

Jaarverantwoording NZa 2022

(Hoofdstuk 3 - Specifieke onderwerpen 2022)

3.7 Strategische risico's, fraude risico's en continuïteit

3.7.1 Risico overzicht

In deze paragraaf benoemen wij de voornaamste risico's en onzekerheden en de getroffen maatregelen om deze te mitigeren. Risicomanagement is een continu proces. Vanaf de begroting 2020 is risicomanagement integraal onderdeel van de planning- en control cyclus. Vanaf 2021 is, naast de reguliere risico identificatie, voor het eerst ook specifieke aandacht besteed aan frauderisico's. Bij het opstellen van de doelstellingen en resultaten moet de organisatie stilstaan bij de risico's die kunnen optreden en eventuele (aanvullende) beheersmaatregelen hierop treffen. Risicomanagement heeft onze continue aandacht. Wij zijn aan het verkennen of het beleid moet worden aangescherpt. In 2022 hebben we geen wijzigingen doorgevoerd.

Risicocategorie	Risico	Beheersmaatregelen	Kans	Impact	Risico effect
Informatie-beveiliging, dataveiligheid en ICT	Risico op uitval van één of meerdere ICT-systemen of onderdelen daarvan. Problemen met de inrichting of stabiliteit van de ICT, waardoor één of meerdere onderdelen (tijdelijk) uitvallen.	De opzet, het bestaan en de werking van incident- en probleemmanagement wordt periodiek getoetst en daar waar nodig aangescherpt. Nu de transitie naar de nieuwe IT infrastructuur vrijwel is afgerond ontstaat ruimte om de informatievoorziening, de kantoorautomatisering, de analyse-omgeving en het datalandschap verder te verbeteren.	L	M	
	Op basis van het dreigingsbeeld ziet de NZa een verhoogde interesse van externe partijen in de aan ons toevertrouwde data.	De maatregelen die op dit moment genomen zijn om indringers van buitenaf tegen te houden zijn onder meer: de standaard netwerkbeveiligingsmaatregelen zoals proxy servers en firewalls. Daarnaast is er een intrusion detection systeem (IDS) dat verdacht verkeer van en naar het internet signaleert. Ook beschikt de NZa over Security Information and Event Management (SIEM) dat de logging uit verschillende systemen analyseert en eventuele malversaties opspoot en rapporteert. Tenslotte beschikken de zero-footprint laptops allemaal over anti-malware bescherming en procesblokkering. Ook de werkplek zelf is voorzien van een virusscanner en procesblokkering waarmee alleen vooraf goedgekeurde programmatuur kan opstarten. Daarnaast heeft de NZa in 2021 geïnvesteerd in de offline back-up faciliteit om risico's te minimaliseren bij een hack.	L	H	
	Toegang tot data: het risico is dat de organisatie te weinig aandacht heeft voor: 1) de privacy-aspecten van data	1) Het omgaan met (gevoelige) data is onderdeel van het werken bij de NZa en opgenomen in het onboarding proces van nieuwe medewerkers. Daarnaast is er een e-learning beschikbaar voor alle medewerkers.	L	M	
	2) de noodzaak van gebruik van bepaalde data.	2) De NZa heeft de aandacht voor de privacy-aspecten in ons werk binnen de organisatie verankerd. Voor processen waarin data worden gebruikt worden Gegevens-effectbeoordelingen (GEB's) opgesteld.	M	H	

