Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Implementatierichtlijn

Risicomanagement voor digitale weerbaarheid

Werken aan de basis. Van Nederland en ons Koninkrijk.

Uitgave

CIO Rijk, afdeling IB&P
Turfmarkt 147, 2511 DP Den Haag
cisorijk@minbzk.nl

September 2025

Rechten

Inhoudsopgave

1 Inleiding

Voor een goede dienstverlening aan burgers en ondernemers is de overheid in grote mate afhankelijk van betrouwbare informatie. Die betrouwbaarheid staat voortdurend onder druk als gevolg van dreigingen op het digitale vlak, die vanwege de aantallen, complexiteit en professionaliteit om een goede beheersing vragen. Goed bestuur vereist een goede beveiliging van die informatie, waarbij nieuwe wetgeving verplicht om bij die beveiliging te kiezen voor een risicogebaseerde aanpak. Dit vraagt om een rijksbreed geaccepteerde en toegepaste aanpak voor gestructureerd risicomanagement voor digitale weerbaarheid.
Deze implementatierichtlijn geeft invulling aan deze rijksbrede aanpak.

Doelgroepen

Deze implementatierichtlijn vormt samen met de beleidsrichtlijn en de handreiking één geheel. Deze documenten bieden een gestructureerde aanpak voor risicomanagement voor digitale weerbaarheid. Deze documenten zijn opgesteld voor verschillende doelgroepen.

- De beleidsrichtlijn is geschreven voor en vanuit het strategische perspectief van de bestuurders en lijnmanagers. Hierin wordt vooral uitgelegd wat er wordt verwacht op het gebied van risicomanagement voor digitale weerbaarheid.
- Deze implementatierichtlijn is technischer van aard en meer geschreven voor en vanuit het perspectief van de specialisten die de bestuurders en de lijnmanagers ondersteunen bij het uitvoeren van risicomanagement. Hierin wordt meer uitgelegd hoe invulling moet worden gegeven aan risicomanagement.
- De handreiking bevat verschillende verdiepingen en aanvullende overwegingen voor de uitvoering van risicomanagement en is vooral gericht aan de inhoudelijk specialisten.

Leeswijzer

De hierboven genoemde documenten behandelen risicomanagement voor digitale weerbaarheid. Om de leesbaarheid te vergroten is dit op sommige plekken in deze implementatierichtlijn ingekort tot alleen de term risicomanagement.

De in deze implementatierichtlijn besproken onderwerpen volgen zo veel als mogelijk de lijn van de NEN-ISO 31000 norm en het daarin beschreven risicomanagementproces.

Binnen informatiebeveiliging wordt vaak gesproken over applicaties en IT-systemen. Omdat applicaties en IT-systemen slechts een middel zijn om informatie te verwerken en voor de leesbaarheid van dit document, worden deze niet expliciet benoemd in deze richtlijn. Echter, met het beveiligen van informatie wordt dus ook het beveiligen van applicaties en IT-systemen bedoeld.

2 Risicomanagement en deze implementatierichtlijn

Risicomanagement heeft als doel om de risico's, die het behalen van doelstellingen in gevaar kunnen brengen, te beheersen. Het behalen van organisatiedoelstellingen, en daarmee dus ook het beheersen van de risico's die dat bedreigen, valt onder de verantwoordelijkheid van het bestuur en het lijnmanagement. Het beheersen van cyberveiligheidsrisico's door middel van passende maatregelen is een vereiste vanuit de Cbw (Cyberbeveiligingswet) en onderliggende regelingen. Deze implementatierichtlijn geeft daar een praktische invulling aan.

Informatie is ondersteunend aan de processen waarmee invulling wordt gegeven aan het behalen van de doelstellingen van een organisatie. Om die ondersteuning te kunnen bieden worden betrouwbaarheidseisen gesteld aan deze informatie, welke zich vertalen in beschikbaarheid, integriteit en vertrouwelijkheid. Om die reden is deze implementatierichtlijn gericht op het waarborgen van deze betrouwbaarheidseisen. Betrouwbaarheidseisen aan informatie kunnen ook door externe factoren, zoals wetgeving, worden bepaald.

