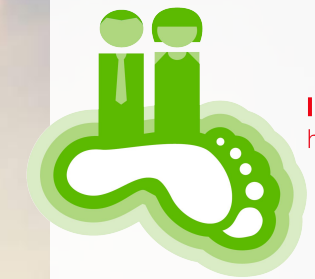
General Principle 1

Countries representing 80% of business certified to **CSR Performance Ladder Level 3**

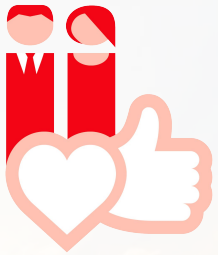
CSR Performance Ladder

3 Focal Points

Reducing our CO_2 footprint



Improving employee health and satisfaction



Enlarging the impact of our services on sustainability

General Principle 2

Certified country chooses and elaborates 2 United Nations **SDG Targets**

De introductie van de CSR-prestatieladder (PL) in 2015 markeerde Kiwa's eerste gestructureerde benadering van ESG. De CSR PL wordt geleid door twee algemene principes en geïmplementeerd via drie aandachtsgebieden (focuspunten), die inzicht bieden in de drie domeinen People, Planet en Performance. Dit sluit nauw aan bij onze strategie en is verankerd in onze doelstellingen.

Een voorbeeld – ESG in de praktijk - Kiwa

ESG in functionele lijnen

- HSE
- HR
- Legal & E&C
- Finance
- M&A
- Operational business

ESG als functie

- ESG Governance / gremia
- CSRD implementatie & DMA
- Integratie in policies – met policy analyze
- ESG Strategy en targets
- ESG report
- ESG trainings
- Planet Week
- GHG data verzamelen, analyse en rapportage
- Capex/Opex investeringen gelinkt aan ESG
- ……

ESG als service

- Sustainability Business Sector

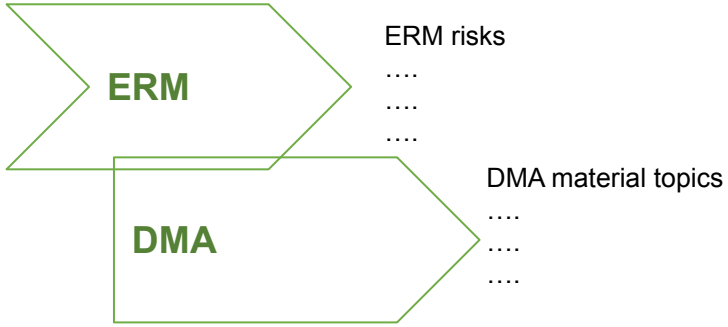
https://www.kiwa.com/en/markets/sustainability/

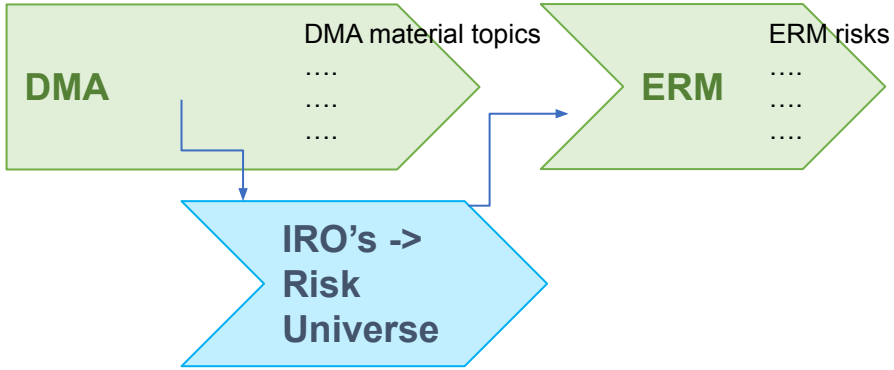
Een voorbeeld – ESG in de praktijk - Kiwa

Work in progress:

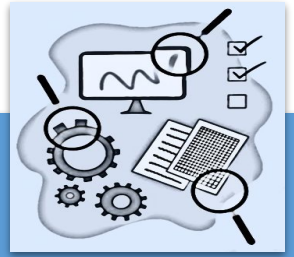
- Update DMA en integratie met ERM proces
- DMA threshold gelinkt aan risk appetite

- ESG/CSRD processen en controls in business processen: voorbeeld - Capex/Opex in Finance forecasting process
- Verdere ontwikkeling van het Kiwa data lake tbv een gestructureerde data flow
- Verdere uitrol van ESG bij Due Diligence
- Verder update van de ESG Strategy en targets
- ESG report naar CSRD vereist format
- ESG training (eLearning) in Kiwa Academy
- …….





Hoe zien wij hier een rol voor Internal Audit en Risk & Control



Internal Audit:

- Quality Assurance op het implementatie proces
- Audit plan – risk based en breder perspectief
- ESG meenemen in audits: check/advies op o.a. Governance, process, controls en local ownership

Internal Audit & Risk&Control:

- Advies op proces en control ontwerp documentatie
- Advies bij de walk through bij proces en control ontwerp

Risk & Control:

- Vertaling CSRD gedefinieerde controls naar het Internal Control Framework
- Integratie DMA en ERM proces
- IRO's voedt een update van de Risk Universe

