Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Beleidsrichtlijn

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**	**5**
	Doelgroepen	5
	Leeswijzer	5
	Reikwijdte en scope	6
	Governance	6
	Legitimatie en doelen	7
2	**Principes en randvoorwaarden voor risicomanagement voor digitale weerbaarheid**	**8**
	Hanteer de 7 principes voor risicogestuurd werken	8
	Stel eenduidige organisatiedoelen vast	9
	Zorg voor een duidelijke verdeling van taken en verantwoordelijkheden	9
	Zorg voor inzicht in de organisatie en in de informatievereisten	10
	Realiseer en behoud een open cultuur	10
3	**Realisatie van organisatiedoelen**	**11**
	Neem goede dienstverlening en organisatiedoelen als uitgangspunt	11
4	**Ongestoord functionerende organisatie**	**12**
	Beschouw betrouwbare informatie als randvoorwaarde	12
5	**Bedreigingen voor de betrouwbaarheid van informatie**	**13**
	Verkrijg inzicht in actoren en dreigingen	13
	Verkrijg inzicht in kwetsbaarheden en risico's	13
	Bepaal de rangschikking van de geïdentificeerde risico's	14
6	**Het borgen van de betrouwbaarheid van informatie**	**15**
	Tref maatregelen op basis van kans en gevolgen	15
	Tref organisatorische, technische en mensgerichte maatregelen	16
7	**Het borgen van de effectiviteit van maatregelen**	**17**
	Monitor veranderingen in het dreigingsbeeld	17
	Monitor de effectiviteit van getroffen maatregelen	17
	Monitor wijzigingen in opzet van de organisatie	18
8	**Het afwegen van belangen en besluiten tot bijsturing**	**19**
	Rapporteer veranderingen, kwetsbaarheden en risicoblootstelling	19
	Bespreek de risicoblootstelling en de digitale weerbaarheid	19
	Weeg opbrengsten en investeringen zorgvuldig af	19
9	**Risicomanagement en externe partijen**	**21**
	Ketens	21
	Leveranciers	22
10	**Definities**	**23**
11	**Appendix A**	**24**

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. Dit beleid geeft invulling aan deze rijksbrede aanpak.

Doelgroepen

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

- Deze beleidsrichtlijn is geschreven voor en vanuit het perspectief van de bestuurders en lijnmanagers. Hierin wordt vooral uitgelegd wat er wordt verwacht op het gebied van risicomanagement voor digitale weerbaarheid.
- De 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

Dit document bevat een beleidsrichtlijn en het toepassen ervan is dus niet verplicht. Om de leesbaarheid te vergroten en om de adoptie naar eigen beleid te vereenvoudigen, is in de rest van dit document de term beleid aangehouden.

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

De hoofdstukindeling van dit beleid is afgestemd op de volgorde van de activiteiten van het risicomanagementproces volgens de NEN-ISO 31000 norm voor risicomanagement. Vanaf het vaststellen van de randvoorwaarden en het kader voor risicomanagement, tot en met het monitoren van de effectiviteit van de getroffen maatregelen ter borging van de betrouwbaarheid van de voor de organisatie relevante informatie.

De beleidsregels voortkomend uit dit beleid worden per hoofdstuk in aparte tabellen aangegeven. Wanneer van toepassing, is per beleidsregel een verwijzing opgenomen naar het gerelateerde hoofdstuk in de implementatierichtlijn. In appendix A is een volledig overzicht opgenomen van de beleidsregels.

Dit beleid omvat risicomanagement voor digitale weerbaarheid. De effectiviteit hiervan is in belangrijke mate afhankelijk van de wijze waarop invulling wordt gegeven aan onderwerpen zoals governance, procesmanagement, assetmanagement en informatiemanagement. Dit zijn afzonderlijke managementdomeinen die daarom niet verder in dit risicomanagementbeleid zijn uitgewerkt.

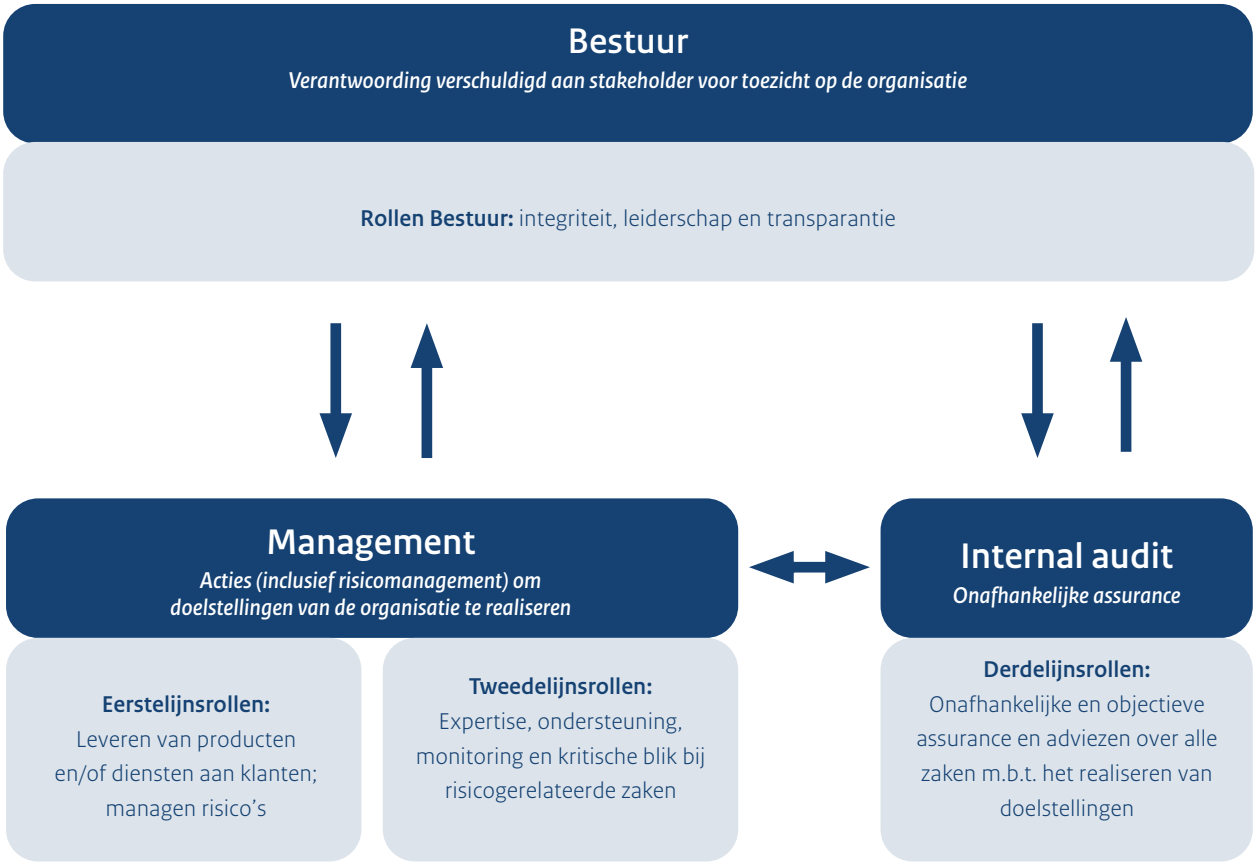
Binnen informatiebeveiliging wordt vaak gesproken over applicaties en IT-systemen. Omdat applicaties en IT-systemen slechts een middel zijn om informatie te verwerken en voor de leesbaarheid van dit document, worden deze niet expliciet benoemd in dit kader. Echter, met het beveiligen van informatie wordt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

Reikwijdte en scope

Dit risicomanagementbeleid, dat zich vertaalt in de beleidsregels zoals vermeld in appendix A, is opgesteld vanuit het perspectief van de digitale weerbaarheid. Dit betekent dat het in dit beleid gaat om het ontwikkelen van het vermogen om risico's die gevolgen kunnen hebben voor de betrouwbaarheid van de voor de organisatie relevante informatie, tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen. Maatregelen die gericht zijn op het voorkomen van incidenten, het vroegtijdig herkennen van incidenten wanneer die zich voordoen en het beperken van de schade van incidenten.

Wat precies verstaan wordt onder digitale weerbaarheid kan per organisatie verschillen en hoeft zich niet te beperken tot de klassieke informatiebeveiliging. Het is goed om te realiseren dat op relevante zaken buiten het digitale domein, ook risicomanagement kan worden toegepast. Het is verstandig om daar gezamenlijk in op te treden.

Governance



De aansturing van een organisatie kan volgens het bovenstaande drie-lijnen-model[1] beschreven worden. Een eerste lijn die de acties uitvoert die invulling geven aan de realisatie van de organisatiedoelen en de beheersing van de gerelateerde risico's.
Een tweede lijn die de eerste lijn ondersteunt in het beheersen van risico's. Een derde lijn die de kwaliteit van de risicobeheersing door de eerste lijn en de samenwerking tussen de eerste en tweede lijn onafhankelijk beoordeelt en adviezen geeft ter verbetering daarvan.
Zowel het management als internal audit leggen verantwoording af aan en rapporteren naar het bestuur. Het bestuur geeft richting, delegeert taken, voorziet in benodigde middelen en houdt toezicht op de gehele organisatie.
Het management en internal audit zorgen voor onderlinge afstemming, communicatie, coördinatie en samenwerking.