Binnen deze implementatierichtlijn wordt uitgegaan van het gebruik van een risicomatrix voor het prioriteren van de risico's en de bijbehorende mitigerende maatregelen. Daarin worden kans en impact tegen elkaar uitgezet, wat gecombineerd de hoogte van het risico aangeeft. Des te hoger de kans en/of impact, des te hoger het risico. De hoogte van een risico wordt gebruikt om de aanpak van het risico (inzet en toewijzing van mensen en middelen) te prioriteren. Een voorbeeld van een risicomatrix is te vinden in de handreiking behorende bij deze implementatierichtlijn. Deze richtlijn maakt gebruik van de risicomatrix, omdat dit een gangbaar middel is binnen risicomanagement en omdat het een handig hulpmiddel is bij het visualiseren en prioriteren van risico's.

Een belangrijke rol binnen risicomanagement is de rol van informatie-eigenaar. Een informatie-eigenaar draagt namens het bestuur zorg voor de informatie die aan die persoon door het bestuur is toegewezen. Bij informatie-eigenaarschap horen, binnen de context van deze richtlijn, meerdere verantwoordelijkheden, namelijk:

- het inzichtelijk (laten) maken van de risico's voor de toegewezen informatie;
- het beoordelen van die risico's;
- het selecteren en (laten) implementeren van de juiste mitigerende maatregelen of
  - als een risico binnen de risicobereidheid valt, een risico accepteren of
  - als deze buiten de risicobereidheid valt, daarover in gesprek gaan met hoger management; en
- over de actuele risico's rapporteren richting het bestuur.

Een informatie-eigenaar is tevens eigenaar van de risico's die horen bij de informatie waar diegene eigenaar van is. Een informatie-eigenaar is daarmee dus ook risico-eigenaar. Een verdere uitwerking van taken en verantwoordelijkheden is te vinden in de RASCI-tabel in appendix A.

3 Reikwijdte, context en criteria

Deze implementatierichtlijn gaat over het beheersen van risico's voor informatie binnen de organisatie. Het doel daarbij is dat de betrouwbaarheid van informatie en de beveiliging van de systemen waarmee die informatie verwerkt wordt, gewaarborgd blijft. Informatie die vanuit digitale systemen naar een niet-digitale vorm wordt omgezet, bijvoorbeeld door deze te printen, vallen nog steeds binnen de reikwijdte van deze implementatierichtlijn.

Binnen de organisatie worden afspraken gemaakt over de betrouwbaarheidseisen aan informatie (beschikbaarheid, integriteit en vertrouwelijkheid) en wie op welke wijze verantwoordelijk is voor het realiseren en waarborgen van deze eisen.

Risicomanagement kent verschillende facetten waar specifieke kennis voor nodig is. Lijnmanagers behoren kennis te hebben van het deel van risicomanagement dat nodig is om invulling te kunnen te geven aan hun verantwoordelijkheid. Voor het beheersen van risico's binnen het digitale domein is specialistische kennis nodig. Een lijnmanager hoeft niet zelf over deze specialistische kennis te beschikken, maar moet wel toegang hebben tot deze kennis via directe collega's (bijvoorbeeld de CISO) of externe adviseurs. Het bestuur van de organisatie heeft de taak om ervoor te zorgen dat de juiste en vereiste kennis over risicomanagement en informatiebeveiliging in voldoende mate voor lijnmanagers beschikbaar is.

4 Verkrijg inzicht in eigen situatie

Om risico's inzichtelijk te kunnen maken, is zicht nodig op de impact van een incident dat uit een risico kan voortkomen, op de betrouwbaarheidseisen die aan informatie gesteld worden en op de actoren die mogelijk een inbreuk kunnen maken op de betrouwbaarheid van informatie en daarmee op het ongestoord functioneren van de organisatie.

Impactcategorieën en referentietabel

Incidenten kunnen op verschillende manieren een impact hebben op de organisatie. Om niet ieder mogelijke vorm van een incident na te moeten gaan, is het beter om te denken vanuit impactcategorieën. Bepaal de voor de organisatie relevante impactcategorieën. Verdeel iedere impactcategorie in een aantal niveaus dat qua aantal overeenkomt met het aantal impactniveaus uit de gekozen risicomatrix. Geef per impactcategorie voor ieder niveau een omschrijving. Het ontstane overzicht heet een referentietabel.

De omschrijvingen in deze referentietabel worden gebruikt om de risicobereidheid vast te stellen (zie volgende hoofdstuk) en om tijdens een risicoanalyse de hoogte van de impact van een incident te kunnen bepalen.

In appendix B is een lijst van mogelijke impactcategorieën opgenomen. De handreiking bevat een voorbeeld-referentietabel.

