Samen aanjagen van vernieuwing

Risicomanagement: de do's en don'ts

Ervaringen met doelgericht integraal risicomanagement in de sector onderwijs en onderzoek

Auteur(s): Dit document is tot stand gekomen door interviews met en samenwerking tussen:

Hogeschool Utrecht
TU Delft – Hans Suijkerbuijk (ERM functionaris)
KNAW – Ferry Korving (Risicomanager)
Fontys Hogeschool – Hub Gerats (CISO)
HogeschoolWindesheim
Hanze Hogeschool
Graafschap College - Rob Gerritsen (CISO)
Universiteit Tilburg
Hogeschool Rotterdam – Marc Kouwenhoven (Risicomanager)
Radboud Universiteit

Redactie:
SURF – Nicole van Deursen, Jeroen Schuuring

Tekstredactie:
Aad van de Wijngaart

Versie: 1.0
Datum: 26 mei 2025

Inhoudsopgave

1 Inleiding

Risicomanagement is een bekend begrip in de sector onderwijs en onderzoek. We kennen de term uit de branchecodes voor goed bestuur, het onderwerp is vaste prik in het jaarverslag en het wordt steeds vaker genoemd als thema bij cybersecurity. Daarnaast bouwen we al jarenlang aan integrale veiligheid en staat de bewaking van publieke waarden centraal binnen de sector. Toch blijft risicomanagement voor velen iets ongrijpbaars. Wat houdt het nu echt in en waar moet je beginnen?

Veel risicokeuzes die we maken gaan bijna onbewust. Daarbij moeten we continu en wendbaar omgaan met nieuwe situaties en onzekerheden. We moeten prioriteiten stellen en knopen doorhakken in een wereld die verandert. Risicomanagement brengt structuur in die denkprocessen, op basis van gedeelde doelstellingen en zorgvuldig geanalyseerde collectieve ervaring tussen verschillende disciplines.

Daardoor is risicomanagement ook een vaardigheid die helpt bij het nastreven van je zakelijke doelstellingen, door prioriteiten te stellen en schaarse capaciteit zo effectief mogelijk in te zetten: namelijk daar waar die capaciteit het hardste nodig is of de meeste impact kan hebben. Goed ingebed risicomanagement stimuleert:

- het samenwerken aan doelen over afdelings- en organisatiegrenzen heen;
- het leervermogen van de organisatie, zodat deze zich niet meerdere malen aan dezelfde steen stoot;
- het aanpassingsvermogen van de organisatie, om goed te blijven functioneren onder veranderende omstandigheden.

Als instellingen aan de slag gaan met risicomanagement, moeten ze hun doelstellingen, keuzes en denkprocessen expliciet maken en vastleggen in woorden. Dat vergt niet alleen motivatie, maar ook hulp van experts zoals controllers, risicomanagers, integrale-veiligheidsmanagers, privacy officers of CISO's. Deze risicofunctionarissen combineren vaak de rollen van aanjager, dirigent en duizendpoot voor alles wat komt kijken bij risicomanagement. Dat vraagt veel van hun vaardigheden én van hun uithoudingsvermogen.

Dit document is geschreven voor en door precies dit soort functionarissen. De auteurs zijn werkzaam bij verschillende onderwijs- en onderzoeksinstellingen. Het doel is om ervaringen te delen die zij hebben opgedaan op hun weg naar integraal risicomanagement, waarbij de samenwerking tussen die functionarissen centraal staat bij het streven om instellingen te helpen hun doelen te bereiken.

In dit document vind je dus (bijna) geen inhoudelijke adviezen, zoals wat het beste model is of wat er in beleidsstukken moet staan[1]. Wel delen we welke lessen er zijn geleerd uit successen en mislukkingen: de do's en de don'ts staan centraal. Wat kun je doen om je slagingskans te vergroten? En welke keuzes staan garant voor frustratie? Wij wensen de lezers goede gesprekken toe over doelstellingen, kansen en keuzes.

[1] Voor kaders, richtlijnen, beleidstemplates en andere instrumenten verwijzen we je naar de expertisecentra Security en Privacy van SURF en het platform Integrale Veiligheid Hoger Onderwijs.

2 Wat zegt u?

In discussies over risico's en risicomanagement spreken mensen vaak vanuit verschillende definities van vaktermen. Daarom is het belangrijk om daar afspraken over te maken. In dit document bedoelen we met de termen risico en integraal risicomanagement het volgende.

Een risico is het effect van onzekerheid op afgesproken doelen[2]. De nadruk ligt hier op het effect van onvolledige kennis (onzekerheid) van omstandigheden, inclusief gebeurtenissen, op de doelstellingen van een organisatie. Hoe meer je weet over de mogelijke omstandigheden en hoe je daar doorheen moet navigeren, hoe minder problematisch een onzekerheid zal zijn.