1 https://www.iia.nl/kenniscentrum/vaktechnische-publicaties/three-lines-model-updated---nl.

Legitimatie en doelen

Legitimatie	Doelen
Risicomanagement als voorwaarde voor goede dienstverlening Wanneer binnen een organisatie geen geaccepteerd risico-managementbeleid wordt toegepast en er geen gemeenschappelijke risicotaal wordt gesproken, kan het werken met en het uitwisselen van informatie binnen de organisatie of met externe partijen op zichzelf al een risicovolle aangelegenheid zijn. Zo kunnen verwachtingskloven ontstaan tussen organisatie-onderdelen over het bestaan en de ernst van risico's. Verschillende opvattingen kunnen ontstaan over de aard en noodzaak van nog te treffen maatregelen en over de werking van de bestaande maatregelen. Een onterecht gevoel van grip op de risico's kan ontstaan, doordat risico's, of niet goed werkende maatregelen, onopgemerkt blijven. Dit kan leiden tot een onjuiste prioritering van risico's en daardoor tot een verkeerde inzet van experts en ineffectieve allocatie van budget voor risicobeheersing. Het kan ertoe leiden dat de organisatie wordt verrast als risico's daadwerkelijk optreden en de schade al is geleden. Er moeten dan extra kosten gemaakt worden voor reparaties en er moet geïnvesteerd worden in herstel van het interne vertrouwen en het vertrouwen van eventuele externe belanghebbenden. Dit alles ten koste van het voorkomen en het vroegtijdig detecteren van risico's die gevolgen kunnen hebben voor de realisatie van de organisatiedoelen en uiteindelijk voor de goede dienstverlening aan burgers en ondernemers.	**Naleving Cyberbeveiligingswet (Cbw) vereisten –** met het toepassen van dit beleid wordt de organisatie in staat gesteld te voldoen aan de vereisten op het gebied van risicomanagement die voortkomen uit de Cbw. **Effectieve sturing –** met efficiënte samenwerking en beter inzicht in risico's op het gebied van de digitale weerbaarheid, kan risico-gebaseerd worden gestuurd op de digitale weerbaarheid. Het maakt het mogelijk om risicobeelden over organisatieonderdelen te kunnen vergelijken en concentraties en stapelingen van risico's te herkennen. Risicoblootstelling en risicobehandeling kunnen gerichter worden afgestemd. **Integraal inzicht –** vollediger inzicht in afhankelijkheden tussen organisatieonderdelen en in de risico's op het gebied van de digitale weerbaarheid die gevolgen kunnen hebben voor de betrouwbaarheid van de voor de organisatie relevante informatie en voor het ongestoord functioneren, ofwel de continuïteit, van de organisatie. **Efficiënte samenwerking –** effectieve en efficiënte samen-werking tussen betrokken ambtenaren bij het uitvoeren van risicomanagementactiviteiten op basis van een gestructureerd risicomanagementproces en een gemeenschappelijke risicotaal.

Er bestaat behoefte om inzicht te hebben in de aard en in de oorsprong van de dreigingen die consequenties kunnen hebben voor de betrouwbaarheid van de voor de organisatie relevante informatie. Ook is er behoefte om inzicht te hebben in de toereikendheid van de getroffen maatregelen die bedoeld zijn om de betrouwbaarheid van die informatie te borgen. Dit inzicht is nodig om organisatiebreed risicogestuurd te kunnen werken.

Met het toepassen van dit beleid wordt een belangrijke bijdrage geleverd aan de borging van de betrouwbaarheid van de voor de organisatie relevante informatie en aan de realisatie van de organisatiedoelen. Dit als basis voor de goede dienstverlening aan burgers en ondernemers. Met betrouwbaarheid van de voor de organisatie relevante informatie wordt de beschikbaarheid, de integriteit en de vertrouwelijkheid van die informatie bedoeld.

Voortschrijdend inzicht en wijzigingen in de wettelijke vereisten kunnen aanleiding zijn voor aanpassing van dit beleid en de bijbehorende implementatierichtlijn.

2 Principes en randvoor-waarden voor risico-management voor digitale weerbaarheid

Het effectief beheersen van risico's en het sturen op risico's die gevolgen kunnen hebben voor de betrouwbaarheid van de voor de organisatie relevante informatie is aan enkele principes en randvoorwaarden verbonden die hieronder worden toegelicht. Wanneer daar niet aan wordt voldaan, berust de digitale weerbaarheid van een organisatie meer op toeval en wordt mogelijk niet voldaan aan de eisen voor risicomanagement die voortkomen uit wet- en regelgeving.

Voor het opstellen van dit beleid en de bijbehorende implementatierichtlijn is rekening gehouden met Europese en Nederlandse vereisten en standaarden op het gebied van risicomanagement en informatiebeveiliging zoals opgenomen in de Cbw en onderliggende regelingen, in NEN-ISO 31000 en in het ENISA-raamwerk. Bestuurders en lijnmanagers volgen het beleid en leggen afwijkingen met een zorgvuldige onderbouwing vast om eventueel te kunnen overleggen aan toezichthouders en andere belanghebbenden.

Hanteer de 7 principes voor risicogestuurd werken

Om risicogebaseerd te kunnen sturen op het voortdurend in stand houden van de digitale weerbaarheid, worden onderstaande zeven principes in acht genomen voor risicomanagement voor digitale weerbaarheid.[2] Deze worden onderstaand kort toegelicht

2 Gebaseerd op de vier kenmerken van daadwerkelijk risicogestuurd werken: Gestructureerd, Geformaliseerd, Geïntegreerd en Geaccepteerd. Bron: Dr. Ir. Martin van Staveren MBA – Risicogestuurd werken in de praktijk. Deze zijn niet bedoeld als groeipad, maar dienen allemaal tegelijk in acht te worden genomen.

Georiënteerd (doel) – Alle risicomanagementactiviteiten zijn primair gericht op het vergroten van de kans op het realiseren van de organisatiedoelen door middel van het ongestoord functioneren van de organisatie op basis van betrouwbare informatie; Georganiseerd (governance) –De taken en verantwoordelijkheden op het gebied van risicomanagement zijn eenduidig gedefinieerd en belegd;

Gestructureerd (proces) – De risicomanagementactiviteiten worden uitgevoerd volgens een gestructureerd en continu proces. Dit proces doorloopt de volgende processtappen: vaststellen van de context, risico-identificatie, risicoanalyse, risico-evaluatie, risicobehandeling, rapportage en monitoring. Door het toepassen van dit beleid en het achtereenvolgens uitvoeren van de in dit beleid opgenomen beleidsregels, wordt het risicomanagementproces stapsgewijs doorlopen;

Geïntegreerd (sturing) - De risicomanagementactiviteiten, -rapportages en -dialogen zijn integraal onderdeel van de bestaande planning & control cyclus en van de reguliere managementactiviteiten, -rapportages en dialogen;

Geformaliseerd (beleid) - Dit risicomanagementbeleid is goedgekeurd door het bestuur van de organisatie. Het naleven van het beleid is daarmee voorbij aan de vrijblijvendheid;

Geaccepteerd (leiderschap) - Het naleven van het risicomanagementbeleid wordt door bestuurders, lijnmanagers, experts en ondersteuners als vanzelfsprekend gezien. Bestuurders dragen het naleven van dit beleid actief en expliciet uit en onderkennen dat zij eindverantwoordelijk zijn voor risicomanagement. Bestuurders en lijnmanagers onderkennen dat risicomanagementtaken en verantwoordelijkheden integraal onderdeel zijn van hun reguliere bestuurstaken en managementactiviteiten;

Geëquipeerd (kennis) - De betrokken bestuurders, lijnmanagers, experts en ondersteuners beschikken over toereikende kennis en middelen om hun taken op het gebied van risicomanagement voor digitale weerbaarheid uit te kunnen voeren.

Stel eenduidige organisatiedoelen vast

De te realiseren organisatiedoelen vormen het uitgangspunt voor alle activiteiten op het gebied van risicomanagement. Alle risicomanagementactiviteiten dragen bij aan het realiseren van de organisatiedoelen. Het effectief beheersen van risico's is daarom alleen mogelijk wanneer de te realiseren organisatiedoelen op een eenduidige manier zijn gedefinieerd en wanneer alle betrokken bestuurders, lijnmanagers, experts en de ondersteunende functionarissen bekend zijn met de organisatiedoelen.

Het is aan de organisatie om vast te stellen wat de organisatiedoelen zijn, bijvoorbeeld de primaire processen, en waar door middel van risicomanagement aan wordt bijgedragen.