Betrouwbaarheidseisen aan informatie

Breng de informatie die binnen de organisatie verwerkt wordt in kaart. Bepaal per informatieverzameling[1] de gevolgen voor de organisatie indien informatie niet meer beschikbaar, niet meer integer of niet meer vertrouwelijk is. Bepaal van daaruit de vereiste niveaus van beschikbaarheid, integriteit en vertrouwelijkheid van deze informatieverzameling. Houd daarnaast ook rekening met wetgeving en regels vanuit de overheid. De in deze paragraaf beschreven processtappen wordt een Business Impact Analyse (BIA) genoemd.

De vereisten aan informatie die gelden voor de organisatie, kunnen afwijken van de vereisten die gelden vanuit eventuele ketenpartners. Ga over de verschillen met ketenpartners in gesprek en pas op basis van de uitkomst van die gesprekken de eisen aan de beschikbaarheid, integriteit en vertrouwelijkheid aan.

Maak voor het in kaart brengen van informatie zoveel mogelijk gebruik van wat er al is, zoals het verwerkingsregister vanuit de AVG. Overweeg om daar een gecombineerd register voor in te richten.

Actoren en hun aanvalsmethoden

Stel de lijst van actoren vast die een inbreuk kunnen maken op de betrouwbaarheid (BIV) van informatie. Denk naast kwaadwillende actoren ook aan niet-kwaadwillende actoren. Dat zijn mensen die door onoplettendheid, onkunde of onwetendheid per ongeluk voor een incident zorgen. Breng voor de kwaadwillende actoren in kaart wat typische en aannemelijke aanvalsmethoden zijn en hoe goed een actor is in het uitvoeren van zo'n aanval.

1 Informatie die vanuit een logische indeling bij elkaar hoort, zoals de personeelsadministratie, financiële administratie, klantgegevens of productiegegevens.

5 Bepaal risicobereidheid

Om te voorkomen dat het wel of niet accepteren van een risico afhangt van het moment of de persoon die een risico beoordeelt, stelt het bestuur van de organisatie de risicobereidheid vast. Zij kiezen daarvoor een risiconiveau (alle risico's met dezelfde kleur) uit de risicomatrix die is vastgesteld voor de organisatie. Maak voor het kiezen van een risiconiveau ook gebruik van de opgestelde referentietabel. Alle risico's van het gekozen niveau of lager mogen geaccepteerd worden. Alle hogere risico's moeten in principe gemitigeerd worden. Bij het vaststellen van de risicobereidheid van de organisatie, dient uiteraard rekening gehouden te worden met geldende wet- en regelgeving.

Om een risico te accepteren dat hoger is dan de risicobereidheid, moet goedkeuring verkregen worden van een bevoegde lijnmanager of het bestuur. Deze goedkeuring mag maximaal een jaar duren, om te voorkomen dat geaccepteerde risico's uit het zicht raken. Na dat jaar wordt het risico opnieuw beoordeeld. Hoe hoger het risico, des te hoger in de lijn deze goedkeuring moet plaatsvinden.

6 Aanleiding voor een risicoanalyse

Om risico's te kunnen beheersen, moeten deze eerst inzichtelijk gemaakt worden. Risico's worden inzichtelijk gemaakt door middel van een risicoanalyse. Er zijn verschillende aanleidingen om een risicoanalyse te starten of een reeds uitgevoerde te herzien. Informatie-eigenaren hanteren minimaal onderstaande aanleidingen.

- Bij de invoering van een nieuw proces of werkwijze voor de verwerking van informatie. Dit vraagt om een geheel nieuwe risicoanalyse, waarbij alle stappen uit het volgende hoofdstuk doorlopen moeten worden. Het is de verantwoordelijkheid van de informatie-eigenaar om de risicoanalyse in gang te zetten.
- Bij een significante wijziging in een bestaand proces, werkwijze of infrastructuur. Afhankelijk van de grootte van de wijziging zal een nieuwe risicoanalyse moeten worden uitgevoegd of kan een bestaande worden bijgewerkt.
- Een verandering in de risicobereidheid of relevante wetgeving kunnen tot strengere beveiligingseisen leiden. Eerdere gemaakte beslissingen in risicoanalyses zullen heroverwogen moeten worden.
- Een verhoging van de classificatie van betrokken informatie kan aanleiding zijn om voor uitgevoerde risicoanalyses na te gaan of maatregelen moeten worden aangescherpt of extra maatregelen nodig zijn.
- Een incident kan aanleiding zijn om van de uitgevoerde risicoanalyses te beoordelen of de eerder gemaakte inschattingen correct zijn of bijgesteld moeten worden.
- Het verstrijken van de geldigheidsduur van een uitgevoerde risicoanalyse. De eerder uitgevoerde risicoanalyse moet geactualiseerd worden.
- Bij een mogelijke verandering in het dreigingslandschap. Het is de verantwoordelijkheid van de CISO om risico-eigenaren hierover te informeren. Denk aan technische redenen zoals het bekend worden van kwetsbaarheden of nieuwe aanvals-technieken, technologische ontwikkelingen, maar ook aan veranderingen in de relatie tussen landen of maatschappelijke ontwikkelingen en gebeurtenissen die aanleiding kunnen zijn voor digitale aanvallen.
- Voorafgaand aan de aanschaf van een ICT-dienst of ICT-product van een leverancier, waarbij ook gekeken wordt naar de afhankelijkheid van die leverancier.

