Risicomanagement

Een introductie

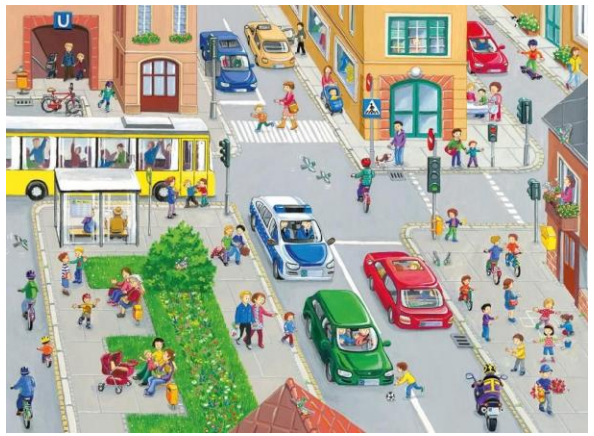
Inhoud

1. Wat is risicomanagement?
2. Wat is een risico?
3. Hoe verhoudt risicomanagement voor informatiebeveiliging tot risicomanagement voor andere thema’s?
4. Wie gaat er over risico’s? Welke taken en verantwoordelijkheden horen daarbij?
5. Hoe oordeel je over een risico?
6. Wat doe je met een risico?

1. Wat is risicomanagement?

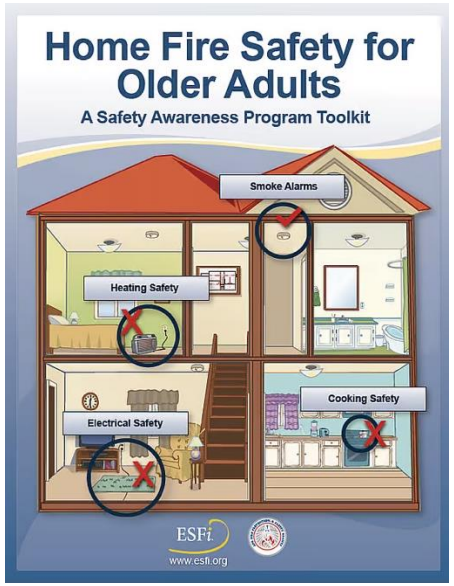
Iedereen doet de hele dag aan risicomanagement

In het verkeer…



Tijdens je sport…

Thuis…

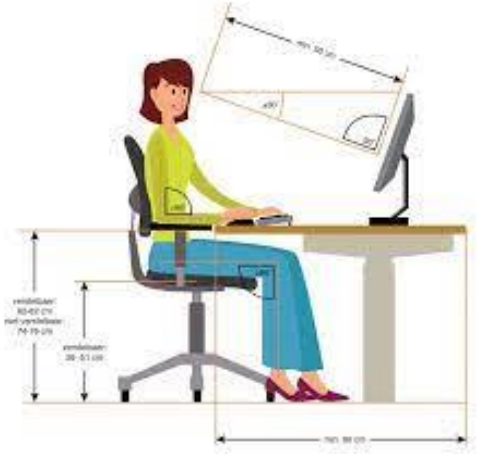


Op het werk zijn we ook gewend aan risicomanagement

voor je project...

voor de campusplanning...

op de werkvloer...



We maken ook steeds bewuster risico-beslissingen voor onze digitale activiteiten

bij vermoedelijke phishing…

zelf keuze maken om mfa in te stellen of niet…

eisen aan ict leveranciers…

SURF Vendor Compliance

Jointly conducting overarching privacy and security risk assessments on vendors

On behalf of institutions, we conduct overarching privacy and security risk assessments on vendors/applications. As far as possible, we negotiate adjustments/contract agreements that benefit the entire education and research sector.

Waarom is het dan soms ongemakkelijk als we er over willen praten?

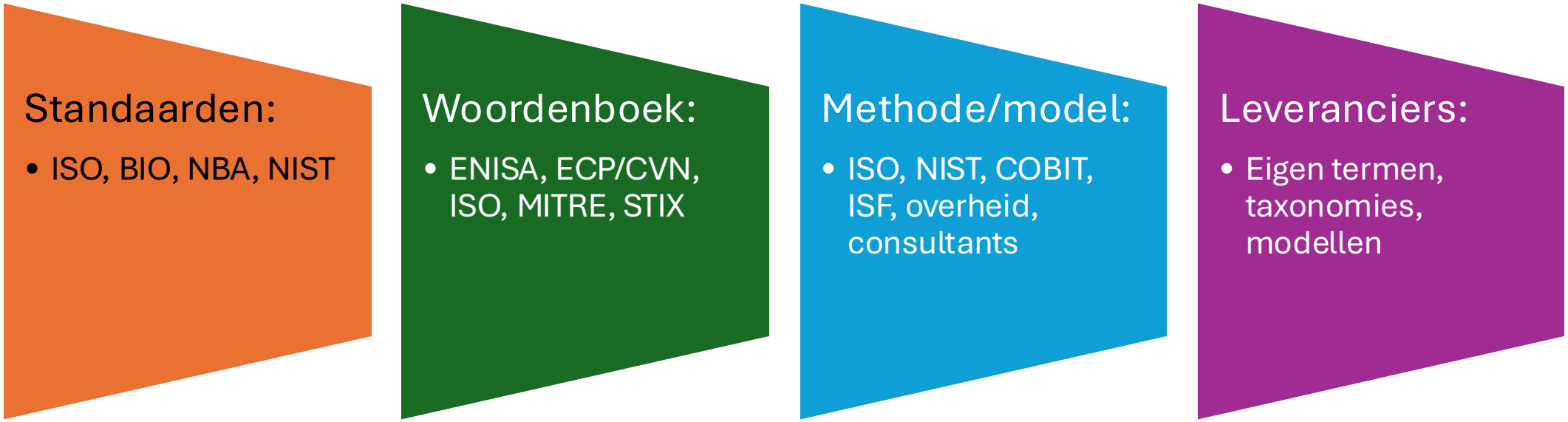
- We praten langs elkaar heen (er bestaan verschillende visies op risicomanagement en verschillende definities)
- We vinden het moeilijk om beslissingen te nemen over risico's
- "Het is zoveel werk"
- "Ik heb geen tijd om er over te praten: geef gewoon een lijstje van wat wel of niet mag"