Zorg voor een duidelijke verdeling van taken en verantwoordelijkheden

Het effectief beheersen van risico's is alleen mogelijk als een duidelijke verdeling van taken en verantwoordelijkheden is vastgesteld tussen de bestuurders, de lijnmanagers, de experts, en de ondersteunende en toezichthoudende functies. Hierbij geldt het algemene uitgangspunt dat de betrokken bestuurders eindverantwoordelijk zijn voor de realisatie van de organisatiedoelen en voor de beheersing van de daarmee samenhangende risico's. Deze bestuurders definiëren afgeleide taken en verantwoordelijkheden en wijzen deze toe aan het lijnmanagement. Binnen het lijnmanagement kunnen we vanuit het digitale perspectief onderscheid maken tussen informatie-eigenaren, systeem-eigenaren, risico-eigenaren en maatregeleigenaren.

Voor alle informatie binnen een organisatie is door het bestuur een informatie-eigenaar aangewezen die zorg draagt voor de betrouwbaarheid van die informatie. Een van die zorgtaken bij informatie is het inzichtelijk maken van de risico's rondom die informatie. Een informatie-eigenaar is risico-eigenaar voor de in kaart gebrachte risico's. Binnen dit beleid wordt voor de leesbaarheid alleen de term informatie-eigenaar gehanteerd. De eigenaar voor mitigerende maatregelen is daarnaast niet per se dezelfde persoon als de eigenaar voor de risico's waar die maatregelen betrekking op hebben. Zo is de ICT-manager een voor de hand liggende maatregeleigenaar voor de ICT-gerelateerde maatregelen. Een maatregeleigenaar is slechts verantwoordelijk voor het correct implementeren van een maatregel. Dat een risico middels passende maatregelen wordt gemitigeerd blijft de verantwoordelijkheid van de risico-eigenaar.

Dit beleid hanteert de term informatie-eigenaar. Hoe informatie-eigenaarschap daadwerkelijk wordt ingericht, is aan de organisatie. Dit kan ook via proceseigenaarschap of systeemeigenaarschap gebeuren. Het doel is dat voor iedere informatie duidelijk is wie daarvan de eigenaar is.

Voor de organisatie is een CISO aangesteld die een adviserende, coördinerende en controlerende rol heeft binnen het risicomanagementproces.

Adviseren – Gevraagd en ongevraagd advies geven over risicomanagement binnen de organisatie, over bijvoorbeeld actuele dreigingen, actoren en hun handelen, kwetsbaarheden in applicaties en systemen en het beheersen van risico's.

Coördineren – Het uitvoeren van een specifieke opdracht op het gebied van risicomanagement waarbij de verantwoordelijkheid bij iemand anders ligt, zoals bijvoorbeeld het opstellen van het risicomanagementbeleid, het beheren van het ISMS, het begeleiden van risicoanalyses en het bijhouden van een register voor risico's en maatregelen.

Controleren – Nagaan of de organisatie zich houdt aan het risicomanagementbeleid, met informatie-eigenaren in gesprek over eventuele tekortkomingen en hierover rapporteren richting het bestuur.

Voor het uitvoeren van de risicomanagementtaken stellen de bestuurders budget en de noodzakelijke hulpmiddelen ter beschikking en zorgen ze voor een passend mandaat.

Tot slot is het belangrijk om duidelijke afspraken te maken over de verdeling van taken en verantwoordelijkheden bij geconstateerde incidenten. Aan wie deze worden gerapporteerd en wie bevoegd is om in te grijpen. De afspraken die worden gemaakt over risicomanagement van de digitale weerbaarheid worden vastgelegd op een manier die door iedereen wordt onderkend.

Zorg voor inzicht in de organisatie en in de informatievereisten

Om de digitale weerbaarheid van de organisatie en de betrouwbaarheid van de noodzakelijke informatie te kunnen borgen, is inzicht nodig in de processen binnen de organisatie. Ook is het belangrijk om vast te stellen van welke informatie en applicaties de organisatie afhankelijk is en in welke mate.

Het is belangrijk om inzicht te hebben in hoe en waar informatie binnen de organisatie wordt verwerkt en wat de betrouwbaarheidseisen zijn voor de informatie. Het moet duidelijk zijn door wie deze eisen zijn vastgesteld en wat de feitelijke betrouwbaarheid van de informatie is. Gezamenlijke aandacht is nodig voor mogelijke kwetsbaarheden die kunnen ontstaan op de koppelvlakken tussen organisatieonderdelen.

Realiseer en behoud een open cultuur

Effectief risicomanagement is slechts een illusie wanneer bestuurders, lijnmanagers en experts zich geremd voelen om eventuele dreigingen, risico's, kwetsbaarheden en incidenten te melden. Dit vraagt dat de bestuurders en lijnmanagers zich continu inzetten voor het realiseren en behouden van een open cultuur. Zij tonen publiekelijk hun waardering voor individuen die bijvoorbeeld een kwetsbaarheid of incident rapporteren. De focus ligt daarbij altijd op het leren en het continue verbeteren van de digitale weerbaarheid.

Beleidsregels voor principes en randvoorwaarden	
1.	Het bestuur zorgt voor een open cultuur waarin alle lijnmanagers, experts en ondersteuners zich niet geremd voelen om dreigingen, risico's en kwetsbaarheden te melden. Zij tonen publiekelijk hun waardering voor individuen die bijvoorbeeld een kwetsbaarheid rapporteren.
2.	Het bestuur specificeert de organisatiedoelen op een zodanige manier dat de realisatie ervan navolgbaar is.
3.	Het bestuur legt de onderlinge verdeling van taken en verantwoordelijkheden vast. Daarbij stellen zij vast wie informatie-eigenaren zijn, wat de daarbij behorende zorgtaken zijn en stellen zij een CISO aan.
4.	Het bestuur zorgt ervoor dat de risicomanagementactiviteiten volgens een gestructureerd proces worden uitgevoerd. Dat gebeurt door middel van het toepassen van dit beleid en de bijbehorende implementatierichtlijn.
5.	Het bestuur integreert risicomanagementactiviteiten, rapportages en besprekingen in de reguliere managementactiviteiten. Separate risicorapportages en besprekingen worden vermeden. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 9 – Registreer risico's en bepaal risicobeeld.*
6.	Het bestuur volgt dit beleid en draagt het actief uit. Afwijkingen, inclusief onderbouwing, wordt door of namens het bestuur geregistreerd. Deze registratie wordt beschikbaar gehouden voor toezichthoudende instanties en andere belanghebbenden.
7.	Het bestuur zorgt ervoor dat de informatieverwerking is gedocumenteerd.
8.	Het bestuur zorgt ervoor dat alle lijnmanagers, experts en ondersteuners over de kennis, middelen en mandaat beschikken die zij nodig hebben voor het uitvoeren van de aan het toebedeelde risicomanagementactiviteiten.

3 Realisatie van organisatiedoelen

Neem goede dienstverlening en organisatiedoelen als uitgangspunt

De goede dienstverlening aan burgers en ondernemers wordt in dit beleid gezien als de ultieme ambitie van de bestuurders, lijnmanagers, specialisten en ondersteuners. De realisatie van deze ambitie is onder andere afhankelijk van het ongestoord functioneren van de organisatie en van de realisatie van de organisatiedoelen. Daarvan afgeleid stellen de bestuurders de criteria vast voor de betrouwbaarheid van de voor de organisatie noodzakelijke informatie. De wijze waarop de vereiste betrouwbaarheid van de relevante informatie wordt behaald, hangt af van de manier waarop risicomanagement voor de digitale weerbaarheid wordt ingevuld.

Beleidsregels voor realisatie van organisatiedoelen	
9.	Het bestuur stelt vast dat de organisatiedoelen bijdragen aan de betrouwbare dienstverlening aan burgers en ondernemers.

4 Ongestoord functionerende organisatie

Beschouw betrouwbare informatie als randvoorwaarde

Bestuurders en lijnmanagers stellen in overleg met elkaar vast welke informatie en applicaties van belang zijn voor de realisatie van de organisatiedoelen. Ook bepalen zij wat de betrouwbaarheidseisen zijn voor die informatie wat betreft beschikbaarheid, integriteit en vertrouwelijkheid.

Beleidsregels voor een ongestoord functionerende organisatie	
10.	Het bestuur en lijnmanagers stellen gezamenlijk vast welke informatie vereist is voor het ongestoord functioneren van de organisatie en de realisatie van de organisatiedoelen.
11.	Het bestuur en lijnmanagers stellen gezamenlijk vast welke applicaties vereist zijn voor het ongestoord functioneren van de organisatie en de realisatie van de organisatiedoelen.
12.	Het bestuur en lijnmanagers stellen gezamenlijk de eisen vast voor de beschikbaarheid, integriteit en vertrouwelijkheid van de voor de organisatie relevante informatie.

5 Bedreigingen voor de betrouwbaarheid van informatie

Verkrijg inzicht in actoren en dreigingen

Voor het borgen van de betrouwbaarheid van de voor de organisatie noodzakelijke informatie, is het van cruciaal belang om inzicht te krijgen in wie mogelijk een actie zou kunnen uitvoeren om de betrouwbaarheid van de informatie te verstoren en op welke manier zij dat zouden kunnen doen. Het verkrijgen van inzicht in de zogenaamde actoren en hun aanvalsmethoden, ofwel inzicht in de dreigingen, is bepalend voor de manier waarop met die dreigingen wordt omgegaan.