7 Voer risicoanalyses uit

Het uitvoeren van een risicoanalyse kan op meerdere manieren gebeuren. Onderstaande beschrijving geeft de stappen aan die minimaal nodig zijn om een goede risicoanalyse uit te voeren. Hoewel deze beschrijving voor de leesbaarheid in stappenplanvorm is opgeschreven, wordt hiermee geen nieuwe methodiek voor risicoanalyse geïntroduceerd, maar slechts de voorwaarden geschetst waar een goede methodiek aan moet voldoen.

Randvoorwaarden

Om een risicoanalyse te starten, wordt minimaal aan de volgende voorwaarden voldaan.

1. De opdracht voor het uitvoeren van een risicoanalyse (zie hoofdstuk 6) moet komen van de persoon die eigenaar is van de informatie waarover de risicoanalyse moet worden uitgevoerd. Deze persoon wordt risico-eigenaar van de in kaart gebrachte risico's.
2. De opdracht voor het uitvoeren van een risicoanalyse moet een duidelijke reikwijdte hebben. Het goed kiezen van de reikwijdte is belangrijk voor het verkrijgen van bruikbare resultaten van een risicoanalyse. Een proces, een afdeling of een project zijn goed om als reikwijdte te kiezen. Een applicatie is wat minder ideaal als reikwijdte, omdat je dan mogelijk te beperkt kijkt en de gevolgen voor het bovenliggende proces mogelijk niet goed kan overzien. De informatie in een applicatie is mogelijk onderdeel van een proces dat verder reikt dan alleen die applicatie. Om te beoordelen of een applicatie veilig is, is een penetratietest een betere aanpak. Om te beoordelen of een netwerk veilig is, is threat modeling een betere aanpak.
3. De opdracht voor het begeleiden van de risicoanalyse moet neergelegd worden bij iemand die daar voldoende kennis van heeft, zoals een CISO, ISO of een security-adviseur. Deze persoon wordt de risicoanalyse-procesbegeleider. De informatie-eigenaar blijft verantwoordelijk voor het treffen van de voorbereidingen en het organiseren van de analyse-sessie.

Voorbereiding

Een goed eindresultaat van een risicoanalyse is voor een belangrijk deel afhankelijk van een goede voorbereiding. Dit geldt zeker als de deelnemers van de analysesessie onvoldoende ervaren zijn in het uitvoeren van een risicoanalyse. De risicoanalyse-procesbegeleider voert bij de voorbereiding minimaal de volgende stappen uit.