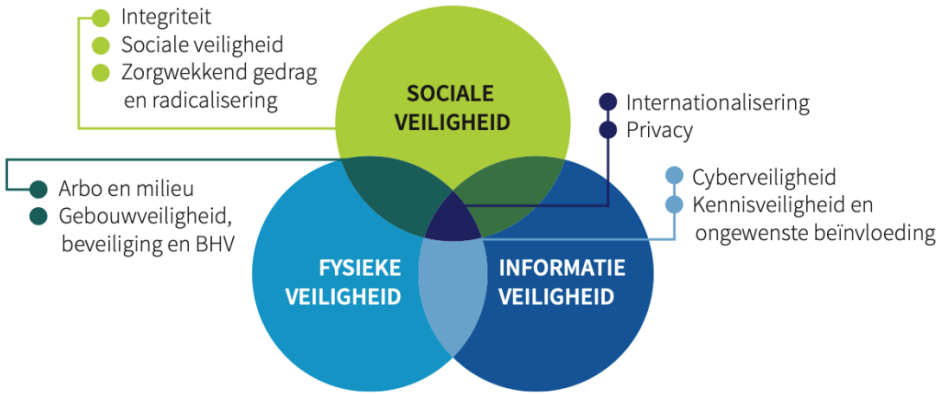
In aanvulling op de definitie van risico hanteren we – voor dit document – een praktische tweedeling in typen risico's.

- Strategische risico's

Door het bestuur onderkende risico's, gerelateerd aan de strategie en keuzes van de instelling. Het bestuur wordt in de omgang hiermee doorgaans ondersteund door een risicomanager of controller.

- Thematische risico's

Dit zijn de risico's die betrekking hebben op specifieke thema's zoals financiën, ethiek of bepaalde projecten, maar ook op de thema's binnen integrale veiligheid, zoals fysieke, sociale en informatieveiligheid[3]. De bestuurders, risicomanagers of controllers worden voor gesprekken over deze thema's vaak ondersteund door specialistische adviseurs.



In de praktijk is het nog niet overal gebruikelijk dat processen rondom strategische en thematische risico's soepel op elkaar aansluiten. Veel instellingen zetten momenteel stappen richting integraal risicomanagement (IRM), waarbij het gaat om de relatie tussen instellingsdoelen en het inzicht in verschillende strategische en thematische risicogebieden in onderlinge samenhang. Er bestaat er geen formule, receptenboek of stappenplan om dat te bereiken. Dit document hoopt een bijdrage te leveren aan de kennisopbouw voor IRM.

[2] *ISO 31000:2018 Risk Management – Guidelines*.

[3] https://integraalveilig-ho.nl

3 Als je aan het begin staat

3.1 Beginnen bij ‘start’

Voor het ‘begin’ van risicomanagement zijn meerdere startpunten denkbaar. Bij de instellingen die meewerkten aan dit document bestaan de volgende varianten:

- Van oudsher is risicomanagement onderdeel van de bedrijfsvoering en daar richt men zich meestal op financiële en strategische risico’s.
- De raad van toezicht vraagt om risicorapportages en doet zelfs de suggestie om een bepaald framework (bijvoorbeeld COSO ERM[4] of ISO 31000[5]) te implementeren. Het CvB stelt dan een (enterprise/integraal) risicomanager aan.
- Een bestuurder heeft ervaring met risicomanagement en stuurt op beleid en dialoog over risico’s.
- De CISO of IT-risicomanager binnen de ict-afdeling is de aanjager voor het maken van een risicomanagementbeleid en -processen. Doel is prioriteiten te kunnen stellen en te voldoen aan de sectorale compliance-eisen voor informatiebeveiliging en privacy.
- De integrale-veiligheidsafdeling start de dialogen die directies bewust maken en adviseert over de risico’s binnen diverse veiligheidsthema’s.
- Vanuit concern control, kwaliteitszorg of procesmanagement worden de eerste stappen gezet om risico’s binnen de processen te beschrijven.

Doordat verschillende startpunten mogelijk zijn, is er niet zoiets als een one-size-fits-all-stappenplan dat bij elke instelling zal passen. Meestal zijn er diverse parallelle initiatieven gaande op verschillende plekken in de instelling, die in meerdere of mindere mate met elkaar samenwerken. Als je aan het begin staat van risicomanagement, waar dan ook binnen de organisatie, dan vind je hieronder de lessen die de auteurs je graag meegeven.