De visie op risicomanagement verandert

Klassiek risicomanagement (control & compliance)	**Modern doelgestuurd werken**
Methode is leidend (we werken volgens ISO 27001/SURFaudit toetsingskader/andere normen)	Doelen zijn leidend (we willen onze bedrijfsdoelstellingen halen en hanteren principes, afwijkingen zijn niet perse fout)
Geld is dominant (veel aandacht voor kosten en budgetten)	Waarde is dominant (we benaderen risico's vanuit publieke waarden)
Zeker willen weten (alles onder controle)	Onzekerheid toelaten (we gaan om met onzekerheden)
Fouten uitsluiten (systemen en processen dichttimmeren)	Fouten vroegtijdig opmerken (we willen vroegtijdig signaleren voordat het escaleert)
Kansen op risico's verkleinen (maatregelen afvinken)	Gevolgen van risico's verkleinen (we willen kunnen reageren en herstellen)
Compleet willen zijn (we moeten minstens volwassenheidsniveau 3)	Keuzes durven maken (we nemen maatregelen waar dat het meest noodzakelijk is)
Afdwingen (afwijkingen worden afgerekend)	Uitnodigen (we geven het goede voorbeeld en hebben focus op gedrag en motivatie)
Controle (we controleren elkaar)	Vertrouwen (we zijn professionals en we weten hoe te handelen)

Tabel: Van traditionele situatie naar modern risicomanagement (geïnspireerd op Van Staveren (2015, p. 82))

Spraakverwarring door verschillende definities



Wat is risicomanagement?

Coordinated activities to direct and control an organization with regard to risk.

The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options.

Risicomanagement gaat om het inventariseren en beoordelen van mogelijke risico's.

NEN-ISO 31000+C11 (2019)

Het doel van risicomanagement is het creëren en beschermen van waarde.

Risicomanagement zijn gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot *risico's*.

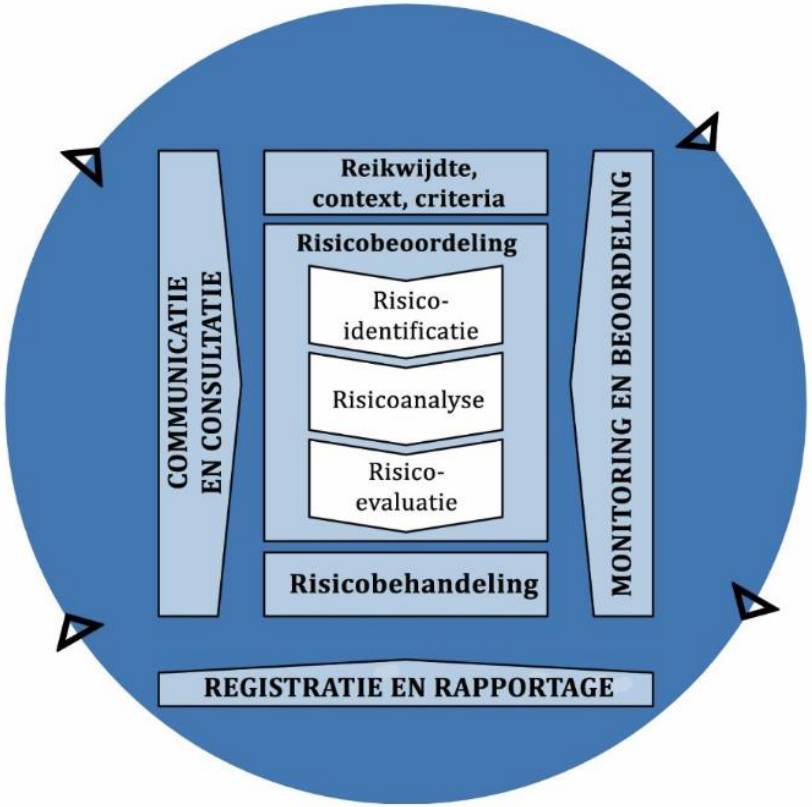
Een risico is het effect van onzekerheid op het behalen van doelstellingen.

Welke gecoordineerde activiteiten zijn dat dan?

Je kunt een internationale norm als uitgangspunt nemen voor de hele instelling, maar dat hoeft niet.

De ene aanpak past niet altijd in alle situaties. Variatie in risicomanagement activiteiten toelaten kan zelfs tot betere inzichten leiden.

Soms heb je ook te maken met samenwerkingsverbanden met andere instellingen die een andere methode hanteren.



ISO 31000 (2019)

6 standaard activiteiten

1. doelen bepalen
2. risico’s beschrijven
3. ernst van risico bepalen
4. beslissen wat te doen
5. effectiviteit van maatregelen evalueren (samen met derde lijn)
6. communiceren en rapporteren (gaat vaak via P&C cyclus)

2. Wat is een risico?

NEN-ISO 31000+C11 (2019)

Een risico is het effect van onzekerheid op het behalen van doelstellingen.

“zonder doelen geen risico, of juist een enorm risico. Want zonder doelen ben je stuurloos en daarmee weerloos overgeleverd aan de onvoorspelbare grillen van de VUCA-wereld”
Quote van M. van Staveren

Wat is dan een risico in context van informatiebeveiliging?

- Deze kun je twee kanten op interpreteren:
  a. Een risico is het effect van onzekerheid op het behalen van **informatiebeveiligingsdoelstellingen**.

  Informatiebeveiligingsdoelstellingen gaan over de eisen (doelen) aan vertrouwelijkheid, beschikbaarheid en continuiteit. Die doelen vind je in de ideale situatie in de ontwerpdocumenten van een proces/systeem/architectuur/onderzoek/project of in de vertaling van strategische instellingsdoelen naar afdelings- of teamdoelen.

  b. Een risico is het effect van **onzekerheid in de informatiebeveiliging** op het behalen van doelstellingen.

  Onzekerheden in de informatiebeveiliging zijn dreigingen en kwetsbaarheden die je nog niet kent. ‘Verwacht het onverwachte’ zoals de NCTV schrijft in het cybersecuritybeeld Nederland 2023.

Keuze in visie op risico's voor informatiebeveiliging – optie A

- Optie a uit de vorige slide is wat veel organisaties doen. Voor alle informatieverzamelingen de doelen beschrijven, de risico's beoordelen en maatregelen doorvoeren. Deze benadering vraagt veel capaciteit, want er zijn veel informatieverzamelingen en dus veel doelen. Het helpt dat er veel best practices en normenkaders bestaan met basismaatregelen om de meeste bekende risico's af te vangen.
- Werk je vanuit deze visie, dan werk je waarschijnlijk ook vanuit de meer traditionele benadering van risicomanagement (slide 8). Immers, risico's die we goed kennen en waarvoor we weten welke maatregelen we moeten treffen zijn geen **onzekerheden** meer. Vaak wordt de verantwoordelijkheid hiervoor gedelegeerd aan een CISO en haar team.