Randstad

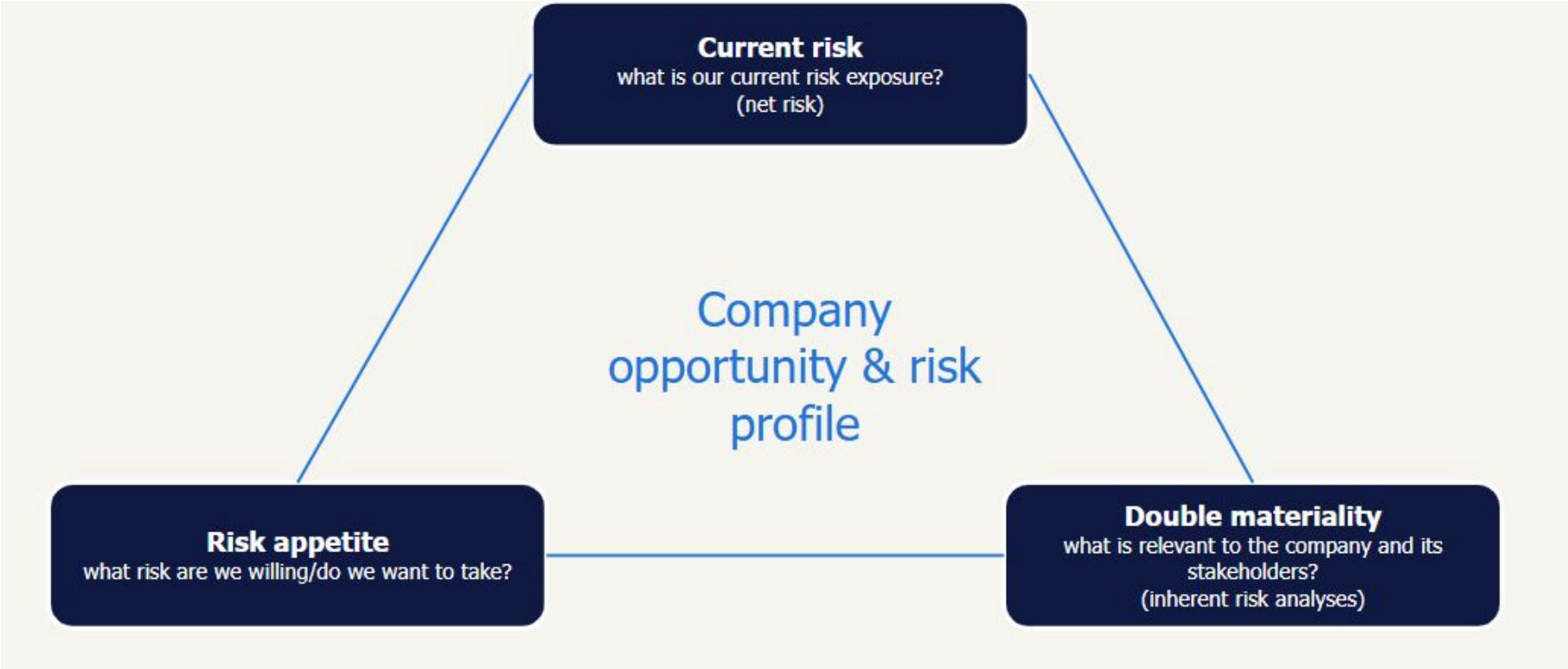
tip van de sluier, onze reis

randstad

partner for talent.

Een voorbeeld, het Randstad perspectief

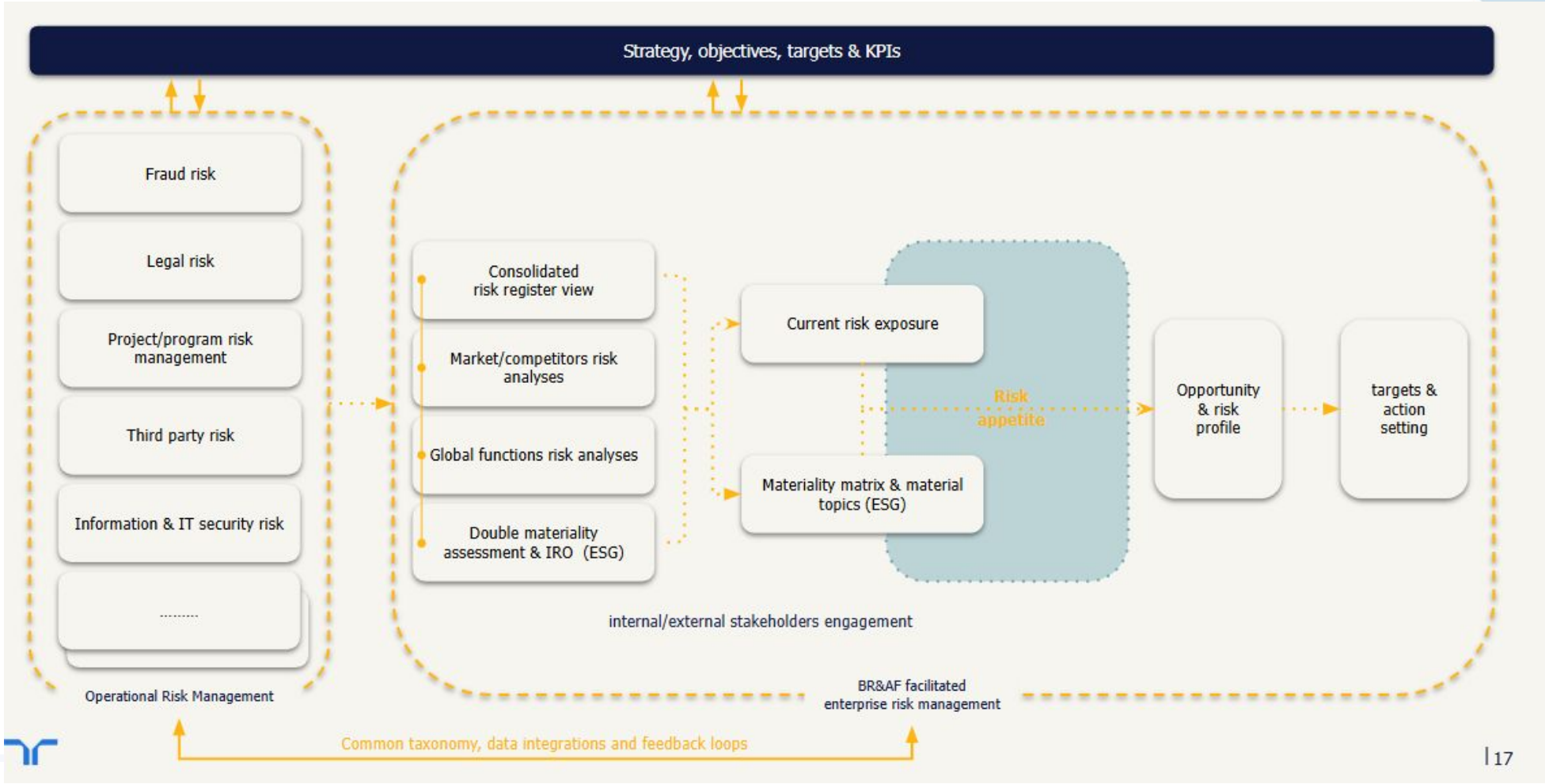
Onze manier om verkokering te vermijden (maar work in progress..)