[4] https://www.coso.org/guidance-erm

[5] https://www.iso.org/standard/65694.html

Do's

1. Maak de doelstellingen van de organisatie het startpunt van risicomanagement. Vaak zal dan blijken dat doelstellingen te weinig concreet zijn geformuleerd. Dat alleen al is winst voor de bedrijfsvoering, want vage doelen leiden tot onzekerheid
2. Maak inzichtelijk dat risicomanagement nu al een logisch onderdeel is van bestuur en management, zij het vaak nog impliciet. Het is dus niets nieuws, maar het verdient wel een explicietere plaats op de bestuurlijke agenda.
3. Zorg dat je je narratief helder hebt (het waarom, hoe en wat).
4. Ga gesprekken aan met bestuurders van alle organisatieonderdelen om te leren hoe zij kijken naar risicomanagement.
5. Gebruik begrijpelijke taal met herkenbare voorbeelden.
6. Als het begrip er eenmaal is, kan gewerkt worden aan commitment. Dat kan wellicht worden vastgelegd in een besluit (charter, terms of reference, plan van aanpak).
7. Start waar energie zit, bijvoorbeeld bij een bepaalde faculteit/afdeling waar je steun vindt.
8. Houd je plannen klein. Het veranderingsproces gaat heel traag.
9. Vorm een vitale coalitie met andere risicofunctionarissen, zowel binnen als buiten je eigen organisatie.
10. Wees ‘agile’: pas je plannen aan als iets niet werkt.

Don'ts

1. Bij integraal risicomanagement (IRM) zijn het bestuur en management van de organisatie leidend. Laat deze laag dus niet in de afwachtende stand staan.
2. Proberen om alle mogelijke risico's te identificeren. Begin klein en bekijk de risico’s per onderdeel, zoals informatieveiligheid.
3. De indruk geven dat IRM de risico’s gaat wegnemen.
4. Werk overnemen van risico-eigenaren die vanuit hun positie verantwoordelijkheid moeten nemen.
5. Opgeven als je de enige roepende in de woestijn bent.

3.2 Er ontstaat beweging

3.2.1 Sleutelfiguren betrekken

Samenwerken met mensen in andere risicofuncties is efficiënt en waardevol. Het voorkomt silovorming en samen sta je ook sterker. Welke functionarissen je betrekt bij de gesprekken in de beginfase, hangt af van waar je startpunt is. Als je bijvoorbeeld vanuit het CvB opdracht hebt gekregen tot IRM, dan begin je vanaf een ander startpunt dan wanneer je vanuit de ict-afdeling of integrale veiligheid start. Sommige instellingen hebben een afdeling waarin verschillende risicofunctionarissen bij elkaar zitten, dicht bij de bestuurslaag van de instelling. Daar vind je dan, onder een directeur, de CISO, controllers, risicomanager en integrale-veiligheidsmanager. In andere instellingen zijn relevante functies in verschillende afdelingen gepositioneerd en kost het in het begin iets meer moeite om elkaar te vinden. De ervaringen van de auteurs hebben geleid tot de volgende tips.

Do's

1. Breng in kaart wat de instelling allemaal al heeft.
2. Bouw expertise op langs de lijn van risicofuncties die vanwege wet- of regelgeving al aanwezig zijn: FG, CISO, privacy officer, interne audit.
3. Geef duidelijk aan waar de verantwoordelijkheid ligt voor het anticiperen op risico's (eerste lijn).
4. Voer risicodialogen met de eerste lijn samen met andere risicofuncties. Een voorbeeld: bij dialogen over cybersecurity kan de CISO de inhoudelijke voorbeelden geven en een business controller/enterprise risk manager uitleggen hoe de cyberrisico's zich verhouden tot de strategische risico's.
5. Train en adviseer de eerste lijn in risicobeoordeling.
6. Hou taal en de betekenis van risico's zo veel mogelijk gelijk door definities vast te leggen en consistent te hanteren. Dit bevordert het onderling begrip over wat bijvoorbeeld termen als governance-risicos, kwaliteitsrisico's en informatierisico's inhouden.

Don'ts

6. Je beperken tot de strategische laag, al is die wellicht wel een punt om te starten met IRM.
7. Risicomanagement beperken tot de eigen organisatie. We opereren in een brede context van onderlinge afhankelijkheid. Zoek dus samenwerking met risicofunctionarissen bij onderwijs- en onderzoekspartners, gemeente, facilitaire partners, de studenteninschrijfketen, leveranciers, enzovoort. Vergeet ook bonden, actievoerders en medezeggenschapsraden niet.

3.2.2 Vraag creëert vaart

De strategie van de organisatie en de publieke waarden vragen om risicomanagement. Je doet niet aan risicomanagement omdat de branchecodes of toezichthouders het vragen: het is gewoon nodig voor de structuur en robuustheid van de organisatie.

Zakelijke doelen brengen altijd onzekerheden met zich mee. Net als in je eigen huishouden denk je na over eventuele risico's. Als een deel van die onzekerheid kan worden weggenomen, geeft dat gemoedsrust en vertrouwen in de slagkracht van de organisatie en de ketens waarin de organisatie opereert. Ook het sectoraal en maatschappelijk belang wordt ermee gediend.

De meeste instellingen merken wel dat risicomanagement veel geduld vergt. Tien jaar is geen onrealistische termijn om nieuwe manieren van werken en denken in te laten slijten. Bovendien kan er vertraging ontstaan door nieuwe visies op risicomanagement, reorganisaties of personele wisselingen onder de sleutelfiguren.

Heeft jouw instelling nog wat hulp nodig om de meerwaarde van risicomanagement in te zien? De volgende do's en don'ts kunnen je wellicht helpen de waardering voor risicomanagement te vergroten en vaart te maken met de implementatie.