Keuze in visie op risico's voor informatiebeveiliging – optie B

- Optie b is een meer strategische benadering, waarbij de doelstellingen op een hoger abstractieniveau zijn beschreven en gekoppeld zijn aan zakelijke doelen. Omdat je uitgaat van onzekerheden (onbekende risico's) zul je je richten op een kleinere lijst van mogelijke scenario's die je zakelijke doelen kunnen beinvloeden. Hierdoor vraagt risicomanagement minder capaciteit, maar wel andere vaardigheden (bijv. futuring). De eindverantwoordelijkheid kan niet bij de CISO liggen, maar ligt bij degene die verantwoordelijk is voor de zakelijke doelen ('de business') en de processen.

- Optie b sluit natuurlijk optie A niet uit. De bekende problemen moeten worden voorkomen en compliance aan wetten/normenkaders/basismaatregelen moet worden bewaakt, bijv. door een kwaliteitszorg medewerker/procesgerichte security officer.

Maar wij hebben helemaal geen uitgeschreven doelen. Wat nu?

- Als je te maken hebt met vaag beschreven doelen of helemaal geen beschreven doelen moet je een extra inspanning verrichten om ze alsnog helder te krijgen.
- Dat vraagt wel om specifieke vaardigheden. Doelen worden soms bewust wat vaag gehouden om er later mee weg te komen als ze niet helemaal worden gehaald. Om ermee aan de slag te gaan kun je wellicht een facilitator inhuren om een werksessie te begeleiden.
- Werk je uit visie A (slide 16) en moet je informatiebeveiligingsdoelen beschrijven, voer dan een BIA uit.
- Let op dat je prioriteiten stelt, je kunt niet alle doelen nastreven.
- Let ook op het abstractieniveau van doelen; strategische doelen kunnen prima leidend zijn voor informatiebeveiliging. Neem bijvoorbeeld publieke waarden als uitgangspunt.
- Probeer doelen op verschillende niveaus aan elkaar te koppelen via een doelenhierarchie.
- Kom periodiek eens terug bij elkaar voor een beoordeling van de doelen.
- Lees ook eens: “hoe breng ik te beschermen belangen in kaart” van het NCSC

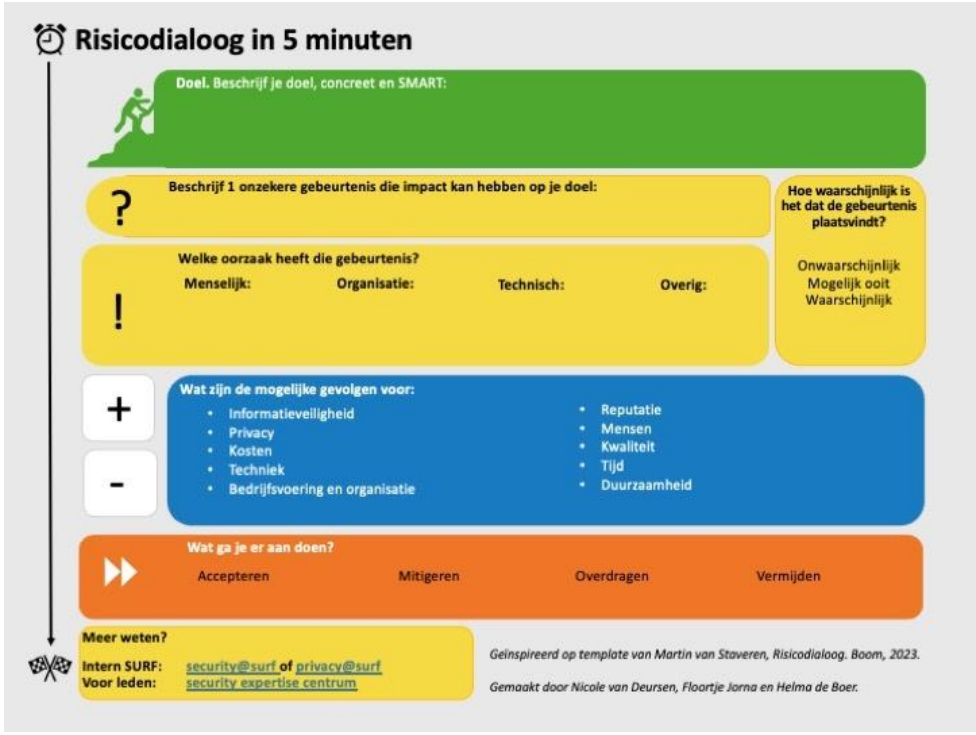
Stel, we hebben een doel, wat dan?

- Dan gaan we in dialoog over onzekerheden, oorzaken, gevolgen. Werk je vanuit visie optie B (slide 18) dan is dit een mooi begin van een proces dat je regelmatig gaat herhalen.

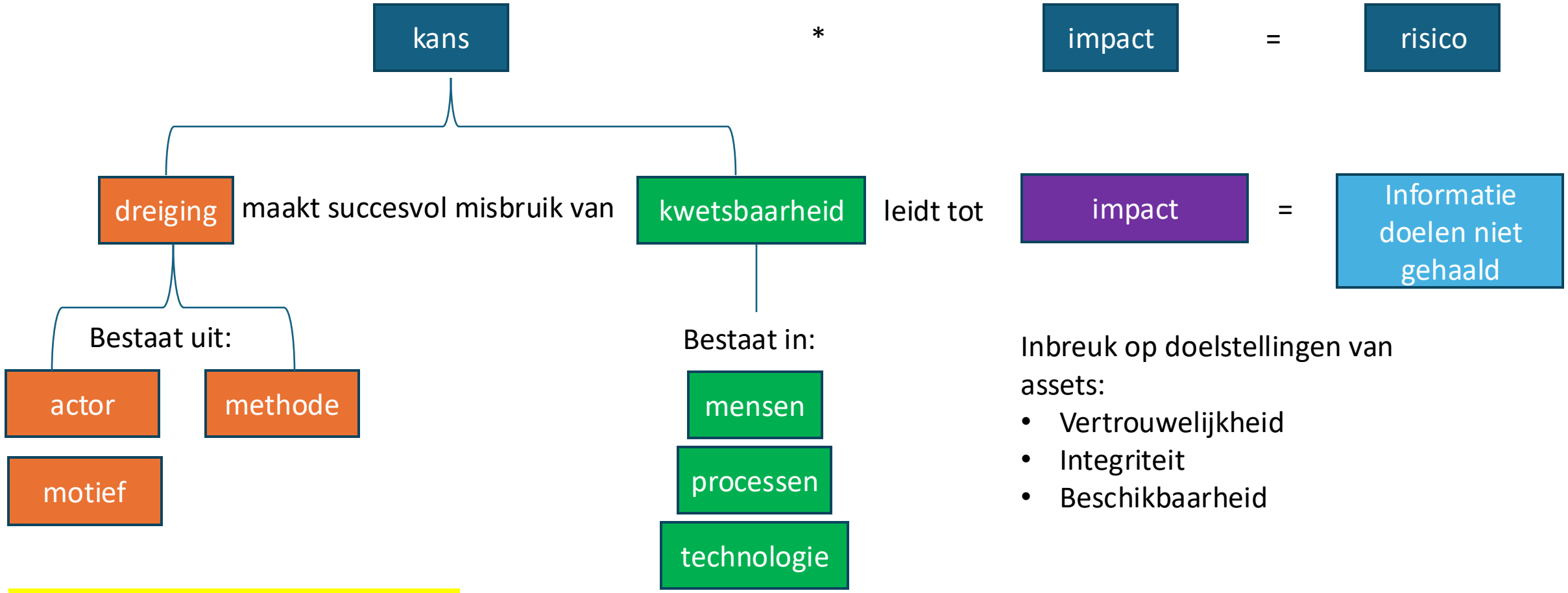
- Je ziet hier al een beetje de samenhang met andere risicogebieden (slide 22).