Legenda: Kans en Impact
L = Laag
M = Midden
H = Hoog

Risicocategorie	Risico	Beheersmaatregelen	Kans	Impact	Risico effect
Draagvlak stakeholders	Het risico is dat er te weinig draagvlak bij stakeholders is voor veranderingen doordat er sprake kan zijn van verschillende belangen. Wanneer draagvlak ontbreekt kan dit gevolgen hebben voor het resultaat of het proces.	Intensief overleg met onze stakeholders, tijdig betrekken en opschalen. Inzet van stakeholdermanagement bij verandertrajecten.	L	M	
	Maatschappelijke onrust als gevolg van toename van aantal knelpunten in de toegankelijkheid van zorg (zoals: huisartsentekort, wachttijden ggz, wachttijsten in ziekenhuizen a.g.v. uitgestelde zorg, wachttijsten in de langdurige zorg, etc.)	• Verzamelen en monitoren van stand van zaken t.a.v. de toegankelijkheid om zo goed mogelijke informatie te geven over waar de knelpunten zich voordoen en zorgverzekeraars en zorgaanbieders zo gericht mogelijk aan te spreken op het oplossen/verkleinen van knelpunten in het toezicht (o.a. toezicht op de zorgplicht). • Onze toezichtsacties transparant maken. • Investeren in communicatie-uitingen om burgers goed te informeren over toegankelijkheidsknelpunten in de zorg, wat zij zelf kunnen doen en wat zij van andere partijen mogen verwachten, en daarbij ook te werken aan verwachtingsmanagement.	H	H	
	Onvoldoende draagvlak voor grote transformaties die nodig zijn in de zorg.	Werken aan (communicatie)strategie om inzicht in noodzaak van de transformatie te vergroten en draagvlak te krijgen voor de stappen die gezet moeten worden.	M	H	
Personeel & Cultuur	Het risico dat medewerkers grensoverschrijdend gedrag vertonen.	Het onderwerp integriteit en ons beleid op dit gebied is regelmatig onderwerp van gesprek. Daarnaast wordt hier binnen de continue dialoog aandacht aan besteed.	L	M	
	Het risico is dat we specifieke functies nu of in de toekomst niet tijdig kunnen invullen. Dit wordt versterkt door de steeds knappere arbeidsmarkt.	In veruit de meeste gevallen werft de recruiter van NZa via onze eigen kanalen en netwerken. Door deze kanalen continu te monitoren, uit te breiden en te vernieuwen blijven we relevant op de arbeidsmarkt. We maken steeds meer gebruik van onze netwerken, zowel intern als extern en zoeken actief naar een zo divers mogelijk aanbod van kandidaten. Op basis van de strategische personeelsplanning wordt ook de toekomstige behoefte in kaart gebracht. In specifieke gevallen vindt (tijdelijk) inhuur plaats om prioriteiten in het werkprogramma en extra taken uit te kunnen voeren.	M	L	
Reputatie	Het onvoldoende of te laat acteren op vraagstukken en ontwikkelingen in de buitenwereld kan reputatieschade leveren. Hierdoor kan verminderd draagvlak ontstaan voor beleid van de NZa, waardoor beleidsdoelen niet bereikt kunnen worden.	Er is een NZa-breed issuemanagementteam dat zich bezig houdt met het in kaart brengen van risico's en issues. D.m.v. een vastgestelde proces wordt het bestuur hierover geïnformeerd. Daarnaast is er een protocol voor crisiscommunicatie.	L	H	
Risico's voor beleidseffectiviteit	Politieke verwachtingen t.a.v. het borgen van de continuïteit van zorg na faillissement van een zorginstelling.	Het Early Warning System (EWS) is intern goed ingebed. Ook stakeholders blijven actief betrokken zodat het draagvlak op peil blijft.	L	M	
Plaats- en tijdsafhankelijk werken	De digitale werkomgeving (software & hardware) faciliteert het plaats- en tijdsafhankelijk werken onvoldoende.	De NZa werkt samen met de nieuwe ICT-partner aan een 'toekomstvast' digitale werkplek, die het plaats- en tijdsafhankelijk werken (thuis en op kantoor) maximaal ondersteunt.	L	M	

Legenda: Kans en Impact
L = Laag
M = Midden
H = Hoog

Risicocategorie	Risico	Beheersmaatregelen	Kans	Impact	Risico effect
Inkopen / aanbestedingen	Het risico dat de Europese en/of interne aanbestedingsrichtlijnen niet worden nageleefd.	Het NZa Inkoopbeleid wordt regelmatig onder de aandacht wordt gebracht in de organisatie. Afwijkingen van het inkoopbeleid voor opdrachten > € 50.000 worden gemotiveerd en besproken in de raad van bestuur. Daarnaast worden inkopen steekproefsgewijs gecontroleerd. Hierover wordt minimaal twee maal per jaar gerapporteerd.	M	M	

Legenda: Kans en Impact

L = Laag

M = Midden

H = Hoog

Risicocategorie	Risico	Beheersmaatregelen	Kans (L)aag, (M)edium, (H)oog	Impact (L)aag, (M)edium, (H)oog	Risico effect
Frauderisico's	Het onttrekken van giraal geld aan de NZa door medewerkers	Slechts een beperkt aantal medewerkers hebben toegang tot het betaalproces. In het betaalproces zijn waarborgen getroffen om het risico op onttrekken van geld aan de NZa te voorkomen. Dit zijn onder andere functiescheiding, controle crediteurenstamgegevens door adviseurs, het noodzakelijk zijn van verplichtingen, autorisatie van facturen, en functiescheiding in het banksysteem. Ook selecteert de betalingsbevoegde bij iedere betaling een	L	M	
Frauderisico's	Fraude bij inkopen en aanbestedingen door samenspanning tussen medewerkers en derden	De NZa heeft het inkoopproces in lijn met de Aanbestedingswet vorm gegeven. Inkoop is deels decentraal belegd in onze organisatie. Voor de meeste inkopen vereisen wij meerdere offertes en gelden er autorisatieprocedures. Hiervoor hanteren wij het mandaat zoals vastgelegd in het Besluit organisatie, mandaat, volmacht en machtiging NZa. Voor Europese aanbestedingen gelden striktere regels die het risico op samenspanning mitigeren. De belangrijkste hiervan zijn het anoniem beoordelen van inschrijvingen, en het toedelen	L	M	
Frauderisico's	Ongeautoriseerde toegang tot gevoelige data	Binnen de NZa hebben een beperkt aantal medewerkers toegang tot gevoelige data. De toegang tot deze data monitoren wij strikt. Daarnaast besteden wij veel aandacht aan dataprivacy en datasecurity. Naast strikte beveiliging ten aanzien van de toegang hebben wij ook detectiemaatregelen ingericht, waaronder logging.	L	M	
Frauderisico's	Het doorbreken van interne beheersingsmaatregelen door management	Het risico dat onze beheersmaatregelen worden doorbroken door management is een belangrijk risico. De waarborgen die wij treffen zijn onder andere aandacht voor tegenspraak binnen de NZa. Ook is er een klokkenluidersregeling, en een integriteitscoördinator. Ook ondervangen wij dit risico doordat besluiten altijd vanuit een directie worden aangeleverd, en door de raad van bestuur worden bekrachtigd.	L	M	

