Internal audit jaarplan 2022-2024

Den Haag, 12 oktober 2021
Versie 1.0 definitief
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

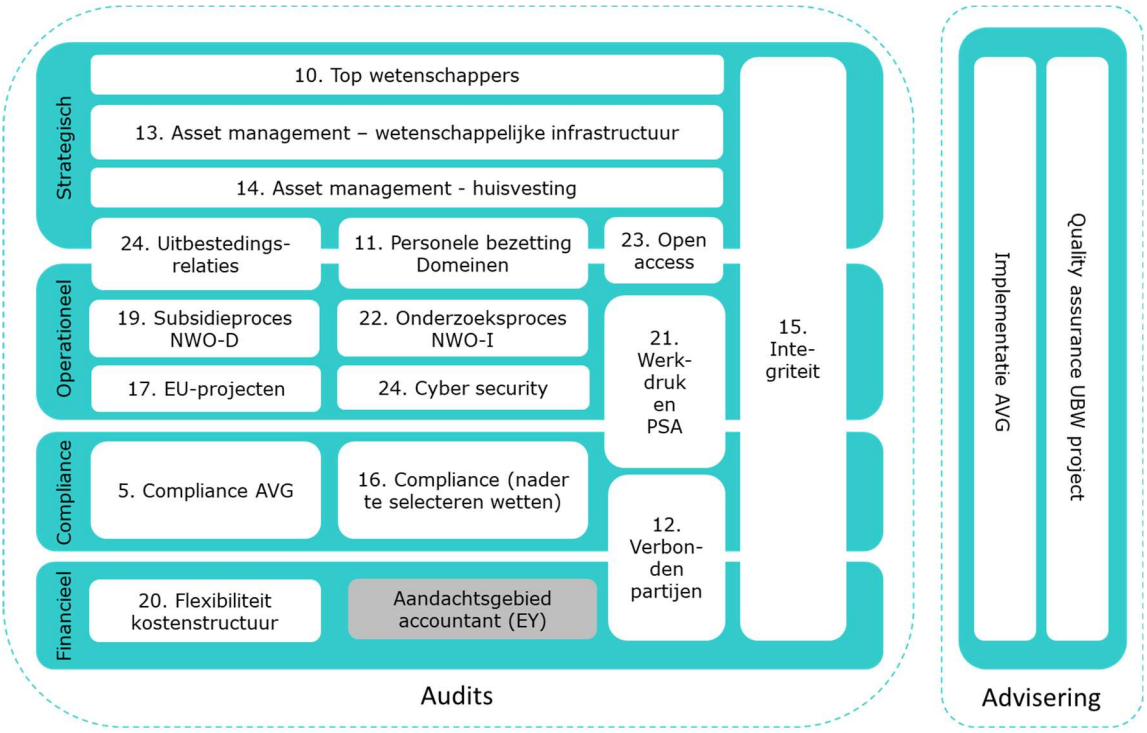
Samenvatting

Sinds juni 2018 heeft NWO een Internal Audit afdeling. De taakopdracht en het functioneren van de afdeling zijn nader uitgewerkt in een audit charter en een kwaliteitsbeheersingssysteem en -beleid. Voor de uit te voeren audits wordt jaarlijks een meerjaren audit plan opgesteld. Dit document is het geactualiseerde plan voor de periode 2022 – 2024.

De onderwerpen waarop door middel van audits additionele zekerheid wordt gegeven zijn bepaald o.b.v. *risk based auditing*. Dat wil zeggen dat de mate van beheersing van risico's die (zeer) groot zijn wordt onderzocht en dat aan kleinere risico's minder tot geen aandacht wordt besteed. Hierbij is aansluiting gezocht bij de strategie, het interne risicoregister, *benchmarks*, actuele ontwikkelingen en bevindingen van de externe accountant. Daarnaast is rekening gehouden met een evenwichtige verdeling van de audits tussen de organisatie-onderdelen:

- NWO-Domeinen (NWO-D), een Zelfstandig BestuursOrgaan (ZBO) met als wettelijke taak het bevorderen van de kwaliteit van wetenschappelijk onderzoek en het initiëren en stimuleren van nieuwe ontwikkelingen daarin;
- NWO-Instituten (NWO-I), een stichting waarbinnen 9 wetenschappelijke onderzoeksinstituten onderzoek uitvoeren met ondersteuning vanuit een Bureau.