Beleidsregels voor inzicht in actoren en dreigingen	
13.	Informatie-eigenaren stellen vast welke dreigingen mogelijk verstorend kunnen zijn voor de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatie waar zij eigenaar van zijn. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 7 – Voer risicoanalyses uit.*
14.	Het bestuur stelt in overleg met de CISO en de informatie-eigenaren vast welke actoren het voorzien kunnen hebben op het verstoren van de betrouwbaarheid van de voor de organisatie relevante informatie. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 7 – Voer risicoanalyses uit.*

Verkrijg inzicht in kwetsbaarheden en risico's

Wanneer een dreiging leidt tot een daadwerkelijke verstoring van de betrouwbaarheid van de relevante informatie, spreken we van een incident. In hoeverre de organisatie weerbaar is tegen dergelijke incidenten, hangt af van de effectiviteit van de door de organisatie getroffen maatregelen. Wanneer een maatregel ontbreekt, in opzet ontoereikend is, of niet wordt uitgevoerd zoals bedoeld, dan is er sprake van een kwetsbaarheid. Als een dreiging in combinatie met een kwetsbaarheid gevolgen kan hebben voor de betrouwbaarheid van de voor de organisatie relevante informatie en daarmee voor de realisatie van de organisatiedoelen, dan is er sprake van een risico. Maatregelen kunnen worden getroffen om incidenten te voorkomen, om incidenten tijdig te detecteren en om de gevolgen van incidenten tot op een acceptabel niveau te reduceren. Het bestuur bepaalt wat volgens hen een acceptabel niveau is voor de organisatie waarvoor zij verantwoordelijk is.

Bestuurders en lijnmanagers moeten zich bewust zijn van eventuele kwetsbaarheden in de digitale weerbaarheid van de organisatie en de gevolgen daarvan. Dit bewustzijn wordt verkregen door samen met specialisten en ondersteuners regelmatig en op een gestructureerde manier te beoordelen of de eerder getroffen maatregelen werken zoals bedoeld en of deze de beoogde effecten realiseren. De resultaten van deze beoordelingen worden gerapporteerd aan en besproken met de bestuurders en lijnmanagers die verantwoordelijk zijn voor het ongestoord functioneren van de organisatie en de realisatie van de organisatiedoelen. Op basis van de verkregen inzichten en het resultaat van de besprekingen met experts en ondersteuners, nemen bestuurders en lijnmanagers besluiten over de door hen uit te voeren interventies, waaronder de eventuele introductie van nieuwe maatregelen of de aanpassing van bestaande maatregelen.

Beleidsregels voor inzicht in kwetsbaarheden en risico's	
15.	Informatie-eigenaren stellen per risico vast welke maatregelen moeten worden getroffen om incidenten te voorkomen, deze vroegtijdig te detecteren en om de gevolgen daarvan te reduceren. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 7 – Voer risicoanalyses uit.*
16.	Informatie-eigenaren en maatregeleigenaren stellen gezamenlijk regelmatig de correcte werking van de maatregelen vast om de feitelijke weerbaarheid van de organisatie te kunnen bepalen. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 10 – Monitor risico's, maatregelen en proces.*
17.	Informatie-eigenaren en maatregeleigenaren bespreken kwetsbaarheden; maatregelen die ontbreken, of niet werken zoals bedoeld. Zij bespreken ook de oorzaken en gevolgen daarvan en besluiten op basis van het verkregen inzicht of en welke interventies nodig zijn ter versterking van de weerbaarheid van de organisatie. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 10 – Monitor risico's, maatregelen en proces.*

Naast de bovengenoemde gestructureerde beoordeling van de werking van de eerder getroffen maatregelen, is het ook erg belangrijk dat de betrokken bestuurders en lijnmanagers een open cultuur promoten zoals eerder in dit beleid is toegelicht. Een cultuur waarin iedereen die betrokken is bij de organisatie zich vrij voelt om eventuele kwetsbaarheden zo snel mogelijk te melden zodat de verantwoordelijke bestuurders en lijnmanagers tijdig correctieve maatregelen kunnen treffen.

Bepaal de rangschikking van de geïdentificeerde risico's

Niet alle risico's zijn voor de organisatie even belangrijk. Deze kunnen verschillen qua kans dat deze zich voordoen en qua gevolgen. Bij het bepalen van de kans van een risico worden de achterliggende actoren en de effectiviteit van bestaande maatregelen in overweging genomen. Bij het bepalen van de gevolgen van een risico wordt altijd eerst gekeken naar de consequenties voor de te realiseren organisatiedoelen en andere zaken die voor de organisatie de hoogste prioriteit hebben.

Het is een illusie te veronderstellen dat alle incidenten voorkomen kunnen worden en dat de gevolgen daarvan tot nul gereduceerd kunnen worden. Net zomin beschikken bestuurders en lijnmanagers over onuitputbare middelen om de betrouwbaarheid van de informatie en de realisatie van de organisatiedoelen te borgen. Het is daarom belangrijk dat informatie-eigenaren de voor de organisatie relevante risico's navolgbaar en gestructureerd documenteren en zorgvuldig prioriteren.

Het bestuur bepaalt vervolgens wat voor de organisatie een acceptabel niveau is van risicoblootstelling, ofwel wat hun risicobereidheid is. Ook bepaalt het bestuur wie namens hen en onder welke voorwaarden akkoord mag geven voor het accepteren van risico's die de risicobereidheid overstijgen.

Wanneer risico's worden geaccepteerd, zeker wanneer daarbij de risicobereidheid wordt overstegen, wordt dat besluit met onderbouwing op een navolgbare manier gedocumenteerd. Dit vormt de basis voor het informeren van toezichthouders en andere belanghebbenden en voor toekomstige heroverwegingen en herzieningen van eerder genomen besluiten. Wanneer de gevolgen van een risico niet aanvaardbaar worden bevonden, moet worden nagedacht over het treffen van aanvullende maatregelen ter verlaging van de impact van het risico. Hierover meer in het volgende hoofdstuk.

Beleidsregels voor het rangschikken van risico's	
18.	Informatie-eigenaren stellen vast op welke manier risico's worden gerangschikt. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 4 – Verkrijg inzicht in eigen situatie.*
19.	Het bestuur stelt de risicobereidheid vast. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 4 – Verkrijg inzicht in eigen situatie.*
20.	Het bestuur stelt vast wie akkoord mag geven voor het accepteren van risico's die de risicobereidheid overstijgen. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 4 – Verkrijg inzicht in eigen situatie.*
21.	Het bestuur legt gemaakte afspraken over het rangschikken van risico's en het accepteren van risico's vast en ziet erop toe dat deze worden nageleefd.
22.	Informatie-eigenaren rangschikken de geïdentificeerde risico's en leggen dit op een gestructureerde en navolgbare manier vast. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 7 - Voer risicoanalyses uit, 8 - Bepaal risicobehandeling en 9 – Registreer risico's en bepaal risicobeeld.*

6 Het borgen van de betrouwbaarheid van informatie

Tref maatregelen op basis van kans en gevolgen

Er bestaan verschillende soorten maatregelen die door de verantwoordelijke bestuurders en informatie-eigenaren kunnen worden ingezet ter borging van de betrouwbaarheid van de voor de organisatie relevante informatie, het ongestoord functioneren van de organisatie en het uiteindelijk realiseren van de organisatiedoelen. Het doel van deze maatregelen is incidenten te voorkomen, deze vroegtijdig te ontdekken en om de schade als gevolg daarvan tot op een aanvaardbaar niveau te beperken en het spoedig herstel na het optreden van een incident te bevorderen.

Het onderstaande overzicht[3] beschrijft met behulp van een voorbeeld de relatie en samenhang tussen de verschillende elementen van een risico en de bijbehorende mogelijke maatregelen.

Risico			
Oorzaken		**Ongewenste gebeurtenis**	**Gevolgen**
Actor	*Kwetsbaarheid*	*Dreiging*	*Impactcategorieën*
Hacker met kennis en motivatie	Achterstallige software update	Ransomware aanval waardoor beschikbaarheid informatie is gecompromitteerd	Niet realiseren van doelen Financiële schade Reputatieschade
Maatregelen			
Preventief (aanpakken oorzaken)		**Detectief** (vroegtijdig ontdekken incident)	**Repressief** (aanpakken gevolgen)
Patchen		Monitoren door een SOC	*Back-up, herstelprocedures*

Door middel van het op een gestructureerde manier inschatten van de kans en de gevolgen van risico's, kan worden vastgesteld of de risicoblootstelling als gevolg van een bepaalde dreiging wel of niet aanvaardbaar zijn. Dit wordt verder in de implementatierichtlijn toegelicht. Als wordt geconcludeerd dat de gevolgen van een risico niet aanvaardbaar zijn, dan moeten op basis van een zorgvuldige afweging van baten en lasten aanvullende maatregelen worden getroffen om de kans en/of de gevolgen van een risico tot op een aanvaardbaar niveau te verlagen. Deze maatregelen kunnen organisatorisch, technisch en mensgericht van aard zijn.