1. Als de risicoanalyse-procesbegeleider niet de CISO is, ga dan bij de CISO na of er eisen zijn aan de te gebruiken methodiek voor een risicoanalyse.
2. Vraag aan de informatie-eigenaar om het doel van de verwerking van informatie binnen de gekozen reikwijdte. Dit bepaalt de denkrichting voor het vaststellen van de relevante risico's en de ernst van een incident met informatie.
3. Vraag bij de informatiebeheerafdeling een overzicht op van de applicaties die binnen de reikwijdte van de risicoanalyse vallen. In een goed overzicht staan de informatiestromen tussen de applicaties en wie op welke informatie bewerkingen uitvoert en om welke reden dat is. Dit helpt bij het zoeken naar hoe en waar zaken fout kunnen gaan en dus een risico opleveren. Indien zo'n overzicht niet beschikbaar is, stel deze dan zelf op.
4. Vraag de BIV-classificatie per informatieverzameling op. Bij voorkeur is deze classificatie beschikbaar vanuit een informatie-beheerafdeling. Als dat niet het geval is, zal deze in samenspraak met de informatie-eigenaar bepaald moeten worden. De classificatie is medebepalend voor de hoogte van de impact van een risico.
5. Controleer of de lijst met actoren (zie hoofdstuk 4) voldoende actueel is. Bepaal of er actoren zijn die tijdens de analyse-sessie extra aandacht behoeven.
6. Zorg voor een lijst van dreigingen, ter inspiratie tijdens de analysesessie. Het geeft de aanwezigen van de analysesessie ideeën over op welke manier dreigingen zich voor kunnen doen. Vul deze lijst aan met nieuwe dreigingen die tijdens de analysesessie zijn vastgesteld.
7. Bepaal wie bij de analysesessie aanwezig gaan zijn. Dat zijn mensen met voldoende (technische) kennis van de betrokken systemen en de reeds bestaande beveiligingsmaatregelen en mensen met kennis van het belang van die systemen en de daarin opgeslagen informatie voor de organisatie. Bij voorkeur is ook de informatie-eigenaar aanwezig.
8. Geef aan degene die bij de analysesessie aanwezig zijn. duidelijke uitleg over wat er gaat gebeuren, wat de risicoanalyse precies inhoudt, wat er van hen verwacht wordt en wat de risicoanalyse moet gaan opleveren.
9. Technische zaken in detail bespreken is niet het doel van een risicoanalyse. Communiceer dit van te voren goed naar de technisch onderlegde mensen, om te voorkomen dat de technisch en minder-technisch onderlegde aanwezigen elkaar verliezen tijdens de analyse-sessie. Indien nodig, kunnen technische details van een aanval, kwetsbaarheid of maatregel buiten de analyse-sessie om doorgesproken worden.

Analyse-sessie

Dit onderdeel vormt de daadwerkelijke risicoanalyse. De risicoanalyse-procesbegeleider hanteert daarbij minimaal de volgende stappen.

1. Bepaal welke dreigingen een gevaar kunnen vormen voor de betrouwbaarheidseisen van de informatie binnen de reikwijdte en beschrijf deze.
2. Bepaal per dreiging, indien van toepassing, welke actor hier mogelijk achter kan zitten. Laat de bedreiging die uitgaat van de actor medebepalend zijn voor de hoogte van de kans. De dreiging die uitgaat van een actor wordt bepaald door de kennis die de actor bezit, de middelen waarover de actor kan beschikken en de motivatie van de actor om een (gerichte) aanval uit te voeren.
3. Stel per dreiging vast op welk(e) informatie(systeem) het betrekking heeft.
4. Bepaal per dreiging mogelijke oorzaken en mogelijke gevolgen.
5. Stel per dreiging de hoogte van de kans (kijkend naar de oorzaken en de actor) en de impact (kijkend naar de gevolgen) vast. Houd daarbij rekening met de reeds bestaande beveiligingsmaatregelen. De hoogte van het risico dat daaruit volgt is vooral bedoeld om de mitigerende maatregelen te prioriteren. Motiveer de gemaakte keuzes.
6. Stel per dreiging vast hoe te handelen (de risico-evaluatie): accepteren, kans verlagen, impact verlagen, kans en impact verlagen, risico overdragen of het risico wegnemen (zie appendix C) en motiveer deze keuze. Deze keuze wordt bij voorkeur door de risico-eigenaar gemaakt. Indien de risico-eigenaar niet aanwezig is, wordt de keuze door de aanwezigen gemaakt en wordt deze later aan de risico-eigenaar voorgelegd ter goedkeuring.
   Het kan gebeuren dat tijdens een analyse-sessie nog niet besloten kan worden hoe te handelen, omdat daar nadere informatie voor nodig is die niet tijdens de analyse-sessie verkregen kan worden. Maak afspraken over door wie en hoe deze informatie verkregen wordt en wanneer de keuze voor hoe te handelen alsnog genomen wordt.
7. Indien ervoor gekozen wordt om een risico te accepteren terwijl deze buiten de risicobereidheid valt, zorg dan voor een officiële acceptatie door de daarvoor aangewezen manager of bestuurder. Zie hiervoor ook hoofdstuk 5 over risicobereidheid.
8. Indien een risico niet wordt geaccepteerd, bepaal dan per dreiging in hoofdlijnen welke maatregelen nodig zijn om het risico te beheersen.