In integratie met o.a. VOR verwachtingen

DMA threshold vs risk appetite…

DMA, ORM, ERM: communicerende vaten



logisch maar toch, een hoop belangen bij elkaar!

Een voorbeeld, het Randstad perspectief

Rome was not built in a day, we take it one step at a time

Wat we niet doen:

ESRS/CSRD based auditing

Wat we wel doen:

Van policy/targets naar operatie audits/evaluaties

Maturity level analyse en terugkoppeling

Soll en ist conversaties

- outlook voor governance
- local vs central verantwoordelijkheden

Waar dit mede toe leidt/moet leiden:
relevante inzichten die management in staat stellen keuzes te maken/bevestigen mede op vlak van:

- policy tot operationele management control structuren
- ownership en management commitment (behoefte) voor operational excellence

Samenvattend

Go ahead, close it!

The Institute of
Internal Auditors
Netherlands

IIA CONGRES
2026 PRIDE & PREJUDICE
4 & 5 JUNI AFAS THEATER LEUSDEN

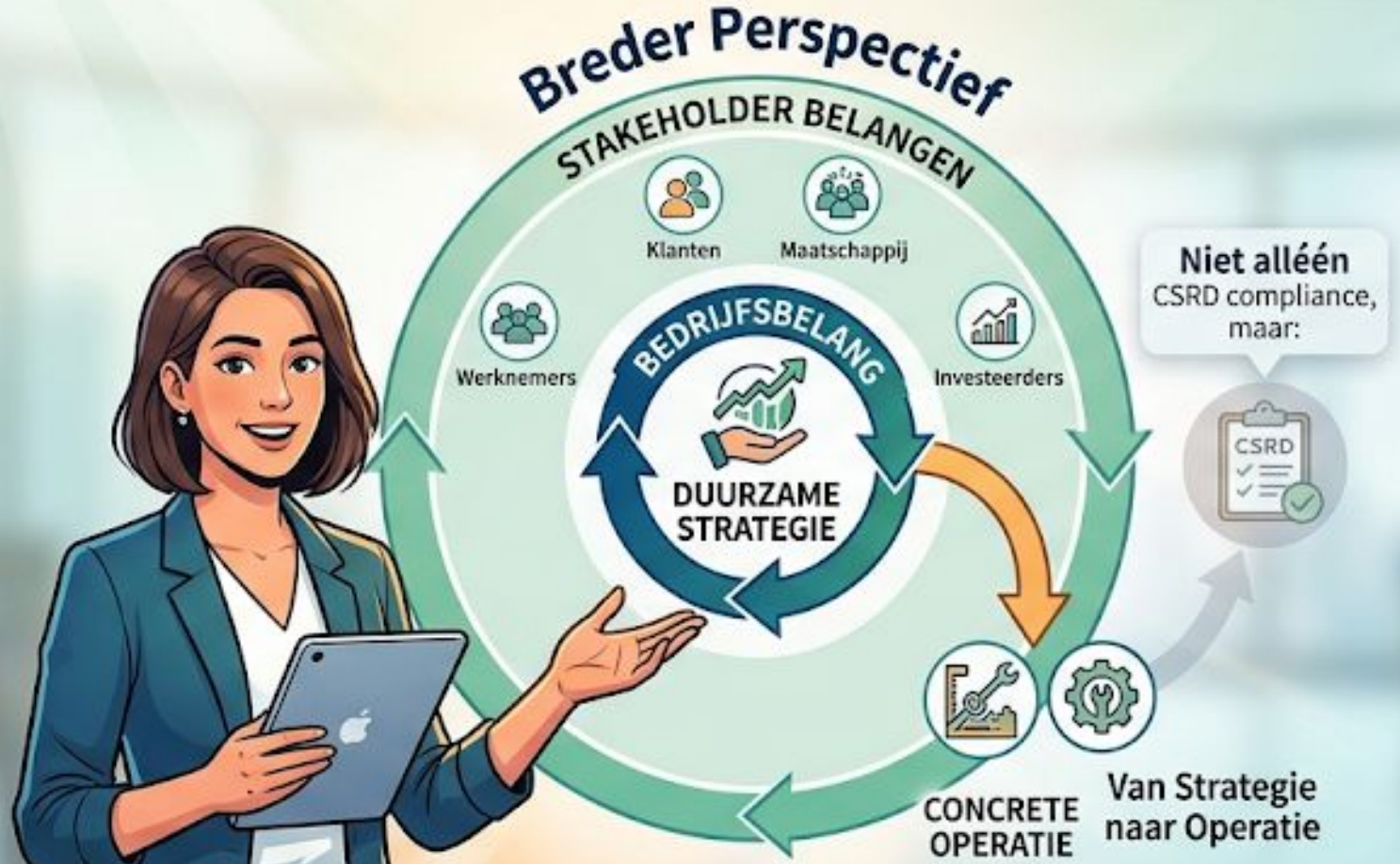
Ok – resume – waar zouden wij starten?
Een checklist naar success