Het kan voorkomen dat de gevolgen van een risico niet acceptabel worden geacht en geen maatregelen kunnen worden geïmplementeerd om de risicoblootstelling terug te brengen tot op een acceptabel niveau. Bijvoorbeeld door ontoereikende middelen of omdat de investeringen voor die maatregelen de baten overstijgen. In dat geval kan worden besloten om de onderliggende activiteit te staken, of om de financiële gevolgen van mogelijke incidenten aan anderen over te dragen. Bijvoorbeeld via een verzekering.

3 Dit overzicht maakt gebruik van de bowtie-methode om een risico te beschrijven.

Tref organisatorische, technische en mensgerichte maatregelen

Om de risicoblootstelling van een dreiging tot op een acceptabel niveau te beperken, zijn meestal meerdere en verschillende soorten maatregelen tegelijkertijd nodig. Daarbij worden ruwweg organisatorische, technische en mensgerichte maatregelen onderscheiden. De zorgvuldige verdeling van taken en bevoegdheden tussen bestuurders, lijnmanagers, experts en ondersteuners die een rol hebben bij het managen van risico's op het gebied van de digitale weerbaarheid, is een voorbeeld van een organisatorische maatregel. Andere voorbeelden van organisatorische maatregelen zijn het opstellen en gebruiken van een werkinstructie, of het gebruik van een register van door de organisatie gebruikte applicaties. Het tijdig actualiseren van de beveiliging van door de organisatie gebruikte software is een technische maatregel. Het trainen van lijnmanagers en experts ter vergroting van hun kennis en risicobewustzijn is een voorbeeld van een mensgerichte maatregel.

Beleidsregels voor het treffen van maatregelen

23. Informatie-eigenaren zien erop toe, dat voor alle risico's die de risicobereidheid overstijgen, een set van maatregelen wordt opgesteld ter verlaging van de kans van die risico's, voor de detectie van incidenten en ter beperking van de gevolgen van die risico's.

    Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 8 – Bepaal risicobehandeling.

24. Informatie-eigenaren zien erop toe dat de maatregelen zodanig specifiek worden gedocumenteerd, zodat de wijze van implementatie duidelijk is en deze op correcte uitvoering getoetst kunnen worden.

    Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 8 – Bepaal risicobehandeling en 9 - Registreer risico's en bepaal risicobeeld.

25. Informatie-eigenaren zien erop toe dat de haalbaarheid van voorgestelde maatregelen is vastgesteld en dat kosten en baten zijn afgewogen alvorens tot implementatie wordt overgegaan.

    Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 8 - Bepaal risicobehandeling.

26. Informatie-eigenaren zien erop toe dat de maatregelen worden gecommuniceerd naar de verantwoordelijken die de maatregelen moeten implementeren en uitvoeren.

    Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 8 - Bepaal risicobehandeling.

7 Het borgen van de effectiviteit van maatregelen

Monitor veranderingen in het dreigingsbeeld

De digitale dreigingen waaraan organisaties blootstaan veranderen voortdurend en in een hoog tempo. Eerder getroffen maatregelen kunnen na verloop van tijd achterhaald of misschien niet meer noodzakelijk zijn. Het is daarom belangrijk om de veranderingen in het dreigingsbeeld en de gevolgen voor de risicoblootstelling nauwlettend te volgen om onbewuste en ongewenste risicoblootstelling te voorkomen.

Beleidsregels voor monitoring van het dreigingsbeeld	
27.	Het bestuur ziet erop toe dat regelmatig en op gestructureerde manier wordt vastgesteld of veranderingen zijn opgetreden in het dreigingsbeeld van de organisatie. Daarbij moet worden beoordeeld of eerder genomen besluiten over het wel of niet treffen van maatregelen nog altijd gelden, of bijgesteld moeten worden. Informatie-eigenaren stellen aanvullend vast of eerder getroffen maatregelen nog altijd toereikend zijn, bijgesteld moeten worden of overbodig zijn geworden. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 6 – Aanleiding voor een risicoanalyse en 10 - Monitor risico's, maatregelen en proces.*
28.	Het bestuur ziet erop toe dat minimaal eenmaal per jaar wordt geïnventariseerd of en welke incidenten zich binnen de organisatie daadwerkelijk hebben voorgedaan en of deze aanleiding geven tot het bijstellen van het dreigingsbeeld, of tot het aanpassen van eerder getroffen maatregelen. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 6 – Aanleiding voor een risicoanalyse en 10 - Monitor risico's, maatregelen en proces.*

Monitor de effectiviteit van getroffen maatregelen

In het algemeen geldt dat de effectiviteit van bestaande maatregelen na verloop van tijd afneemt wanneer de correcte uitvoering ervan niet wordt getoetst. Als niet goed werkende maatregelen niet of niet tijdig worden opgemerkt, kan sprake zijn van onbewuste en ongewenste risicoblootstelling. In het meest ernstige geval wordt het niet goed werken van bestaande maatregelen pas geconstateerd bij een incident, nadat de schade is geleden. Om niet goed werkende maatregelen te kunnen detecteren en om tijdig te kunnen bijsturen, toetsen informatie-eigenaren en maatregeleigenaren op een gestructureerde manier of eerder getroffen maatregelen worden uitgevoerd zoals bedoeld en of die maatregen het beoogde effect bereiken.
Als dat niet het geval blijkt te zijn, wordt onderzocht wat daarvan de oorzaak is om passende interventies te kunnen bepalen.

Beleidsregels voor monitoring van maatregelen	
29.	Informatie-eigenaren en maatregeleigenaren zien gezamenlijk erop toe dat regelmatig op gestructureerde manier wordt vastgesteld of eerder geïmplementeerde maatregelen nog altijd effectief en efficiënt zijn en of deze correct worden uitgevoerd. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 10 - Monitor risico's, maatregelen en proces.*
30.	Als een maatregel onvoldoende effectief is of niet correct wordt uitgevoerd, dan is er sprake van een kwetsbaarheid. Informatie-eigenaren en maatregeleigenaren zien gezamenlijk erop toe dat de oorzaken en gevolgen van bestaande kwetsbaarheden worden vastgesteld en dat op basis van het verkregen inzicht een verbeterplan wordt opgesteld en uitgevoerd. Zij zien toe op de voortgang van uitvoering van het verbeterplan. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 10 - Monitor risico's, maatregelen en proces.*

Monitor wijzigingen in opzet van de organisatie

Mogelijke wijzigingen in de samenstelling van de organisatie of in de formele hiërarchische structuur kunnen impact hebben op de verdeling van taken, verantwoordelijkheden en bevoegdheden voor risicomanagement voor digitale weerbaarheid van de organisatie. Dit geldt ook voor wijzigingen in de activiteiten en in de doelstelling van de organisatie, of voor wijzigingen in het gebruik van informatie en applicaties door de organisatie. Daarnaast kunnen deze wijzigingen gevolgen hebben voor de risicoblootstelling of voor de weerbaarheid van de organisatie.

Beleidsregels voor monitoring van wijziging in organisatieprocessen	
31.	Het bestuur ziet erop toe dat regelmatig op gestructureerde manier wordt vastgesteld of wijzigingen in de samenstelling of in de aansturing van de organisatie gevolgen hebben voor de risicomanagementactiviteiten van de organisatie. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 6 – Aanleiding voor een risicoanalyse en 10 - Monitor risico's, maatregelen en proces.*
32.	Het bestuur borgt dat wijzigingen in de organisatieprocessen, in gebruikte informatie of applicaties tenminste jaarlijks, of zoveel vaker als nodig worden gemonitord en beoordeeld op de gevolgen voor de risicomanagementactiviteiten en de risicoblootstelling van de organisatie. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 6 – Aanleiding voor een risicoanalyse.*

8 Het afwegen van belangen en besluiten tot bijsturing

Rapporteer veranderingen, kwetsbaarheden en risicoblootstelling

Veranderingen in het dreigingsbeeld die leiden tot nieuwe risico's worden evenals de effectiviteit van bestaande maatregelen regelmatig en op een gestructureerde manier gerapporteerd aan de bestuurders en lijnmanagers die verantwoordelijk zijn voor de realisatie van de organisatiedoelen en voor de beheersing van de daarmee samenhangende risico's. Zo worden zij bewust gemaakt van de risicoblootstelling en de feitelijke digitale weerbaarheid van de organisatie. Met andere woorden, of zij door middel van de al getroffen maatregelen in staat zijn om de kans om getroffen te worden door incidenten en de gevolgen daarvan tot op een aanvaardbaar niveau te reduceren. Zodanig dat de betrouwbaarheid van de voor de organisatie relevante informatie en het ongestoord functioneren van de organisatie geborgd kan worden.

De risicorapportages zijn integraal onderdeel van de reguliere managementrapportages. Alleen als tussentijds significante veranderingen optreden in het dreigingsbeeld of in de risicoblootstelling van de organisatie, dan wordt dit ad-hoc en separaat gerapporteerd aan de verantwoordelijke bestuurders en lijnmanagers.