Het is ook mogelijk en zelfs ook wenselijk om risico's buiten een analysesessie om vast te stellen. Stimuleer collega's, vooral bij diegenen die meewerken in een project, om risico's te melden bij de eigenaar van hetgeen waar het risico betrekking op heeft. Dit kan ook via een projectleider gebeuren. Het is aan de informatie-eigenaar om het risico vervolgens af te handelen conform de beschrijving in het volgende hoofdstuk.

8 Bepaal risicobehandeling

Na de analysesessie is het belangrijk om de resultaten op een goede manier te verwerken. De risicoanalyse-procesbegeleider hanteert daarbij minimaal de volgende stappen.

1. Werk de maatregelen die tijdens de analyse-sessie in hoofdlijnen zijn bepaald verder uit. Denk daarbij aan verschillende mogelijke oplossingsrichtingen, zoals organisatorische, technische en mensgerichte maatregelen. Maak onderscheid tussen preventieve maatregelen (gericht op de oorzaken), detectieve maatregelen (gericht op het incident zelf) en repressieve maatregelen (gericht op de gevolgen).
2. Bepaal per maatregel wie de beoogde maatregeleigenaar wordt en wat de gewenste einddatum voor de implementatie is.
3. Indien de risico-eigenaar niet aanwezig was bij de analyse-sessie, maak dan in overleg met de risico-eigenaar de risico's en de maatregelen definitief. Dat betekent dat de risico-eigenaar de gemaakte keuzes tijdens de analyse-sessie accepteert of aanpast.
4. Laat de risico-eigenaar de geldigheidsduur van de risicoanalyse aangeven. Verwerk deze in de rapportage. Na het verstrijken van deze tijd zal de risicoanalyse geactualiseerd moeten worden.
5. Lever de rapportage over de risicoanalyse op aan de risico-eigenaar.
6. Leg de risico's vast in het risicoregister (zie hoofdstuk 9).
7. Werk in overleg met inhoudelijk experts de eventuele technische details van de maatregelen uit. Let daarbij op de haalbaarheid en de kosten van de maatregelen.
8. Maatregelen worden mogelijk door iemand anders dan de risico-eigenaar doorgevoerd. Deze andere persoon wordt daarmee de maatregeleigenaar. Maak in overleg met de risico-eigenaar en de maatregeleigenaar de maatregelen definitief.
9. Indien een risico niet wordt geaccepteerd, maar de maatregelen om wat voor een reden dan ook niet doorgevoerd (kunnen) worden, dan zorgt de risico-eigenaar voor een officiële acceptatie van het risico door de daarvoor aangewezen manager of bestuurder.
10. Leg de maatregelen vast in het risicoregister.

9 Registreer risico's en bepaal risicobeeld

De organisatie beschikt over een eigen risicoregister. Bij voorkeur is dit risicoregister een algemeen risicoregister, waar ook risico's op vlakken anders dan digitale weerbaarheid in bijgehouden worden, zodat een organisatiebreed risicobeeld ontstaat.

In het risicoregister worden ook de bijbehorende mitigerende maatregelen geregistreerd.

Het risicoregister wordt gebruikt om rapportages op te stellen voor het bestuur over het actuele risicobeeld. Maak afspraken over wie deze risicorapportages opstelt, wanneer dat gebeurt, in welke vorm en aan wie deze worden opgeleverd.
Neem rapportages over risicomanagement op in bestaande managementrapportages. Maak de bespreking van risico's en de beheersing daarvan onderdeel van bestaande overleggen tussen en met informatie-eigenaren, bestuurders en experts op het gebied van risicomanagement en cybersecurity.

Vermijd in rapportages richting het bestuur zoveel mogelijk het gebruik van technische termen die om uitleg vragen. Risico-management vindt, inhoudelijk gezien, voornamelijk plaats in de lijnmanagement-laag. De bestuurlijke laag heeft als taak om te sturen op dat managementproces. De rapportages moeten daarom vooral gaan over hoe het staat met het proces en de effectiviteit van de sturing daarop en niet over afzonderlijke risico's. Uiteraard zijn uitzonderingen te maken voor risico's die, vanwege de hoogte van het risico of de impact van een te nemen beslissing, aandacht van het bestuur vereisen.

10 Monitor risico's, maatregelen en proces

De risico's in het risicoregister worden door de risico-eigenaren periodiek geëvalueerd om te beoordelen of deze nog steeds geldig zijn of niet. De in hoofdstuk 6 aangegeven aanleidingen voor het opnieuw beoordelen van eerder uitgevoerde risicoanalyses, worden door de organisatie gemonitord.