- Wil je de diepte in op informatie?

  >volgende slide



Anatomie van een **informatie** risico



Inbreuk op doelstellingen van assets:

- Vertrouwelijkheid
- Integriteit
- Beschikbaarheid

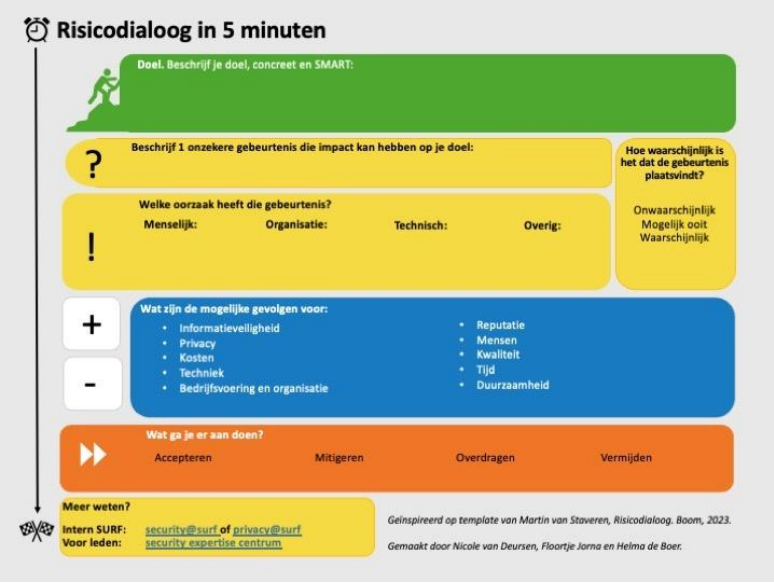
meer info: zie toolkit risicobeoordeling

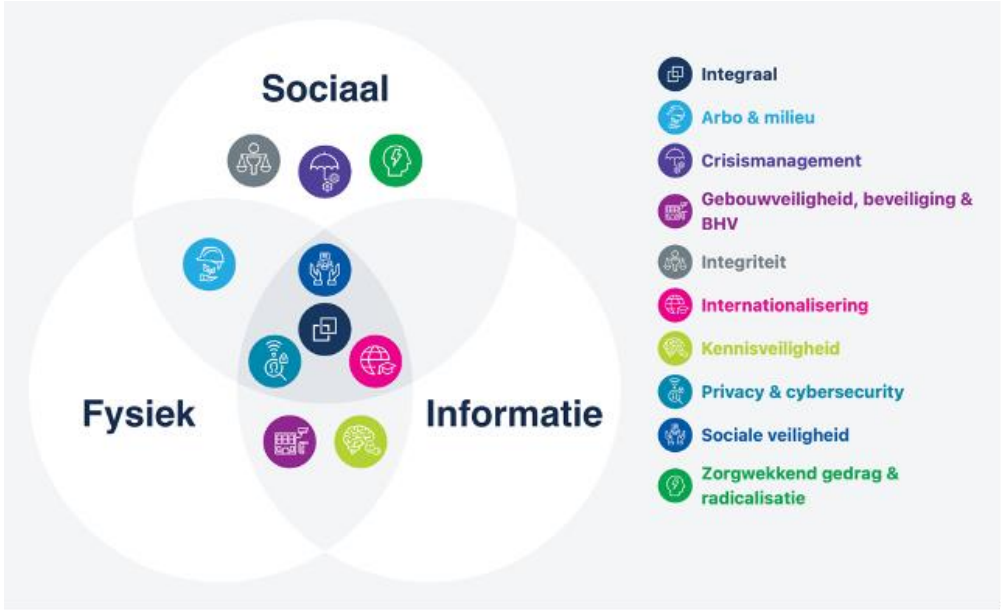
Impact werkt ook door op andere doelstellingen

3. Hoe verhoudt risicomanagement voor informatiebeveiliging tot risicomanagement voor andere thema’s?

Risicomanagement gaat niet over informatiebeveiliging in isolatie

- Je zag het al in het blauwe vak op slide 20 in het template voor de risicodialoog





Bron: Integrale veiligheid Hoger Onderwijs

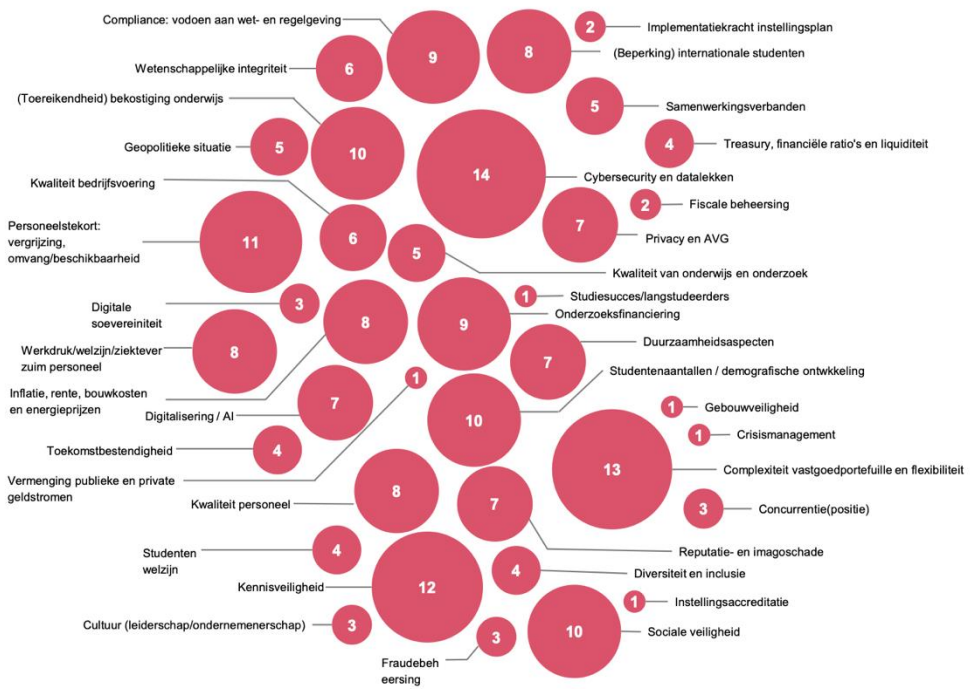
Risicomanagement voor IB moet onderdeel zijn van het bredere risicomanagement