Bespreek de risicoblootstelling en de digitale weerbaarheid

De risicorapportages zijn belangrijke input voor de periodieke gesprekken tussen bestuurders, lijnmanagers, experts en ondersteuners over de risicoblootstelling en de digitale weerbaarheid van de organisatie. Tijdens deze risicodialogen wordt onder andere besproken of de situatie acceptabel is, of dat bijsturing op organisatorisch, technisch of mensgericht niveau noodzakelijk wordt geacht. Dit is afhankelijk van de oorzaken en de gevolgen van geconstateerde risico's en kwetsbaarheden.
In de rapportages en tijdens de bespreking ervan staat telkens de toereikendheid van de digitale weerbaarheid van de organisatie ten behoeve van het behalen van organisatiedoelen centraal.

Weeg opbrengsten en investeringen zorgvuldig af

De middelen waarover bestuurders en lijnmanagers kunnen beschikken voor de borging van de digitale weerbaarheid van organisatie en de betrouwbaarheid van de daarvoor noodzakelijke informatie zijn beperkt beschikbaar. Zij moeten daarom keuzes maken over het bijsturen op de uitvoering van de bestaande maatregelen, over het introduceren van nieuwe maatregelen of het opheffen van bestaande maatregelen. Deze keuzes worden gemaakt op basis van de via de risicorapportages en de risicodialogen verkregen inzichten. Daarbij wordt rekening gehouden met de extra kosten van de beoogde bijsturing in relatie tot de baten gezien vanuit de beoogde organisatiedoelen en de goede dienstverlening aan burgers en ondernemers.

Beleidsregels voor rapportage en escalatie

33.	Het bestuur richt een rapportage en escalatiestructuur in voor de organisatie. Zij beleggen binnen deze structuur de verantwoordelijkheid voor het beoordelen van de rapportages inzake het monitoren van het dreigingsbeeld, het monitoren van de risico's en van de maatregelen en voor het risicogebaseerd inzetten van interventies om de digitale weerbaarheid op het gewenste niveau te krijgen en te houden. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 9 - Registreer risico's en bepaal risicobeeld en 10 – Monitor risico's, maatregelen en proces.*
34.	Het bestuur borgt dat veranderingen in het dreigingsbeeld, net als de effectiviteit van bestaande maatregelen regelmatig en gestructureerd aan henzelf en de informatie-eigenaren worden gerapporteerd. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 6. – Aanleiding voor een risicoanalyse en hoofdstuk 9 - Registreer risico's en bepaal risicobeeld.*
35.	Het bestuur borgt dat de risicorapportages volledig worden geïntegreerd in de bestaande reguliere managementrapportages. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 9 - Registreer risico's en bepaal risicobeeld.*
36.	Het bestuur borgt dat plotselinge significante wijzigingen in de risicoblootstelling van de organisatie als gevolg van wijzigingen in het dreigingsbeeld, of door geconstateerde kwetsbaarheden zo snel mogelijk op ad-hoc basis aan henzelf en de informatie-eigenaren worden gerapporteerd. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 6 – Aanleiding voor een risicoanalyse en 10 - Monitor risico's, maatregelen en proces.*
37.	Het bestuur borgt dat de risicorapportages worden besproken tijdens de periodieke risicodialoog tussen henzelf, informatie-eigenaren, experts en ondersteuners, als onderdeel van de bespreking van de reguliere managementrapportages. *Voor een verdere toelichting, zie Implementatierichtlijn hoofdstuk 9 - Registreer risico's en bepaal risicobeeld.*
38.	Het bestuur borgt dat zijzelf en informatie-eigenaren weloverwogen en risicogebaseerd besluiten nemen over het al dan niet toepassen van interventies voor het verstevigen van de digitale weerbaarheid van de organisatie wanneer de risicorapportage daartoe aanleiding geeft. Zij borgen dat deze besluiten op een navolgbare manier worden vastgelegd.
39.	Het bestuur wijst de verantwoordelijkheid en het mandaat voor het uitvoeren van interventies toe aan een specialist binnen de organisatie. Deze rapporteert over de uitvoering en voortgang van de interventies aan het bestuur en de informatie-eigenaren.
40.	Het bestuur ziet erop toe dat in het kader van Coordinated Vulnerability Disclosure (CVD), voorheen 'responsible disclosure', bij het NCSC melding wordt gemaakt van een aangetroffen kwetsbaarheid in een applicatie of IT-systeem van de Rijksoverheid.

9 Risicomanagement en externe partijen

Het is heel aannemelijk dat een organisatie vroeg of laat te maken krijgt met de samenwerking met een andere organisatie. Bij die samenwerking kunnen risico's ontstaan die beheerst moeten worden. Hoewel de beheersing van dat soort risico's op de manier aangepakt kan worden zoals in de vorige hoofdstukken beschreven is, is een aantal specifieke punten te benoemen die om aandacht vragen.

Ketens

Om op een goede manier mee te kunnen werken aan een ketendoel, is het noodzakelijk dat een organisatie om te beginnen weet van welke ketens de organisatie onderdeel is. Iedere organisatie dient daar dus een centrale registratie van te hebben. Voor iedere keten waar een organisatie bij aangesloten is, dient binnen de organisatie een aanspreekpunt beschikbaar te zijn.

Bij een keten[4] werken meerdere organisaties samen aan een gezamenlijk doel, waarbij iedere organisatie een eigen inbreng heeft in het behalen van dat doel. Om helderheid te krijgen in de werking van de keten, is het belangrijk om vast te leggen wat het aandeel is van iedere ketenpartner in het geheel en welke afspraken daarbij worden gemaakt.

Omdat bij een keten meerdere organisaties betrokken zijn, is het belangrijk om vast te stellen wie de eindverantwoordelijkheid draagt over de keten. Deze eindverantwoordelijke(n) kunnen een ketenmanager aanstellen om de dagelijkse zorg voor de keten op te pakken. De ketenpartners nemen een gezamenlijk besluit over het mandaat van al deze personen. Een beslissing binnen een keten kan namelijk gevolgen hebben voor een andere organisatie dan waar deze personen werkzaam zijn.

Binnen een keten wordt mogelijk informatie uitgewisseld. Daarbij is het denkbaar dat de eisen die een ketenpartner stelt aan beschikbaarheid, integriteit en vertrouwelijkheid van informatie niet overeenkomen met de eisen vanuit een andere ketenpartner. Een incident met informatie bij een ketenpartner kan leiden tot problemen bij een andere ketenpartner. De kans daarop wordt vergroot als informatie wordt verwerkt volgens een lagere classificatie dan wat een andere ketenpartner noodzakelijk vindt. Dat kan leiden tot een vertrouwensbreuk binnen de keten, wat het behalen van het ketendoel in gevaar brengt. Voor een goede ketensamenwerking is het daarom belangrijk dat alle ketenpartners informatie verwerken volgens een classificatie waar iedere ketenpartner mee akkoord is.

Naast de risico's die een ketenpartner inzichtelijk maakt en beheerst voor de activiteiten die zij uitvoeren voor en binnen de keten, dienen ook de risico's voor de gehele keten inzichtelijk te worden gemaakt en te worden beheerst. Dat betekent het uitvoeren van ketenbrede risicoanalyses en het registeren en afhandelen van deze risico's op een wijze die voor iedere ketenpartner duidelijk, acceptabel en uitvoerbaar is. Risico's die vanuit een ketenpartner worden geïdentificeerd en betrekking hebben op de keten, worden met de relevante andere ketenpartners besproken en gezamenlijk opgepakt.

Bestuurders van ketenpartners bespreken periodiek de effectiviteit en efficiëntie van de risicobeheersing binnen de keten en voeren verbeteringen door waar nodig.

4 Naar de definitie van een keten volgens NORA, zoals beschreven in https://www.noraonline.nl/images/noraonline/c/cb/Ketens_de_Baas_tweede_druk.pdf.

Beleidsregels voor monitoring van wijziging in organisatieprocessen	
41.	Iedere organisatie registreert voor zichzelf van welke ketens de organisatie onderdeel is en wie binnen de organisatie aanspreekpunt is voor die keten.
42.	Ketenpartners leggen de onderlinge afspraken over de inrichting en werking van de keten vast.
43.	Voor iedere keten wordt een ketenverantwoordelijke en eventueel een ketenmanager aangesteld. De ketenpartners nemen een gezamenlijk besluit over het mandaat van deze personen om beslissingen te nemen voor de keten.
44.	Ketenpartners stellen gezamenlijk de classificatie vast van de informatie die binnen de keten verwerkt wordt, welke door alle ketenpartners gehanteerd dient te worden bij de verwerking van die informatie.
45.	Risico's voor een keten worden inzichtelijk gemaakt en besproken en opgepakt met relevante ketenpartners.
46.	Ketenpartners bespreken periodiek de effectiviteit en efficiëntie van de risicobeheersing binnen de keten en voeren verbeteringen door waar nodig.

Leveranciers

De samenwerking tussen een organisatie en een of meerdere leveranciers wordt ook wel een leverancierssketen genoemd. Echter, een belangrijk verschil met een keten zoals hierboven bedoeld, is het doel van de samenwerking. Bij een keten werken meerdere organisaties mee aan hetzelfde doel. Bij de samenwerking tussen een leverancier en een afnemer is dat anders. Een leverancier heeft geld verdienen of het behouden van bestaansrecht als doel en doet dat door het leveren van een betrouwbare dienst of een goed product. Voor de afnemer is die dienst of het product vanuit de leverancier slechts een middel om een eigen doel te behalen. Hoewel een leverancier en een afnemer met dezelfde risico's te maken kunnen hebben, zoals cybercriminaliteit, hebben ze vanwege een eigen doel ook te maken met eigen risico's.