Do's

1. Begín gewoon. Bijvoorbeeld door een training te combineren met risicoanalyse. Dan gaat het risicomanagement leven.
2. Maak een vliegende start met in-companytraining voor een grote groep. Onderwerpen: hoe praat je over risico's, welke vaste structuur kun je kiezen voor risicomanagement. Zo gaan de neuzen dezelfde kant op staan.
3. Doe meerdere dingen parallel en zie wat werkt.
4. Oefen het voeren van risicodialogen.
5. Stel kernvragen aan bestuurders en managers: 'Heeft het bestuur/management een goed beeld van hoe het ervoor staat met risicomanagement en de bijbehorende compliance?' en 'Waar maak je je zorgen over?'
6. Maak duidelijk dat IRM een meerwaarde heeft in de bedrijfsprocessen, bestuur en management. Geef voorbeelden van hoe de reguliere bedrijfsvoering hier baat bij heeft. Maak concreet hoe je kunt anticiperen op risico's, verrassingen kunt vermijden en wellicht kosten kunt besparen.
7. Blijf benadrukken dat risicomanagement al lang een onderdeel is van het dagelijks handelen van managers en bestuurders, maar vaak niet expliciet en systematisch. IRM zorgt dat dit wél structureel gebeurt. Probeer daarbij zoveel mogelijk aan te haken bij herkenbare processen. Zo worden de zorgpunten en de beheersing daarvan beter aangepakt binnen de bestuurlijke dialoog en besluitvorming.
8. Laat zien hoe IRM antwoord geeft op de vraag of je voldoende bent voorbereid op zaken die het behalen van je doelen bemoeilijken. Strategische doelen vereisen vaak een andere inrichting of aanpak van je bedrijfsprocessen.
9. Laat zien dat anticiperen op risico's leidt tot overzicht en gemoedsrust: 'Hoe hadden we in voorbereiding op situatie X kunnen anticiperen op onzekerheden?'
10. Praat met studenten over risicomanagement.

Don'ts

1. Proberen om alle risico's te identificeren. Leg uit dat we leven in een wereld die zich kenmerkt door verandering en onzekerheid. Daarom moeten we veerkracht ontwikkelen. Omgaan met onzekerheid is de essentie van risicomanagement.
2. Jargon van risicomanagement gebruiken. Probeer in plaats daarvan begrippen uit de leefwereld te gebruiken. Bijvoorbeeld: ‘Waar maak je je zorgen over?’ Of: ‘Wat zijn de onzekerheden?’
3. Gebruik van ingewikkelde theoretische modellen in je promotiecampagne. Zeggen dat de toezichthouder risicomanagement vereist, of dat het een onderdeel is van ‘goed bestuur’. Dit betreft alleen de borging, niet de aanpak.

3.3 Instrumentarium kiezen

Als je risicomanagement op een instrumentele manier benadert, dan moet er veel gebeuren: de keuze van een framework (COSO ERM of ISO 31000), het inrichten van governance-structuren, beleidsdocumenten, methoden en technieken voor risico-analyse, registers, tooling en rapportageprocessen. In sommige organisaties werkt een instrumenteel kader prettig vanaf het begin, bij andere organisaties moet dat in kleine stapjes worden opgebouwd om de balans te vinden tussen autonomie en controle. De instellingen die meewerkten aan dit document hebben elk een ander soort instrumentarium, maar er zijn wel rode draden in hun ervaringen.

Do's

1. Verzamel wat er al is en sluit daarbij aan. Bijvoorbeeld een kwaliteitszorgsysteem of bestaande en (h)erkende controls binnen de P&C-cyclus.
2. Hanteer formats en rapportagetools die aansluiten bij de actuele situatie van de instelling of het programma. Of, liever nog: maak ze zelf. Bijvoorbeeld eerst gewoon beginnen met een risicoregister in Excel. In een volgende fase kun je dan een risicomanagement tool aanschaffen.
3. Gebruik in registers de bekende kernelementen: onderscheid tussen strategie, (bestuurlijke) werkafspraken en de reguliere bedrijfsvoering; risico's; beheersmaatregelen; eigenaarschap, rest-risico's & risk appetite. En maak duidelijk waar je nog lege vakken hebt. Voorkom daarbij stress voor jezelf: eigenaarschap van die lege vakken ligt bij de eerste lijn, niet bij de risicofunctionaris.
4. Definieer een standaardformaat voor het formuleren van een risico, bijvoorbeeld BowTie of scenario's.
5. Houd de technische informatie over registers voor je, want mensen haken snel af bij 'lijstjes'. Blijf faciliterend.
6. Evalueer wat je doet en leer ervan: is het effectief? Draagt het bij aan de doelen?
7. Zorg dat het CvB het beleid heeft goedgekeurd: dan kun je mensen gemakkelijker uitleggen dat ze het echt moeten uitvoeren.