- Dat is efficient
- Dat is logisch als je vanuit doelen werkt
- Toezichthouders letten daar op
- Nationale cybersecurity autoriteiten promoten dit:
  - NIST heeft een kennisbank voor integrating cybersecurity risk in ERM
  - NCSC UK risk management guidance bied ook veel info

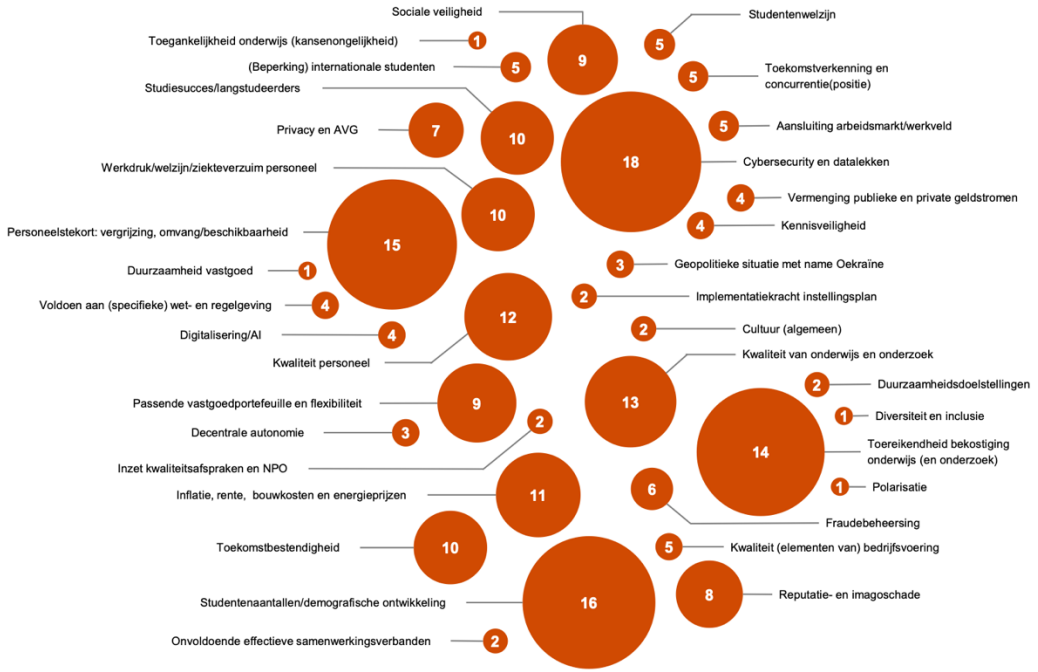
Beslissingen over risico’s gaan over het geheel

- Soms willen we bewust wel een activiteit doen ondanks kans op schade (denk aan e-bike fietsen zonder helm).
- Het budget gaat naar hetgeen met meeste prioriteit (en dat is soms een lekkend dak en niet een lekkend ict systeem)

Kijk maar eens naar alle thema's waar bestuurders een balans in moeten vinden:



Risicothema's in jaarverslagen 2022 Universiteiten



Risicothema's in jaarverslagen 2022 hbo instellingen

bron: pwc benchmark publicaties

4. Wie gaat er over risico’s? Welke taken en verantwoordelijkheden horen daarbij?

Wie gaat er over risico’s?

nee, Uncle Sam is er niet van.
En de CISO ook niet.

Iedereen is verantwoordelijk voor eigen doelen

- Jij werkt naar een doel, dus jij hebt je eigen risico's.
- Soms kun je oplossingen voor risicobeheersing in gezamenlijkheid doen, bijv. via je eigen ict-afdeling of via de cooperatie SURF. Dat scheelt geld en tijd, maar soms krijg je dan een oplossing die niet ideaal is voor jou en daar moet je je bij neerleggen (en geen geitenpaadjes gaan bedenken)
- Maar zij gaan niet over jouw doelstellingen, dus kunnen die verantwoordelijkheid niet overnemen (jouw resultaten zijn je eigen verantwoordelijkheid)
- Je zult dus zelf actief maatregelen moeten treffen, en dus ook kosten moeten dragen
- Sommige risico's kun je verzekeren (brand), ook collectief
- Voor informatierisico's/cybersecurity bestaan verzekeringen maar de ervaringen zijn niet overal positief. Het mbo onderzoek momenteel de mogelijkheden van risicopooling, waarbij iedereen bijdraagt aan de schade van een ander indien nodig.

Ben je lijnmanager?

Voor de lijnmanager spelen specifiek twee aandachtsgebieden in relatie tot informatiebeveiliging een rol:

- De **personeelsverantwoordelijkheid**. De lijnmanager is verantwoordelijk voor het handhaven van de personele beveiliging met eventuele ondersteuning door Personeelszaken.
- De **procesverantwoordelijkheid**. De lijnmanager is verantwoordelijk voor het uitvoeren van activiteiten in processen op basis van de beschreven inrichting ervan. De verantwoordelijkheid voor de naleving van specifieke beveiligingsaspecten hangt af van het soort proces. Binnen procesverantwoordelijkheid horen nog een aantal andere verantwoordelijkheden: budgetverantwoordelijkheid, IT verantwoordelijkheid (technisch) en IV-verantwoordelijkheid (vooral functioneel). Deze zijn sterk afhankelijk van hoe het mandaat binnen een organisatie belegd is.