Legenda: Kans en Impact

L = Laag

M = Midden

H = Hoog

3.7.2 Fraude risico's en continuïteit

Fraude- en corruptierisico's

Wij onderkennen dat wij als organisatie risico's lopen ten aanzien van fraude. Wij hebben veel oog voor fraude en oneigenlijk gebruik van zorggeld. Des te meer onderkennen wij het belang van het zorgvuldig omgaan met belastinggeld. Daarom voeren wij een uitvoerige analyse uit van de voor ons relevante interne frauderisico's. Ook hebben wij oog voor de risico's van corruptie en omkoping door derden.

De risicobereidheid van de NZa ten aanzien van fraude- en corruptierisico's is zeer beperkt. Wij onderkennen dat wij een belangrijke maatschappelijke rol hebben. Zowel op het gebied van regulering als toezicht vinden wij het ontzettend belangrijk om het goede voorbeeld te geven. De zorgsector is continu in beweging. Dat maakt dat wij, om onze rol effectief in te vullen, wendbaar moeten zijn. Deze benodigde wendbaarheid betekent dat wij risico's zoveel mogelijk willen mitigeren, maar niet in alle gevallen volledig afdekken wanneer het belang van wendbaarheid voor de zorgsector belangrijk is.

Identificatie van fraude- en corruptierisico's

De NZa voert een uitvoerige risico-inventarisatie uit. Wij bespreken de belangrijkste risico's binnen de directies en over de directies heen. Hierbij gaan wij uit van bruto risico's. Dat wil zeggen dat wij de risico's wegens zonder de interne beheersingsmaatregelen mee te nemen. De risico's bespreken wij minimaal tweemaal per jaar op bestuursniveau. Daarnaast heeft bespreking ook binnen de directies plaats. Door de bespreking van risico's op verschillende niveaus krijgen wij een goed en volledig beeld van de risico's voor de NZa. Waaronder ook fraude- en corruptierisico's. Bij de bespreking van de risico's gaan wij uit van de elementen uit de fraudedriehoek: gelegenheid, rationalisatie en motivatie (gedrag).

In 2022 identificeerden wij de volgende fraude- en corruptierisico's welke materieel kunnen worden als deze zich voordoen:

- Het onttrekken van giraal geld aan de NZa door medewerkers
- Fraude bij inkopen en aanbestedingen door samenspanning tussen medewerkers en derden
- Ongeautoriseerde toegang tot gevoelige data
- Het doorbreken van interne beheersingsmaatregelen door management

Daarnaast zien wij de volgende fraude- en corruptierisico's welke niet materieel kunnen worden, maar wel onze aandacht hebben:

- Het onttrekken van goederen aan de NZa
- Beïnvloeding van derden op onze processen ten aanzien van regulering en toezicht

De NZa heeft een belangrijke maatschappelijke rol. Integer handelen, en bewust met maatschappelijke middelen omgaan is onderdeel van ons bestaansrecht. Naast een mogelijke materiële impact hebben deze risico's ook mogelijke gevolgen voor onze reputatie en de impact die wij hebben op de zorg in Nederland. Daarom richtten wij maatregelen in om deze risico's te mitigeren.

Beheersmaatregelen

Om de risico's zoveel mogelijk te mitigeren hebben wij beheersmaatregelen ingericht.

Het onttrekken van giraal geld aan de NZa door medewerkers

Slechts een beperkt aantal medewerkers hebben toegang tot het betaalproces. In het betaalproces zijn waarborgen getroffen om het risico op onttrekken van geld aan de NZa te voorkomen. Dit zijn onder andere functiescheiding, controle crediteurenstamgegevens door adviseurs, het noodzakelijk zijn van verplichtingen, autorisatie van facturen, en functiescheiding in het banksysteem. Ook selecteert de betalingsbevoegde bij iedere betaling een steekproef om de juistheid te controleren.