Don'ts

1. Risicomanagement alleen vanuit een tool introduceren en dat over de schutting gooien.
2. Je laten verleiden tot discussies over de systematiek. Houd het doel voor ogen; de aard van de aanpak is volgend.
3. Van IRM een losstaand proces maken. Verweef het met bestaande cycli: als er strategische sessies zijn, heb het dan ook over risico's; als afdelingen hun (jaar)plannen maken, vraag ze dan ook om de risico's en heb daarna een integrale afstemming over de doelen en risico's.
4. Een risicohouding vastleggen en risk appetite ingewikkeld maken. Maak eenvoudig duidelijk waar de organisatie risico's accepteert en waar niet.
5. De bestuurders overvoeren: als je het CvB een lijst van 150 risico's of 10 individuele themarapportages stuurt, ben je verkeerd bezig.

4 Als je al een tijdje bezig bent

4.1 Verandering als constante factor

Er komt een punt waarop je voorstellen gaat doen voor een organisatiestructuur van het risicomanagement. Streef naar een flexibele organisatie, ingericht op veranderingen in de samenleving. Zorg daarnaast voor een duidelijke scheiding tussen eerste en tweede lijn, waarbij ook de rapportagelijnen gescheiden zijn tot aan het hoogste bestuursniveau van de organisatie.

De eerste lijn is immers de plek waar de doelen van de organisatie bereikt moeten worden. Risicomanagement moet deze lijn helpen om bewuste keuzes te maken, en eigenaarschap maakt dat transparant. De tweede lijn is licht, in de basis ervaren en ingericht op drie taken: overzicht houden, uitdagen en adviseren.

Evalueer daarnaast elke activiteit en maatregel op effectiviteit bij het bereiken van de doelen; stap zo snel mogelijk af van zaken die niet productief zijn. Het is wellicht lastig, maar uiteindelijk zullen we eraan moeten wennen dat de enige constante in een effectieve organisatie – effectief in het behalen van doelen als excellent onderzoek of onderwijs – verandering is. Want een organisatie staat niet op zichzelf, maar is onderdeel van een veranderende maatschappij. Om relevant te blijven moet ze zich steeds aanpassen.

Do's

1. Omhels verandering, want je kunt het niet vermijden en zonder verandering is er geen verbetering.
2. Promoot de strikte scheiding tussen eerste en tweede lijn. Ze hebben verschillende rollen, en die moeten afzonderlijk beoordeeld kunnen worden.
3. Laat de controle soms even los. De organisatie moet eigenaarschap ontwikkelen.
4. Steun elk (klein) initiatief en vier elk klein succes. Mensen hebben behoefte aan beloning. Jijzelf ook.
5. Durf keuzes te maken, want anders kom je nergens.
6. Blijf communiceren met de organisatie, in elke vorm die past binnen die organisatie.

Don'ts

1. Alles zeker willen weten. Risicomanagement is het omgaan met onzekerheden.
2. Naar volledigheid streven: je zult nooit alle risico’s in kaart kunnen brengen.
3. Benadrukken wat er allemaal niet goed gaat. Je wilt de mensen niet ontmoedigen.
4. Organiseren van overleggen met besluitnemers als daarin niets te besluiten valt.

4.1.1 Organisatiecultuur

De cultuur in een organisatie is voor het slagen van risicomanagement van groot belang. Fouten, incidenten, onverwachte gebeurtenissen – ze zijn de beste bron om als organisatie te begrijpen waar je nog tekortschiet in risicobeheersing.

Een omgeving waarin mag worden geleerd van fouten is dan ook een belangrijke factor bij risicomanagement. Alles wat we doen is mensenwerk, dus fouten worden gemaakt. Zorg dat die fouten niet worden verhuld maar dat ze worden beschouwd, gevierd zelfs, als leermomenten. Het zal de bereidheid vergroten om eigenaarschap te nemen van risico's en gebleken kwetsbaarheden te verhelpen. Is de kans op fouten groot maar de impact relatief klein, zoals in testomgevingen? Maak die fouten dan gerust. Maar zorg wel voor een goede vastlegging.

Risicomanagement helpt om het belang van incidenten of bevindingen te bepalen. Daarnaast biedt het handvatten om eigenaren aan te wijzen en middelen toe te kennen, zonder dat dit ervaren wordt als 'over de schutting gooien'.

Dit voorkomt een ander contraproductief cultuuraspect: de vaak gehanteerde, impliciete regel dat degene die een probleem signaleert het ook moet gaan oplossen. Uiteindelijk leidt die gewoonte ertoe dat medewerkers die de organisatie willen verbeteren hun bevindingen niet meer melden. Bijvoorbeeld omdat ze het al druk genoeg hebben met eerder benoemde problemen.