Omdat vanuit de leverancierspositie dit beleid al kan worden toegepast, gaat dit hoofdstuk verder in op de positie van de afnemer.

Om de risico's rondom het gebruik van ICT-diensten en -producten vanuit leveranciers goed te kunnen beheersen, is het noodzakelijk dat de organisatie daar zicht op heeft. Per dienst of product is iemand binnen de organisatie aangewezen die zorg draagt voor de risicobeheersing rondom die dienst of dat product. Voordat een organisatie overgaat tot de aanschaf van zo'n dienst of product, worden eerst de risico's rond het gebruik daarvan in kaart gebracht. De beheersing van deze risico's wordt meegenomen in de aanschaf.

Bij het aangaan van een overeenkomst met een leverancier, wordt een zekere afhankelijkheid gecreëerd. Dat is niet erg, zolang deze afhankelijkheid geen onacceptabel risico vormt. Zo kan het onvoorzien wegvallen van een dienst of product voor problemen zorgen. Ook kunnen in de toekomst situaties ontstaan waardoor het gebruiken van een dienst of product niet meer acceptabel is. Daarom dient de organisatie per dienst of product vanuit een leverancier een actieplan te hebben, zodat zonder deze dienst of dit product de organisatiedoelen toch behaald kunnen worden (exit-strategie).

Beleidsregels voor leveranciersrisicomanagement	
47.	De organisatie heeft zicht op alle ICT-diensten en ICT-producten vanuit leveranciers.
48.	Binnen de organisatie is per afgenomen ICT-dienst of ICT-product een verantwoordelijke aangewezen, die zorg draagt voor de risico-beheersing rondom de dienst of het product.
49.	Voor de aanschaf van een ICT-dienst of ICT-product van een leverancier, worden eerst de risico's voor het gebruik daarvan in kaart gebracht en beheerst.
50.	Per dienst of product, welke nodig is voor het behalen van een organisatiedoel, is een actieplan beschikbaar hoe tijdelijk of definitief (exit-strategie) zonder deze dienst of dit product het organisatiedoel toch behaald kan worden.

10 Definities

De hieronder opgenomen definities zijn overgenomen uit gangbare documenten en bronnen die binnen de Rijksoverheid worden gehanteerd. Het is goed te beseffen dat in de praktijk soms meerdere definities worden gehanteerd voor een en hetzelfde begrip. Stem daarom binnen de organisatie zorgvuldig af, welke definitie wordt gehanteerd.

Begrip	Definitie
Betrouwbaarheid informatie	De betrouwbaarheid van informatie is een verzamelterm voor de beschikbaarheid, de integriteit en de vertrouwelijkheid van die informatie.
Cyberincident	1. (Samenhangende set van) gebeurtenissen of activiteiten die kunnen leiden tot verstoring van één of meer (digitale) processen. (Bron: Cybersecuritybeeld Nederland 2023) 2. (Samenhangende set van) gebeurtenissen of activiteiten die kunnen leiden tot verstoring van één of meer (digitale) processen. Dit omvat zowel een cyberaanval (moedwillige activiteit van een actor die is gericht op het met digitale middelen verstoren van een of meer digitale processen) als uitval als gevolg van bijvoorbeeld natuurlijke of technische oorzaken of menselijke fouten. (Bron: Nederlandse Cybersecuritystrategie 2022-2028)
Digitale weerbaarheid	Het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om incidenten te voorkomen en wanneer incidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging. Die kan helpen om de juiste technische, procedurele of organisatorische maatregelen te kiezen. (Bron: Nederlandse Cybersecuritystrategie 2022-2028)
Dreiging	1. Potentiële oorzaak van een ongewenst incident dat kan resulteren in schade aan een systeem of een organisatie. (Bron: ISO27002 -> ISO/IEC 27000:2018, 3.74) 2. Een opzettelijk of niet-opzettelijk gevaar dat kan leiden tot een cyberincident of een combinatie van gelijktijdige of opeenvolgende cyberincidenten. (Bron: Cybersecuritybeeld Nederland 2023) 3. Een cyberincident dat zich kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten. (Bron: Nederlandse Cybersecuritystrategie 2022-2028)
Kwetsbaarheid	Zwak punt van een bedrijfsmiddel of beheersmaatregel waar een of meer dreigingen gebruik van kunnen maken. (Bron: ISO27002 -> ISO/IEC 27000:2018, 3.77)
Maatregel	Maatregel die risico in stand houdt en/of wijzigt (Bron: ISO 27002)
Risico	1. De (combinatie van de) kans dat een dreiging leidt tot een cyberincident én de impact van het cyberincident op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid. (Bron: Cybersecuritybeeld Nederland 2023) 2. Effect van onzekerheid op (het behalen van) doelstellingen. (Bron: NEN-ISO 31000)
Risicobereidheid	Risicobereidheid, of risk appetite, beschrijft welke risico's het bestuur bereid is te accepteren in het licht van het bereiken van de organisatiedoelen en rekening houdend met de opgelegde (wettelijke) verplichtingen.
Risicoblootstelling	Mogelijk gevolgen van een risicogebeurtenis of incident voor de organisatie, rekening houdend met het risicobeperkende effect van de voor en door de organisatie getroffen maatregelen.
Risicomanagement	Gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's. (Bron: ISO 31000 + C11 3.2.)

11 Appendix A

Nr.	Beleidsregels	Implementatie richtlijn
Beleidsregels voor randvoorwaarden en principes		
1.	Het bestuur zorgt voor een open cultuur waarin alle lijnmanagers, experts en ondersteuners zich niet geremd voelen om dreigingen, risico's, kwetsbaarheden en incidenten te melden. Zij tonen publiekelijk hun waardering voor individuen die bijvoorbeeld een kwetsbaarheid of incident rapporteren.	
2.	Het bestuur specificeert de organisatiedoelen op een zodanige manier dat de realisatie ervan navolgbaar is.	n.v.t.
3.	Het bestuur legt de onderlinge verdeling van taken en verantwoordelijkheden vast. Daarbij stellen zij vast wie informatie-eigenaren zijn, wat de daarbij behorende zorgtaken zijn en stellen zij een CISO aan.	n.v.t.
4.	Het bestuur zorgt ervoor dat de risicomanagementactiviteiten volgens een gestructureerd proces worden uitgevoerd. Dat gebeurt door middel van het toepassen van dit beleid en de bijbehorende implementatierichtlijn.	n.v.t.
5.	Het bestuur integreert risicomanagementactiviteiten, rapportages en besprekingen in de reguliere management-activiteiten. Separate risicorapportages en besprekingen worden vermeden.	H9
6.	Het bestuur volgt dit beleid en dragen het actief uit. Afwijkingen, inclusief onderbouwing, wordt door het bestuur geregistreerd. Deze registratie wordt beschikbaar gehouden voor toezichthoudende instanties en andere belanghebbenden.	n.v.t.
7.	Het bestuur zorgt ervoor dat de informatieverwerking is gedocumenteerd.	n.v.t.
8.	Het bestuur zorgt ervoor dat alle lijnmanagers, experts en ondersteuners over de kennis en middelen beschikken die zij nodig hebben voor het uitvoeren van de aan het toebedeelde risicomanagementactiviteiten.	n.v.t.
Beleidsregels voor realisatie van organisatiedoelen		
9.	Het bestuur stelt vast dat de organisatiedoelen bijdragen aan de betrouwbare dienstverlening aan burgers en ondernemers.	n.v.t.
Beleidsregels voor ongestoord functionerende organisatie		
10.	Het bestuur en lijnmanagers stellen gezamenlijk vast welke informatie vereist is voor het ongestoord functioneren van de organisatie en de realisatie van de organisatiedoelen.	n.v.t.
11.	Het bestuur en lijnmanagers stellen gezamenlijk vast welke applicaties vereist zijn voor het ongestoord functioneren van de organisatie en de realisatie van de organisatiedoelen.	n.v.t.
12.	Het bestuur en lijnmanagers stellen gezamenlijk de eisen vast voor beschikbaarheid, integriteit en vertrouwelijkheid van de voor de organisatie relevante informatie.	n.v.t.
Beleidsregels voor inzicht in actoren en dreigingen		
13.	Informatie-eigenaren stellen vast welke dreigingen mogelijk verstorend kunnen zijn voor de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van de informatie waar zijn eigenaar van zijn.	H7
14.	Het bestuur stelt in overleg met de CISO en de informatie-eigenaren vast welke actoren het voorzien kunnen hebben op het verstoren van de betrouwbaarheid van de voor de organisatie relevante informatie.	H7
Beleidsregels voor inzicht in kwetsbaarheden en risico's		
15.	Informatie-eigenaren stellen per potentiële dreiging vast welke maatregelen moeten worden getroffen om incidenten te voorkomen, deze vroegtijdig te detecteren en om de gevolgen daarvan te reduceren.	H7
16.	Informatie-eigenaren en maatregeleigenaren stellen gezamenlijk regelmatig de correcte werking van de maatregelen vast om de feitelijke weerbaarheid van de organisatie te kunnen bepalen.	H10
17.	Informatie-eigenaren en maatregeleigenaren bespreken kwetsbaarheden; maatregelen die ontbreken, of niet werken zoals bedoeld. Zij bespreken ook de oorzaken en gevolgen daarvan en besluiten op basis van het verkregen inzicht of en welke interventies nodig zijn ter versterking van de weerbaarheid van de organisatie.	H10
Beleidsregels voor het rangschikken van risico's		
18.	Informatie-eigenaren stellen vast op welke manier risico's worden gerangschikt.	H4
19.	Het bestuur stelt de risicobereidheid vast.	H4