Voor de maatregelen van vervallen risico's wordt beoordeeld of deze afgeschaft kunnen worden. De risico-eigenaar bepaalt dit in overleg met de maatregeleigenaar.

De maatregelen in het risicoregister worden door de maatregeleigenaren periodiek geëvalueerd om te zien of deze nog effectief en efficiënt zijn. Voor niet-effectieve of niet-efficiënte maatregelen worden in overleg met de risico-eigenaren correctieve acties of alternatieve maatregelen bepaald.

De CISO monitort de correcte uitvoering van het risicomanagementproces voor digitale weerbaarheid binnen de organisatie en rapporteert daarover naar het bestuur.

Het bestuur van de organisatie bespreekt de rapportages ter verbetering van het risicomanagementproces. De frequentie van rapporteren en overleggen worden door het bestuur bepaald, maar deze worden vooral bepaald door de noodzaak om het risico-managementproces te verbeteren.

11 Appendix A: RASCI-tabel

	Responsible	Accountable	Supporting	Consulted	Informed
Risicomanagement					
Bestuur		X			X
Informatie-eigenaar	X				
CISO			X	X	
Monitoren op de effectiviteit van risicomanagement					
Bestuur		X			X
CISO	X				
Uitvoeren van een risicoanalyse					
Informatie-eigenaar		X		X	
RA-procesbegeleider	X				
CISO			X		
Accepteren van risico's buiten de risicobereidheid					
Bestuur		X		X	
Informatie-eigenaar	X				
CISO			X		
Opstellen van de risicoanalyserapportage					
Informatie-eigenaar		X		X	X
RA-procesbegeleider	X				
CISO					X
Bestuur					X
Overdragen van de maatregelen naar een maatregeleigenaar					
Bestuur		X			X
Informatie-eigenaar	X				
Maatregeleigenaar				X	X
Implementeren van de maatregelen					
Informatie-eigenaar		X			
Maatregeleigenaar	X				
Monitoren op de geldigheid van de risico's					
Bestuur		X			X
Informatie-eigenaar	X				
CISO			X		
Monitoren op de effectiviteit en efficiëntie van de maatregelen					
Informatie-eigenaar		X			X
Maatregel-eigenaar	X				
CISO			X		

Informatie-eigenaar: Dit is hier bedoeld als algemene term. Een informatie-eigenaar wordt na het uitvoeren van een risicoanalyse risico-eigenaar van de in kaart gebrachte risico's. Het kan voorkomen dat een risico qua eigenaarschap beter aan iemand anders kan worden toegewezen. Dit zal in goed overleg moeten gebeuren.

RA-procesbegeleider: Risicoanalyse-procesbegeleider. Indien een informatie-eigenaar onvoldoende kennis heeft van de uitvoering van een risicoanalyse, kan diegene daar iemand met de juiste kennis voor inschakelen. Dit kan de CISO zijn.

Maatregeleigenaar: De implementatie en het onderhoud van een maatregel hoeft niet per se onder de verantwoordelijkheid van de risico-eigenaar te vallen. Zo kan bijvoorbeeld een ICT-maatregel onder de verantwoordelijkheid van de ICT-manager vallen. De maatregeleigenaar informeert de risico-eigenaar over de implementatie, effectiviteit en efficiëntie van de maatregel.

12 Appendix B: Impact-categorieën

Een risico kan leiden tot een incident. Een incident kan gevolgen hebben voor de beschikbaarheid, de integriteit en vertrouwelijkheid van informatie. Dit zijn de directe of primaire gevolgen.

Deze directe gevolgen kunnen echter ook weer leiden tot indirecte of secundaire gevolgen, welke zich op meerdere manieren kunnen voordoen. Deze verschillende manieren staan in onderstaande categorieën-lijst uiteengezet. De vertaling van de directe naar indirecte gevolgen is belangrijk om de hoogte van de impact goed te kunnen bepalen.

Uiteraard kan een gevolg in een categorie leiden tot een nieuw gevolg in een andere categorie. Zo kunnen juridische gevolgen leiden tot financiële gevolgen (boetes of schadevergoeding) en maatschappelijke gevolgen leiden tot imago-schade (minder vertrouwen in de overheid).

Hanteer onderstaande lijst als uitgangspunt, maar vul deze vooral aan met organisatie-specifieke impact-categorieën. Zie ook de BIO voor relevante impact-categorieën.