Lijnmanager: personeelsverantwoordelijkheid

- Wordt er gewerkt met geheim te houden gegevens? Is er sprake van kwetsbaarheden binnen de functie, bijvoorbeeld omgang met geld, of bestaat de mogelijkheid om toegangsrechten toe te kennen, te wijzigen of in te trekken? Gelden voor uitzendkrachten en ander tijdelijk personeel dezelfde criteria bij indiensttreding als bij vaste medewerkers? De eisen die aan medewerkers worden gesteld bepalen de maatregelen die bij de personele beveiliging worden getroffen. De lijnmanager weet welke rol de medewerker binnen de organisatie vervult en welke risico's aan die rol zijn verbonden.

- Over het algemeen zal het personeelsbeleid generiek zijn beschreven en zullen algemene afspraken over maatregelen bij aanstelling, functiewijziging en vertrek van medewerkers zijn vastgelegd. De lijnmanager moet in overleg met de afdeling Personeelszaken en de CISO bepalen aan welke specifieke beveiligingseisen medewerkers eventueel aanvullend moeten voldoen, bijvoorbeeld in het kader van **kennisveiligheid**.

Lijnmanager: procesverantwoordelijkheid

De lijnmanager is verantwoordelijk voor de uitvoering van maatregelen.

- *organisatorische* maatregelen, zoals het opstellen van informatiebeveiligingsbeleid en het benoemen van functies en verantwoordelijkheden, het inrichten van een incidentenregistratie en een meldingsprocedure, het opstellen van een calamiteitenplan en dergelijke. Organisatorische maatregelen hebben betrekking op de hele organisatie. Maatregelen op dit niveau moeten door de lijnmanager worden geaccepteerd en kunnen door hem niet buiten toepassing worden gelaten.
- *technische maatregelen*, waarbij geautomatiseerde controles worden aangebracht om de betrouwbaarheid, integriteit en vertrouwelijkheid van de gegevens conform een afgesproken beveiligingsniveau te beschermen. Daarnaast kan gedacht worden aan maatregelen om de bedrijfscontinuïteit te garanderen (back-up en uitwijkvoorzieningen). De lijnmanager bepaalt welk beschermingsniveau passend is op basis van de betrouwbaarheidseisen van het informatiesysteem. Uitvoering van deze maatregelen ligt veelal bij de ICT-afdeling of een externe dienstenaanbieder.
- *procedurele* maatregelen, die bestaan uit de inrichting van het bedrijfsproces op een zodanige manier dat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie wordt gewaarborgd. De lijnmanager is onder andere verantwoordelijk voor het toepassen van een adequate functiescheiding om de betrouwbaarheidseisen te waarborgen.
- *fysieke* maatregelen, zoals de opslag van dossiers in een daartoe aangewezen bewaarplaats en niet langer dan gedurende een door de lijnmanager of op basis van regelgeving bepaalde termijn. Afspraken over het registreren en begeleiden van bezoekers naar beperkt toegankelijke ruimten zijn ook een voorbeeld van een fysieke maatregel die in overleg met de lijnmanager wordt genomen.

Ook als de uitvoering van maatregelen in relatie tot het informatiesysteem elders ligt, moet de lijnmanager op de hoogte zijn welke maatregelen getroffen zijn, maar ook speciaal welke niet getroffen zijn. Uiteindelijk bepaalt de lijnmanager welke (rest)risico's geaccepteerd worden na de implementatie van alle bovenstaande maatregelen, en bewaakt de lijnmanager ook welke maatregelen nog geïmplementeerd moeten worden of voor welke maatregelen tijdelijke andere maatregelen genomen worden.