Omgaan met weerstand
- Check uw houding – zit ik goed?
- Adem ik vanuit de buik of zit ik inmiddels hoog in de ademhaling en ervaar ik dus stress.
- Als dit laatste, adem terug naar uw buik.

Reflectie op de rollen
- Check wie welke rol speelt binnen uw organisatie
- Welke weerstand ondervindt u bij welke persoon / rol
- Wat is de invloed van deze persoon / rol binnen uw organisatie
- Wat is de maturity van uw organisatie? Of delen van de organisatie? -> welk gesprek kan ik op welk niveau gebruiken?
- Begrijp de balans: is de trias politica van ESG (je hebt alle drie de rollen nodig) in balans. Zijn deze alle drie adequaat vertegenwoordigd binnen jouw organisatie?

Vindt de balans
- Heeft u voldoende stappen gezet vandaag?
- Ben ik daadwerkelijk aan het auditen op het gebied wat waarde toevoegt voor de organisatie? => alleen compliance vragen / ook strategische vraagstukken / high risk areas
- Check je Risk Universe en ERM proces en tijdslijnen, en kijk in hoeverre DMA hierin opgenomen kan worden
- Auditor: check deze Risk Universe en IRO's vanuit de DMA, om je risico inschatting voor je audit risk analyses en objectives te versterken
- Link aan de risk appetite!- focus je op high risks of ook nihil risks? (toegevoegde waarde voor bedrijf)

VRAGEN? / Stel ze gerust!



DIT IS UW MOMENT!

Wij horen graag uw gedachten, vragen of opmerkingen over:

- Hoe auditoren een bredere blik kunnen aannemen.
- Het verbinden van strategie met dagelijkse operatie.
- De impact op uw organisatie.

Wij gaan graag met u in gesprek.

YOU GO! # YOU GOT THIS!

Dank u voor uw aanwezigheid, u bent helemaal zen en kan er weer tegenaan!

En denk er aan:

- Make your point or lose my attention
- Keep it simple, stupid
- So what?
- In your shoes
- Stay away from your island – dare to take a boat sometimes and sail away
- NIVEA – niet invullen voor een ander (dus ook niet voor die activist)
- En wat er ook gebeurt……

The Institute of Internal Auditors Netherlands

IIA CONGRES 2026 PRIDE & PREJUDICE 4 & 5 JUNI AFAS THEATER LEUSDEN