- **Organisatiedoel.** De realisatie van een organisatiedoel is verstoord.
- **Financieel.** Alle kosten voor het herstellen van de gelopen schade. Denk hierbij ook aan schade voor derden.
- **Imago / reputatie.** Een vervelend aspect van imago-schade is dat het lastig te meten is. De grootte van de imago-schade is afhankelijk van hoe breed het incident bekend wordt, maar ook hoe lang een eventueel opgedane slechte naam aan de organisatie blijft kleven.
- **Juridisch.** Indien het niet voldoen aan wettelijke (beveiligings)voorschriften (mede)oorzaak is van het ontstaan van het incident en derde partijen schade hebben ondervonden als gevolg van het incident, dan kan dat juridische gevolgen hebben.
- **Maatschappelijk.** Een incident kan leiden tot de verstoring van een proces van bijvoorbeeld een uitvoeringsorganisatie, waardoor (delen van) de maatschappij geraakt worden.
- **Milieu.** Een verstoring van systemen met fysieke gevolgen, zoals brand, explosies, overstromingen of het ontsnappen van giftige stoffen, kunnen schadelijke gevolgen hebben voor het milieu. Een incident kan ook negatieve gevolgen hebben voor het milieu als deze zich voordoen bij overheidsorganisaties die waken over het milieu of het verbeteren van het milieu als taak hebben.
- **Politiek.** Grote incidenten kunnen (mede-)aanleiding zijn voor het aftreden van een directeur, een minister of zelfs het vallen van een kabinet.
- **Veiligheid personeel.** Het lekken van informatie over bijvoorbeeld personen die heimelijk werk uitvoeren (politie, inlichtingendienst, Defensie, et cetera), kan de veiligheid van die personen in gevaar brengen.

13 Appendix C: Risico-evaluatie

Is een risico eenmaal geïdentificeerd, dan is de volgende stap om te besluiten hoe daarmee om te gaan. Deze stap wordt in de ISO 31000 de risico-evaluatie genoemd. Daarvoor zijn verschillende mogelijkheden beschikbaar.

1. **Accepteren.** Geen enkel risico is naar nul terug te brengen. Extra maatregelen blijven nemen is op een gegeven moment niet meer efficiënt. Het restrisico accepteren is dan een logische keuze.
2. **Impact verlagen.** Informatiebeveiliging is in de praktijk vaak gericht op het voorkomen van incidenten. Echter, voor lage-kans/hoge-impact risico's is het efficiënter om de impact te verlagen dan om de kans nog verder te verlagen. Vanuit het perspectief van risicomanagement betekent dat mogelijk andere soorten maatregelen dan gebruikelijk zijn.
3. **Kans verlagen.** Naast een impact-verlagende aanpak, kan ook voor een kans-verlagende aanpak gekozen worden. Dit is vooral effectief bij de hoge-kans risico's.
4. **Kans en impact verlagen.** Voor risico's waarbij zowel de kans als de impact hoger dan laag wordt ingeschat, is het verstandig om maatregelen te nemen die zowel de kans als de impact verlagen.
5. **Risico overdragen.** De gevolgen van een risico kunnen worden overgedragen. Denk daarbij aan een verzekering, waarbij de financiële gevolgen naar de verzekeraar worden overgedragen. Het is goed om te realiseren dat een risico vaak gevolgen kan hebben op meerdere vlakken. Denk bijvoorbeeld aan imago-schade of gevolgen voor betrokkenen indien persoonsgegevens geraakt worden. Indien naast het overdragen geen verdere maatregelen genomen worden, dan worden die gevolgen dus in feite geaccepteerd.
6. **Risico wegnemen.** Naast het nemen van maatregelen, kan ook gekozen worden om te stoppen met de activiteit die een risico oplevert. Daarmee wordt het risico weggenomen. Dit is een goede aanpak voor activiteiten waarbij het voordeel van die activiteit niet opweegt tegen het risico dat daardoor ontstaat.
7. **Beslissing uitstellen.** Indien tijdens een risicoanalyse te weinig informatie beschikbaar is voor de risico-evaluatie, dan kan besloten worden om daar nader onderzoek naar te doen. Maak afspraken over door wie en hoe deze informatie verkregen wordt en wanneer de risico-evaluatie opnieuw zal plaatsvinden.

Deze brochure is een uitgave van:
CIO Rijk, afdeling IB&P

Turfmarkt 147, 2511 DP Den Haag
cisorijk@minbzk.nl

September 2025