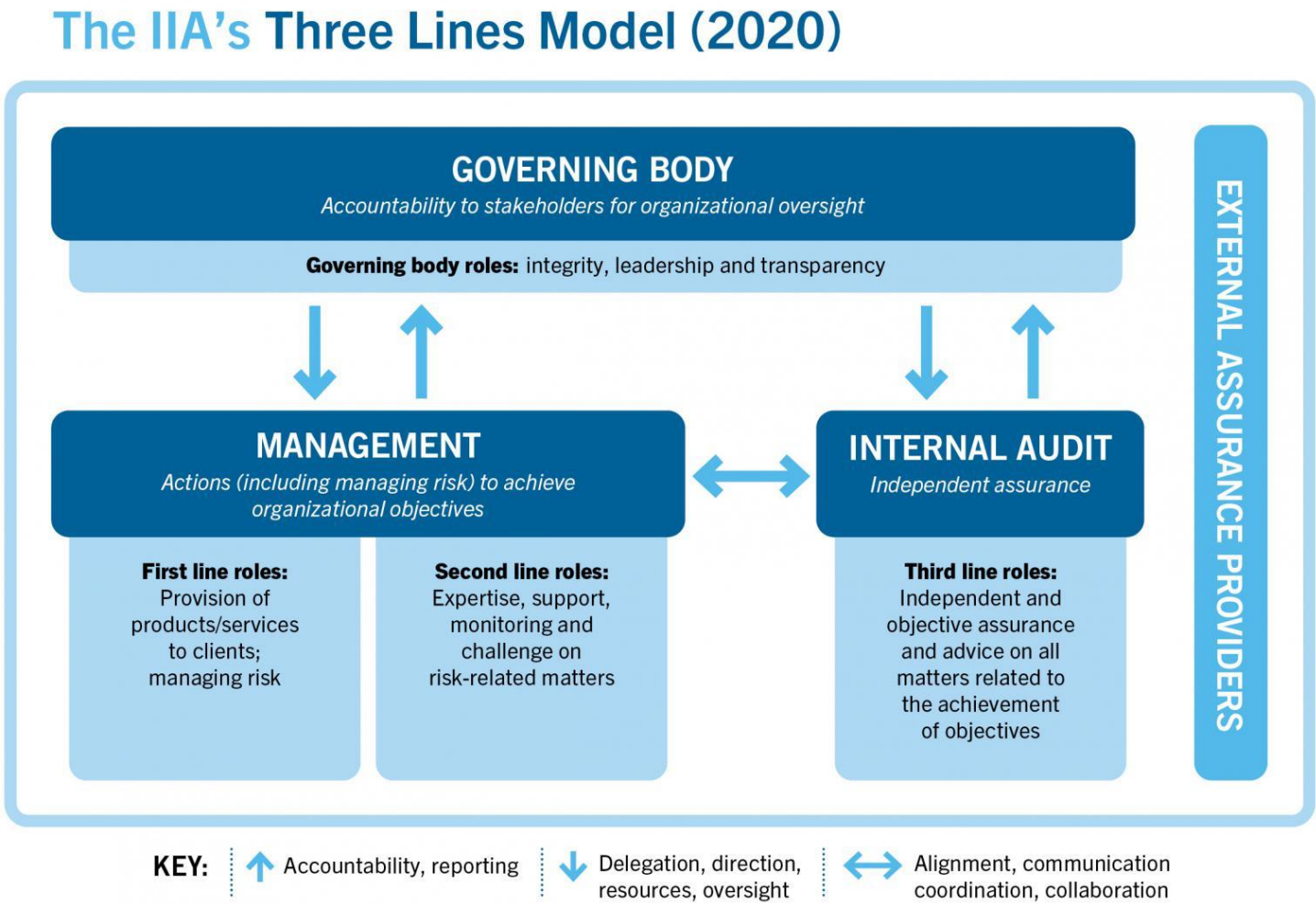
Lijnmanager: voorbeeldgedrag

- De lijnmanager heeft een belangrijke rol om onveilig gedrag van medewerkers te voorkomen. Dat uit zich in toezicht op naleving van regels en richtlijnen door medewerkers en het bevorderen van het beveiligingsbewustzijn van medewerkers. Maatregelen om het bewustzijn bij medewerkers te vergroten zijn bijvoorbeeld het hanteren van een gedragscode, waarin regels zijn vastgelegd voor een verantwoorde omgang met informatie en het benoemen van informatiebeveiliging als onderwerp tijdens werkoverleg en in functionerings- en beoordelingsgesprekken.
- Het toezicht op naleving van afspraken door medewerkers heeft uiteraard alleen zin wanneer de lijnmanager zelf voorbeeldgedrag vertoont en in zijn dagelijkse werkzaamheden tot uitdrukking brengt dat informatiebeveiliging serieus wordt genomen. De afspraken die voor medewerkers gelden, gelden onverkort ook voor de lijnmanager.

Wat doet een risicomanager dan nog?

- Een risicomanager of een CISO:
  - *doet* niets met jouw risico's
  - helpt en adviseert jou om risico's te herkennen, begrijpen, beoordelen en te mitigeren, maar beslissingen en mitigerende maatregelen neem je helemaal zelf (tenzij er collectief iets kan, bijv. via ict afdeling)
  - coordineert de voortgang, effectiviteit, en status van jouw risicobeheersing en de samenhang met andere risico's
  - ondersteunt bestuurders en directeuren om de balans te houden tussen prioriteiten en diverse thema's door onafhankelijk advies te geven

3 lines model, wie zit waar?



5. Hoe oordeel je over een risico?

Oordelen over een risico

- je moet het risico eerst bedenken
- dan een inschatting geven van de kans en ernst
- vervolgens op basis van je risicobereidheid beslissen wat je gaat doen

Hoe ‘verzin’ je mogelijke risico’s?

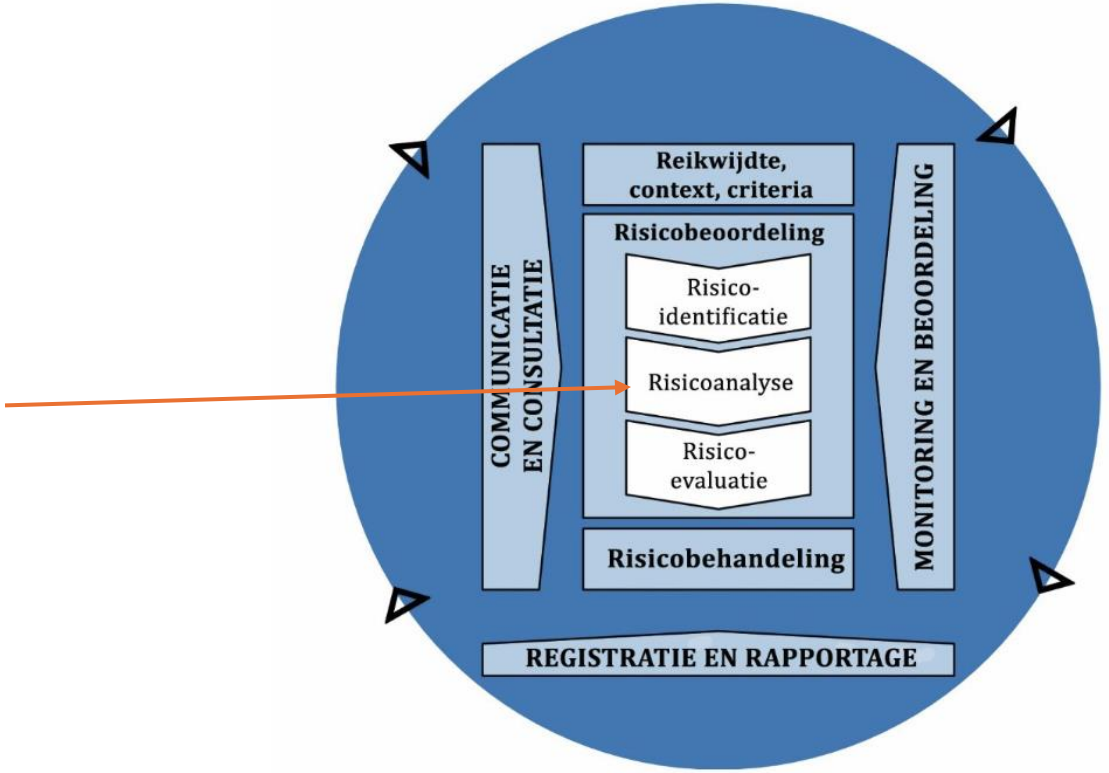
- Welke onzekere gebeurtenissen of situaties kunnen je doel beinvloeden? Wat zijn daarvan de mogelijke oorzaken? Wat kunnen de effecten op je doel zijn?
- Je kunt hier zelf over nadenken, in de gesprek met de CISO of in groepsverband met, bijvoorbeeld, je team.
- Gebruik hiervoor technieken van toekomstverkenners of futuring.
- Heb je echt geen inspiratie, begin dan eens met bekende situaties of lees dreigingsbeelden van SURF, de NCTV of ENISA. Maar let op: dreigingsbeelden beschrijven meestal risico’s die we al kennen, en zijn dus vaak geen risico’s meer omdat ze niet onzeker zijn.

Is jouw organisatie meer van visie A (slide 16)?

https://sec.surf.nl/toolkit-risicobeoordeling/

Risico-analyse

- Hoe schat je de kans in dat een risico optreedt?
- Wat zijn de gevolgen als het risico optreedt?