Do's

1. Identificeer de grootste risico's: degene die het voortbestaan van de organisatie bedreigen. En manage ze tot in detail.
2. Zorg voor voldoende ruimte om te testen en experimenteren, en moedig dit ook aan.
3. Definieer een standaardwijze van vastleggen van incidenten.
4. Hanteer een standaardwijze om risico's in te schatten en toe te wijzen.
5. Zorg dat leidinggevenden ook een goed voorbeeld geven.
6. Tot het tegendeel onweerlegbaar vaststaat, kun je het beste uitgaan van goede intenties wanneer mensen fouten hebben gemaakt.
7. Streef ernaar het risico van menselijke fouten met een grote impact zo klein mogelijk te maken, door voldoende training, opleiding, uitrusting en begeleiding; en door controle daarop.
8. En controleer of die controle effectief is. Pas als dit aantoonbaar het geval is, is er bij een fout mogelijk sprake van verwijtbaar gedrag. Zorg dat sancties voor iedereen duidelijk bedoeld zijn als preventieve maatregel.

4.2 Iedereen wordt een risicoleider

Risicomanagement biedt kansen om als organisatie op alle fronten beter te worden in het behalen van de doelen. Daarbij gaat het niet alleen om het voorkomen van ict- en andere verstoringen, maar bijvoorbeeld ook om het in de hand houden van werkdruk en sociale veiligheid, en het zichtbaar maken daarvan.

Uiteindelijk is risicomanagement niet iets wat een risicomanager doet. In een stabiele omgeving kan een traditionele risicomanager als staffunctionaris nuttig zijn om risicomodellen te administreren. Maar in de huidige VUCA[6]-wereld moet je streven naar een situatie waarin iedere medewerker, te beginnen met het bestuur en/of directie, risicoleider is[7]. Iedereen moet het belang daarvan inzien, blijvend begrijpen wat de voordelen zijn, en hiernaar handelen.

Streef dus naar persoonlijk risicoleiderschap van iedereen. Blijf echter realistisch en volg het tempo van je organisatie. Risico-eigenaarschap is een van de taaiste onderwerpen; communicatie en training zijn essentieel voor blijvend bewustzijn. De auteurs hebben vele lessen geleerd, die ze graag met je delen.

Do's

1. Gebruik risico-eigenaren die 'het snappen' als influencer. Laat ze eens een blog schrijven of betrek ze bij je presentaties. Het kan anderen over de streep trekken.
2. Vorm een vitale coalitie voor risicomanagement en organiseer samenspel.
3. Blijf risicomanagement eenvoudig en met een positieve insteek presenteren.
4. Speel in op actualiteit of op een voorbeeld uit de eigen praktijk. Zo kun je bijvoorbeeld een thema eruit lichten en daar eens wat dieper op ingaan.
5. Voer dialogen en werk daarbij aan een gemeenschappelijke risicotaal. Gebruik die termen en definities ook consistent.
6. Train de eerste lijn in risicotaal en risicobeoordeling.

Don'ts

1. Negeren van weerstand: ga de discussie aan.
2. Te veel jargon gebruiken. Dat maakt de doelstellingen namelijk abstract en daardoor minder relevant in de ogen van medewerkers.
3. Doen alsof de lastige onderwerpen niet bestaan: anderen mogen ook best weten waar het nu echt om gaat.
4. Je boodschap brengen met angstaanjagende kreten als 'hack',' datadiefstal', studentenaantallen of 'bezuinigingen'. Risico's zijn scenario's: het gaat dus om het hele verhaal van doel, dreiging, onzekerheden, zwakke plekken en impact.

[6] VUCA staat voor Volatile, Uncertain, Complex & Ambiguous. Lees hier meer: https://en.wikipedia.org/wiki/VUCA

[7] Van Staveren, M. (2018). *Risicoleiderschap.* Management impact.

4.3 Instrumentarium groeit mee

In de loop der tijd komt er steeds meer structuur en inzicht en ook steeds meer informatie om te documenteren. Het instrumentarium zal mee moeten groeien. Hoe tijdrovend en vervelend het ook kan zijn, in een organisatie waar taken door meer dan één persoon worden uitgevoerd zijn goede communicatie en transparantie net zo belangrijk als de inhoud van het werk zelf.

En hoe groter de organisatie, hoe meer inspanningen geleverd moeten worden om elkaar effectief te informeren. Standaardisatie in procesbeschrijvingen, evaluatie- controlemomenten – doen we nog het juiste, op de juiste manier, en doen we niets dubbel? – zijn daarom onmisbaar. Rapportage daarover eveneens.

In deze fase wordt datakwaliteit ook belangrijker. In het begin is incomplete, kwalitatieve data goed genoeg. Het is immers beter dan helemaal niets te registreren[8]. Wanneer registraties van gebeurtenissen, bevindingen en rapportages beter worden, zijn er betrouwbare trends te ontdekken. Toe- of afnames van incidenten of bevindingen met een hoge impact worden zichtbaar. Maar bijvoorbeeld ook trends die aangeven of de cultuur in de gewenste richting beweegt: het nemen van eigenaarschap of het (correct) registreren van incidenten per divisie of afdeling. Hierdoor kan gericht gecommuniceerd en getraind worden.