Nr.	Beleidsregels	Implementatie richtlijn
20.	Het bestuur stelt vast wie akkoord mag geven voor het accepteren van risico's die de risicobereidheid overstijgen.	H4
21.	Het bestuur legt gemaakte afspraken over het rangschikken van risico's en het accepteren van risico's vast en ziet erop toe dat deze worden nageleefd.	n.v.t.
22.	Informatie-eigenaren rangschikken de geïdentificeerde risico's en leggen dit op een gestructureerde en navolgbare manier vast.	H7 + H8 + H9
Beleidsregels voor het treffen van maatregelen		
23.	Informatie-eigenaren zien erop toe, dat voor alle risico's die de risicobereidheid overstijgen, een set van maatregelen wordt opgesteld ter verlaging van de kans van die risico's, voor de detectie van incidenten en ter beperking van de gevolgen van die risico's.	H8
24.	Informatie-eigenaren zien erop toe dat de maatregelen zodanig specifiek worden gedocumenteerd, zodat de wijze van implementatie duidelijk is en deze op correcte uitvoering getoetst kunnen worden.	H8 + H9
25.	Informatie-eigenaren zien erop toe dat de haalbaarheid van voorgestelde maatregelen is vastgesteld en kosten en baten zijn afgewogen alvorens tot implementatie wordt overgegaan.	H8
26.	Informatie-eigenaren zien erop toe dat de maatregelen worden gecommuniceerd naar de verantwoordelijken die de maatregelen moeten implementeren en uitvoeren.	H8
Beleidsregels voor monitoring van het dreigingsbeeld		
27.	Het bestuur ziet erop toe dat regelmatig en op gestructureerde manier wordt vastgesteld of veranderingen zijn opgetreden in het dreigingsbeeld van de organisatie. Daarbij moet worden beoordeeld of eerder genomen besluiten over het wel of niet treffen van maatregelen nog altijd gelden, of bijgesteld moeten worden. Informatie-eigenaren stellen aanvullend vast of eerder getroffen maatregelen nog altijd toereikend zijn, bijgesteld moeten worden of overbodig zijn geworden.	H10 + H6
28.	Het bestuur ziet erop toe dat minimaal eenmaal per jaar wordt geïnventariseerd of en welke incidenten zich binnen de organisatie daadwerkelijk hebben voorgedaan en of deze aanleiding geven tot het bijstellen van het dreigingsbeeld, of tot het aanpassen van eerder getroffen maatregelen.	H10 + H6
Beleidsregels voor monitoring van maatregelen		
29.	Informatie-eigenaren en maatregeleigenaren zien gezamenlijk erop toe dat regelmatig op gestructureerde manier wordt vastgesteld of eerder geïmplementeerde maatregelen nog altijd effectief en efficiënt zijn en of deze correct worden uitgevoerd.	H10
30.	Als een maatregel onvoldoende effectief is of niet correct wordt uitgevoerd, dan is er sprake van een kwetsbaarheid. Informatie-eigenaren en maatregeleigenaren zien gezamenlijk erop toe dat de oorzaken en gevolgen van bestaande kwetsbaarheden worden vastgesteld en dat op basis van het verkregen inzicht een verbeterplan wordt opgesteld en uitgevoerd. Zij zien toe op de voortgang van uitvoering van het verbeterplan.	H10
Beleidsregels voor monitoring van wijziging in organisatieprocessen		
31.	Het bestuur ziet erop toe dat regelmatig op gestructureerde manier wordt vastgesteld of wijzigingen in de samenstelling of in de aansturing van de organisatie gevolgen hebben voor de risicomanagementactiviteiten van de organisatie.	H10 + H6
32.	Het bestuur borgt dat wijzigingen in de organisatieprocessen, in gebruikte informatie of applicaties tenminste jaarlijks, of zoveel vaker als nodig worden gemonitord en beoordeeld op de gevolgen voor de risicomanagementactiviteiten en de risicoblootstelling van de organisatie.	H6
Beleidsregels voor rapportage en escalatie		
33.	Het bestuur richt een rapportage en escalatiestructuur in voor de organisatie. Zij beleggen binnen deze structuur de verantwoordelijkheid voor het beoordelen van de rapportages inzake het monitoren van het dreigingsbeeld, het monitoren van de risico's en van de maatregelen en voor het risicogebaseerd inzetten van interventies om de digitale weerbaarheid op het gewenste niveau te krijgen en te houden.	H9 + H10
34.	Het bestuur borgt dat veranderingen in het dreigingsbeeld, net als de effectiviteit van bestaande maatregelen regelmatig en gestructureerd aan henzelf en de lijnmanagers worden gerapporteerd.	H6 + H9
35.	Het bestuur borgt dat de risicorapportages volledig worden geïntegreerd in de bestaande reguliere managementrapportages.	H9

Nr.	Beleidsregels	Implementatie richtlijn
36.	Het bestuur borgt dat plotselinge significante wijzigingen in de risicoblootstelling van de organisatie als gevolg van wijzigingen in het dreigingsbeeld, of door geconstateerde kwetsbaarheden zo snel mogelijk op ad-hoc basis aan henzelf en de lijnmanagers worden gerapporteerd.	H10 + H6
37.	Het bestuur borgt dat de risicorapportages worden besproken tijdens de periodieke risicodialoog tussen henzelf, lijnmanagers, experts en ondersteuners, als onderdeel van de bespreking van de reguliere managementrapportages.	H9
38.	Het bestuur borgt dat zijzelf en lijnmanagers weloverwogen en risicogebaseerd besluiten nemen over het al dan niet toepassen van interventies voor het verstevigen van de digitale weerbaarheid van de organisatie wanneer de risicorapportage daartoe aanleiding geeft. Zij borgen dat deze besluiten op een navolgbare manier worden vastgelegd.	n.v.t.
39.	Het bestuur wijst de verantwoordelijkheid en het mandaat voor het uitvoeren van interventies toe aan een specialist binnen de organisatie. Deze rapporteert over de uitvoering en voortgang van de interventies aan het bestuur en de informatie-eigenaren.	n.v.t.
40.	Het bestuur ziet erop toe dat in het kader van Coordinated Vulnerability Disclosure (CVD), voorheen 'responsible disclosure', bij het NCSC melding wordt gemaakt van een aangetroffen kwetsbaarheid in een applicatie van de Rijksoverheid.	n.v.t.
Beleidsregels voor ketenrisicomanagement		
41.	Iedere organisatie registreert voor zichzelf van welke ketens de organisatie onderdeel is en wie binnen de organisatie aanspreekpunt is voor die keten.	n.v.t.
42.	Ketenpartners leggen de onderlinge afspraken over de inrichting en werking van de keten vast.	n.v.t.
43.	Voor iedere keten wordt een ketenverantwoordelijke en eventueel een ketenmanager aangesteld. De ketenpartners nemen een gezamenlijk besluit over het mandaat van deze personen om beslissingen te nemen voor de keten.	n.v.t.
44.	Ketenpartners stellen gezamenlijk de classificatie vast van de informatie die binnen de keten verwerkt wordt, welke door alle ketenpartners gehanteerd dient te worden bij de verwerking van die informatie.	n.v.t.
45.	Risico's voor een keten worden inzichtelijk gemaakt en besproken en opgepakt met relevante ketenpartners.	n.v.t.
46.	Ketenpartners bespreken periodiek de effectiviteit en efficiëntie van de risicobeheersing binnen de keten en voeren verbeteringen door waar nodig.	n.v.t.
Beleidsregels voor leveranciersrisicomanagement		
47.	De organisatie heeft zicht op alle ICT-diensten en ICT-producten vanuit leveranciers.	n.v.t.
48.	Binnen de organisatie is per afgenomen ICT-dienst of ICT-product een verantwoordelijke aangewezen, die zorg draagt voor de risicobeheersing rondom de dienst of het product.	n.v.t.
49.	Voor de aanschaf van een ICT-dienst of ICT-product van een leverancier, worden eerst de risico's voor het gebruik daarvan in kaart gebracht en beheerst.	n.v.t.
50.	Per dienst of product, welke nodig is voor het behalen van een organisatiedoel, is een actieplan beschikbaar hoe tijdelijk of definitief (exit-strategie) zonder deze dienst of dit product het organisatiedoel toch behaald kan worden.	n.v.t.

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

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

September 2025