Inschatten kans van optreden

- Dit kun je zo ingewikkeld maken als je zelf leuk vindt:
  - kwalitatief: laag-midden-hoog, groen-oranje-rood
  - kwantitief: 1x per maand/jaar/eeuw of .05%
- Je kunt het inschatten met een groep in een stemronde en dan een gemiddelde nemen, of je kunt een gestructureerd proces als de Delphi methode gebruiken.

Kans

- We splitsen kans vaak uit in een formule: dreiging * kwetsbaarheid (oftewel: hoe weerbaar ben je)
- Een sterke dreiging komt van geavanceerde actoren met veel beschikbare middelen om cyberaanvallen uit te voeren

		Weerbaarheid		
		Mens, proces, en/of technologie is kwetsbaar voor de dreiging.	Gematigd kwetsbaar	Beperkt kwetsbaar
Dreiging	Actor heeft sterke intentie. Actor heeft capaciteit beschikbaar. Het is al eerder waargenomen.	5 zeer waarschijnlijk	4 waarschijnlijk	3 mogelijk
	Gematigde dreiging	4 Waarschijnlijk	3 mogelijk	2 onwaarschijnlijk
	Beperkte dreiging	3 mogelijk	2 onwaarschijnlijk	1 zeer onwaarschijnlijk

Impact

1	2	3	4	5	
minimaal	**significant**	**serieus**	**kritiek**	**catastrofaal**	***schaal volgens ISO 27005***
Verwaarloosbaar. Er wordt niet of nauwelijks hinder ondervonden door de gebeurtenis en het kan volledig hersteld worden met beperkte middelen.	Het geraakte system of proces functioneert tijdelijk niet naar behoren door uitval van beschikbaarheid, integriteit en/of vertrouwelijkheid. De consequenties voor de organisatie zijn zwaar, maar te overkomen	Het geraakte systeem of proces functioneert niet meer en moet hersteld worden, met flinke reputatieschade en financiële en/of juridische gevolgen. En/of heeft het tot onveilige situaties geleid.	De impact is groot. De geraakte organisatie functioneert niet meer, en zal er niet of nauwelijks meer van kunnen herstellen. Ook diens partners worden dus geraakt. En/of het heeft zwaar letsel tot gevolg.	De impact is direct en immens. Alle aangesloten onderwijsinstellingen kampen met serieuze problemen en dat raakt ook nationale belangen. En/of het heeft dood tot gevolg.	

Gedoe over heatmaps

- Lovers
  - Makkelijk in gebruik
  - Communiceert fijn naar mensen die er niet zoveel van weten
  - Handig om prioriteiten te stellen
- Haters
  - Managers gaat sturen op ‘groen’ bereiken ipv onzekerheden accepteren
  - De schalen (laag, midden, hoog) zijn vaak vaag beschreven
  - De heatmap wordt vaak een doel op zich in plaats van een startpunt voor een gesprek
  - Wiskundig gezien klopt er geen hout van

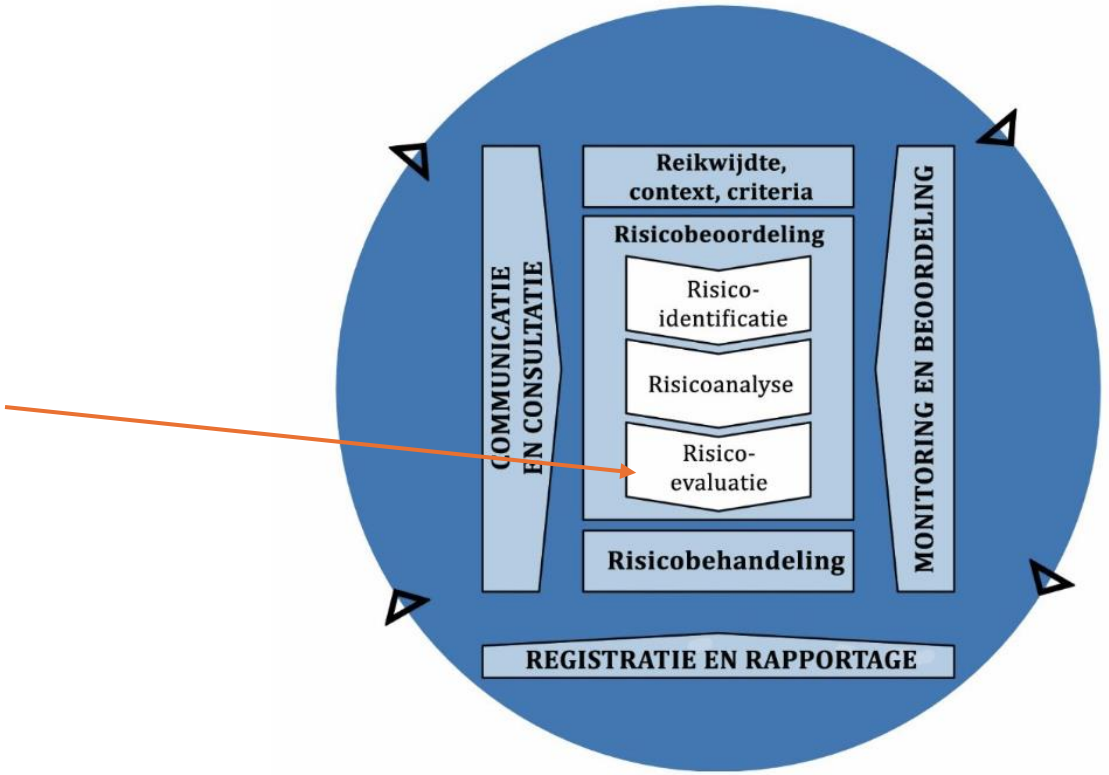
Gebruik ze gerust, maar maak ze niet leidend voor je beslissingen.

6. Wat doe je met een risico?

Risico-evaluatie

- Wat ga je doen?

- Opties voor risicobehandeling
  - Vermijden
  - Aanvaarden
  - Waarschijnlijkheid verminderen
  - Veranderen gevolgen
  - Delen van risico



Risicobereidheid

- De branchecode goed bestuur van UNL vereist dat universiteiten in hun jaarverslag de risicobereidheid beschrijven (9.2 ii).
- Heeft jouw instelling de risicobereidheid niet beschreven? Dan hoef je daar niet op te wachten. Je weet zelf meestal wel hoeveel risico jijzelf bereid bent (of gemandeerd bent) te nemen voor jouw doelen. En ja, dat is soms best spannend om die beslissing te nemen.
- Maak de keuzes en onderbouw ze.

Meer lezen?

Aanbevolen bronnen

- https://sec.surf.nl/risicomanagement/
- https://wiki.surfnet.nl/pages/viewpage.action?spaceKey=IVHO&title=Kennisdossier+risicomanagement