Het uiteindelijke doel van rapportage is het geven van inzicht aan belanghebbenden – collega's, bestuurders – zodat op basis daarvan besluiten genomen kunnen worden en activiteiten kunnen worden opgestart of bijgestuurd. De rapportages zouden dat doel moeten faciliteren.

[8] Hubbard, D.W. (2014). *How to measure anything: Finding the value of intangibles in business* (3rd ed.). Wiley.

Do's

1. Laat het risicoregister ondersteunend zijn, passend bij wat werkt.
2. Zorg dat risico's en compliance op elkaar aansluiten.
3. Geef voorbeelden van hoe je in jouw instelling een risico opschrijft. Minimaal bevat die beschrijving oorzaak en gevolg.
4. Houd integraal overzicht van de grootste risico's en laat de experts per thema rapporteren.
5. Kies de standaarden die het beste passen bij je organisatie: steek je licht op bij vergelijkbare organisaties en hanteer indien mogelijk dezelfde standaarden.
6. Probeer een balans te vinden: enerzijds wil je korte, inhoudsvolle en 'actionable' rapportages, anderzijds veel, maar korte (maximaal een half uur), goed voorbereide vergaderingen. Bij die sessies moeten de personen aanwezig zijn die een knoop kunnen doorhakken.
7. Investeer in voorbereiding en secretariaat. Hierdoor kan op elk niveau in de organisatie verantwoordelijkheid worden genomen. Overigens kan het ook effectief zijn om alleen maar af te stemmen, bijvoorbeeld ter voorbereiding van een besluit.
8. Streef naar het gebruik van uniforme standaarden en processen. ISO 27005 bijvoorbeeld biedt definities van impacts ('consequences'). Het komt de samenwerking ten goede als elke afdeling binnen elke organisatie diezelfde criteria hanteert.
9. Vind een balans tussen algemeen toepasbare instrumenten en organisatie- of afdelingsspecifieke instrumenten die mogelijk lokaal beter passen maar niet door iedereen begrepen worden. Er bestaan mogelijkheden om resultaten uit verschillende instrumenten te 'vertalen 'naar algemene rapportages.

Don'ts

1. Het invullen van een risicoregister een star mechanisme maken: een goed inhoudelijk gesprek is effectiever dan het vullen van veel kolommen. Notulen van zo'n gesprek zijn belangrijk om aan te tonen dat er bewust gesproken is over risico's.
2. Zoveel mogelijk risico's opnemen in het register.
3. De methode leidend laten zijn voor alle stappen.
4. Een rapportage opleveren die geen betrouwbaar beeld geeft.

5 Bestendig wat je hebt opgebouwd

5.1 Lerende organisatie

Zijn de rollen belegd en hebben de early adopters al enkele cycli doorlopen? Ga dan niet op je lauweren rusten, maar blijf toegankelijk voor nieuwe ambassadeurs én inzichten. Kennisdeling is hiervoor zeer waardevol: in een netwerk met andere instellingen, maar ook met onderzoekers en met de studenten.

Ga ook mee in organisatieontwikkelingen. De risicodialogen moeten centraal staan, en het realiseren en monitoren van effectieve maatregelen. Niet het feit dat een specifieke rol is belegd bij een specifieke medewerker.

Als de basis eenmaal staat en er enige ervaring is opgebouwd, kun je gaan leren van die ervaring. Dit lukt het beste wanneer gebeurtenissen en bevindingen op een standaardmanier worden vastgelegd. Waak bij die vastlegging voor omslachtigheid en bureaucratie. De manier van vastleggen mag bijvoorbeeld geen inhoudelijke risicodialoog belemmeren of de organisatie onnodig belasten.

In een volwassen, lerende organisatie worden ook bijna-incidenten (safety) en relevante gebeurtenissen en incidenten uit de buitenwereld geregistreerd, behandeld en gerapporteerd. Bijvoorbeeld een ransomware aanval op een collega-instelling.

Casuïstiek helpt ook om rapportages meer zeggingskracht te geven. Ze maken dan concreet hoe een bepaald risico werkelijkheid werd, maar ook hoe de businesscase van deugdelijk risicomanagement in de praktijk heeft uitgepakt.

Do's

1. Deel je kennis: zo bouw je aan een slagvaardige organisatie.
2. Blijf toegankelijk.
3. Gebruik herkenbare voorbeelden van incidenten.
4. Zorg voor standaardmethodieken in de grondoorzakenanalyses *(root-cause analyses).*
5. Zorg stelselmatig voor checks en dubbelchecks op je data.

Don'ts

1. Beperk je dialogen niet tot gesprekken met sleutelfiguren. Iedereen is risicoleider, en dus maakt iemands rol niet uit.
2. Van de vastlegging van incidenten een bureaucratisch proces maken.