Fraude bij inkopen en aanbestedingen door samenspanning tussen medewerkers en derden

De NZa heeft het inkoopproces in lijn met de Aanbestedingswet vorm gegeven. Inkoop is deels decentraal belegd in onze organisatie. Voor de meeste inkopen vereisen wij meerdere offertes en gelden er autorisatieprocedures. Hiervoor hanteren wij het mandaat zoals vastgelegd in het Besluit organisatie, mandaat, volmacht en machtiging NZa. Voor Europese aanbestedingen gelden striktere regels die het risico op samenspanning mitigeren. De belangrijkste hiervan zijn het anoniem beoordelen van inschrijvingen, en het toedelen van punten door een beoordelingsteam.

Ongeautoriseerde toegang tot gevoelige data

Binnen de NZa hebben een beperkt aantal medewerkers toegang tot gevoelige data. De toegang tot deze data monitoren wij strikt. Daarnaast besteden wij veel aandacht aan dataprivacy en datasecurity. Naast strikte beveiliging ten aanzien van de toegang hebben wij ook detectiemaatregelen ingericht, waaronder logging.

Het doorbreken van interne beheersingsmaatregelen door management

Het risico dat onze beheersmaatregelen worden doorbroken door management is een belangrijk risico. De waarborgen die wij treffen zijn onder andere aandacht voor tegenspraak binnen de NZa. Ook is er een klokkenluidersregeling, en een integriteitscoördinator. Ook ondervangen wij dit risico doordat besluiten altijd vanuit een directie worden aangeleverd, en door de raad van bestuur worden bekrachtigd.

Het onttrekken van goederen aan de NZa

De NZa heeft een strikte fysieke toegangsbeveiliging in de vorm van een passysteem en toegangspoortjes. De NZa beschikt tevens over een camerasysteem. Daarnaast is er een register van waardevolle goederen waardoor onttrekking hiervan gedetecteerd kan worden bij een inventarisatie. Iedere medewerker tekent voor de door de NZa in bruikleen gekregen apparatuur.

Beïnvloeding van derden op onze processen ten aanzien van regulering en toezicht

Naast belangrijke waarborgen in onze cultuur, en in ons aannamebeleid, zorgen wij dat beslissingen in teams worden genomen. Ook dragen wij zorg voor wisselende samenstellingen van teams. Binnen de NZa worden besluiten waarop beïnvloeding relevant zou zijn genomen in samenspraak met meerdere medewerkers. Besluiten worden door de raad van bestuur genomen.

Cultuur en soft controls

De NZa ziet integriteit als onderdeel van zijn bestaansrecht. Dit draagt het bestuur en management op alle lagen uit. Medewerkers krijgen bij indiensttreding een dilemmatraining en leggen de ambtseed af. Alle medewerkers overleggen een verklaring omtrent gedrag bij hun indiensttreding. Ook sluit de NZa op vrijwillige basis aan bij de Gedragscode Integriteit Rijk.

De naleving van de gedragscode vindt plaats door gesprekken tussen medewerkers en leidinggevend. Ook maakt dit onderdeel uit van het inwerkprogramma van nieuwe werknemers. Bij

(vermoede) overtredingen worden in overleg gepaste maatregelen genomen. Ook onderzoeken wij de oorzaak van mogelijke overtredingen om een eventuele bredere impact op de organisatie bloot te leggen en ook hier passende maatregelen op te kunnen nemen.

Wij hebben een integriteitscoördinator, interne en externe vertrouwenspersonen en een klokkenluidersregeling. Gedurende het jaar vestigen wij aandacht op de integriteit, en de beschikbare kanalen. Dat deden wij onder andere tijdens de week van de integriteit, en een dialoogweek. Daarnaast heeft het onderwerp tegenspraak een belangrijke plek in ons werkprogramma. Hiermee draagt de NZa het belang van integriteit uit naar haar medewerkers, maar ook naar externen.

Gematerialiseerde fraude- en corruptierisico's

Er hebben zich in 2022 en in de periode tot en met het opstellen van de jaarverantwoording geen fraude- of corruptierisico's gematerialiseerd.

Continuïteit

De NZa kenmerkt zich door één financieringsstroom vanuit VWS. Deze financiering stelt VWS jaarlijks vast. Wij monitoren de uitputting van het budget gedurende het jaar en bespreken dit met VWS. Ook kan VWS ons budget aanpassen naar aanleiding van ontwikkelingen in de werkzaamheden van de NZa, en de financiering hiervan. Gezien de stabiele financiering en de verankering van onze taken in de Wmg zien wij geen risico's ten aanzien van de continuïteit.

•