5.2 Holistisch risicomanagement

Risicomanagement is een kwestie van permanent uitbouwen, evalueren en volhouden. De doelen van een organisatie zouden algemeen bekend, of in elk geval op intranet eenvoudig vindbaar moeten zijn. Datzelfde geldt voor de eventuele strategie die de organisatie hanteert om deze doelen te bereiken, én voor de risico's die deze strategie kunnen bedreigen. Deze risico's zouden duidelijk gedefinieerd moeten zijn, zodat iedereen er hetzelfde onder verstaat. Dat is belangrijk, want risicomanagement kan mensen helpen om gezamenlijk – ook over afdelingsgrenzen heen – aan de doelen te werken.

De urgentie van risico's wordt het sterkst gevoeld door de mensen die al een verantwoordelijkheid dragen in een proces. Zij zijn bovendien in staat zaken te concretiseren vanuit hun dagelijkse praktijk en ook tot passende maatregelen te komen. Probeer dus het risicomanagementproces zoveel mogelijk aan te laten sluiten bij de bestaande governance.

Een aandachtspunt daarbij kan integraliteit zijn tussen de verschillende onderdelen of bedrijfsfuncties van de organisatie, alsook de uniformiteit van vastlegging. Deze punten kunnen worden aangepakt door gezamenlijke training in een gedeelde methodiek, maar ook met specifieke ondersteuning voor de vastlegging.

Idealiter zijn ze onderdeel van de on-boarding en komen ze vóór welke andere training dan ook. Benadruk daarbij het gezamenlijk belang, en het teamwork dat nodig is om de doelen zo prettig en efficiënt mogelijk te bereiken.

Zo wordt de organisatie holistisch benaderd: goed doorgevoerd risicomanagement kan leiden tot minder zuilvorming, duidelijk eigenaarschap en heldere, goed onderbouwde beslis- en ingrijpmomenten, die daardoor op meer begrip kunnen rekenen.

Do's

1. Zorg voor een goede onboarding-training op basis van risicomanagement.
2. Benadruk gezamenlijk belang en teamwork.
3. Wijs risico-eigenaren aan en zorg dat gebeurtenissen, ontwikkelingen en incidenten worden gekoppeld aan risico's. De risico-eigenaar moet de bevoegdheid hebben om, indien noodzakelijk, over afdelingen heen resources in te zetten om de risico's te beheersen.
4. Heb je de cyclus al meermaals doorlopen, schrijf dan op wat je hebt gedaan en hoe het ging, en deel dat met anderen.
5. Vul het risicomanagementproces consequent in als PDCA-cyclus (Plan-Do-Check-Act).
6. *Practice what you preach.*
7. Wees voorspelbaar, door vaste momenten in het jaar te kiezen voor terugkerende processtappen. Dat geeft ook vertrouwen.

5.3 Wanneer klinkt succes?

Stip op de horizon is doorgaans de bestendiging in de eerste lijn. Dit is wanneer iedereen zich risico-eigenaar voelt en het persoonlijk leiderschap voor de doelstellingen kan verwoorden. Dat vraagt wat van de hele organisatie: van het werven van personeel, het inwerken, de leiderschapsstijl, de organisatiecultuur en de governance tot het instrumentarium dat ter beschikking wordt gesteld. De risicofunctionarissen zijn dan als dirigenten bijna overbodig, want het instrumentarium is zelfsturend geworden.

De realistische stip op de horizon is echter voor elke organisatie anders. Verschillende stakeholders kunnen verschillende doelen nastreven. Voor sommige is het voldoende dat bepaalde doelen gehaald worden, zoals het scoren van een 3 op de benchmark voor informatiebeveiliging. Andere instellingen streven slechts naar minder incidenten. Weer andere instellingen hebben een heel helder beeld van integraal risicomanagement en willen langs die weg de organisatie gaan besturen. Tenslotte kan het ook zijn dat een stip op de horizon voor jouw instelling helemaal niet handig is: misschien is het doel van je werk slechts te kunnen aantonen dat je alles hebt gedaan wat redelijkerwijs kan.

Wanneer kun je spreken van het ultieme succes? Dat is wanneer het evalueren van risico's en effectiviteit en het nemen van relevante maatregelen vanzelf gaan, doordat iedereen op de werkvloer het in zijn DNA heeft. Tot die tijd zijn alle kleine stapjes ook successen!

Do's

1. Blijf permanent streven naar je doelen op het gebied van risicomanagement.
2. Meet de voortgang van dat streven. Dit kan via testen, benchmarken of sfeerimpressies (als je geen data hebt).
3. Ken de voorkeuren van de verschillende stakeholders, zodat je de sturingsinformatie daarop kan toespitsen. Een stakeholder die van data houdt, ziet graag cijfers. Een ander persoon hoort liever een verhaal. Zo bestendig je je draagvlak.
4. Vier je successen.
5. Evalueer niet alleen binnen de eigen kring, maar bevraag iedereen. Doe dit met een warme methodiek: geen survey, maar een persoonlijk gesprek. Elk contactmoment biedt immers de kans risicobewustzijn aan te wakkeren en nieuwe ambassadeurs te ontmoeten.

Don'ts

1. Streven naar nul incidenten en nul risico's. Dat is een utopie.
2. Alles willen controleren.