Uitgaande van de capaciteit aan auditors zijn voor 2022 6 audits gedefinieerd, hetgeen oploopt naar 9 audits in 2024 (figuur). Daarnaast is in de planning rekening gehouden met het uitvoeren van niet geplande audits op ad hoc basis indien daar een behoefte aan bestaat en om een bijdrage te kunnen leveren aan projecten en andersoortige initiatieven.



Figuur: audits 2022 – 2024 (iedere audit heeft een eigen uniek doorlopend referentienummer)

Voor iedere audit zal een audit plan en gedetailleerd werkprogramma worden opgesteld dat zal worden afgestemd met de voor het onderwerp verantwoordelijke manager of directeur (*auditee*). Per uitgevoerde audit zal een concept rapport worden opgesteld dat met de *auditee* zal worden besproken en waarop deze commentaar kan geven. Dat commentaar zal worden verwerkt, waarna het rapport definitief zal worden gemaakt. Audit rapportages worden afhankelijk van het onderwerp besproken in het Directie Team, Instituutsmanager Overleg, Directeuren Overleg en de Raad van Bestuur of het Stichtingsbestuur. Jaarlijks wordt een samenvatting over alle onderwerpen gepresenteerd aan de (Audit Commissie van de) Raad van Toezicht.

Inhoud

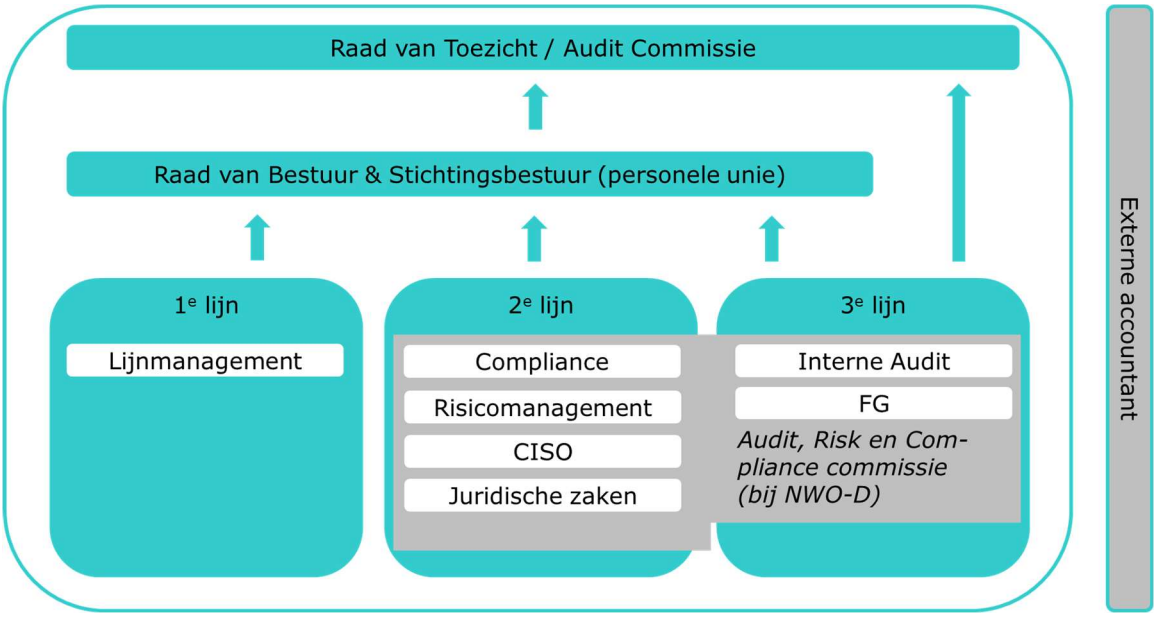
1 Inleiding

In 2018 is de Internal Audit (IA) afdeling van NWO gevormd. De eerste jaren is op basis van een ingroeimodel zowel een adviserende rol in de 2e lijn als een controlerende rol in de 3e vervuld. Voor NWO-D wordt sinds 2021 een zuivere rol in de 3e lijn vervuld. Met ingang van 2022 zal dat ook voor NWO-I gaan gelden. De afdeling valt onder de verantwoordelijkheid van de vicevoorzitter van de Raad van Bestuur (RvB).

1.1 Positionering internal audit

NWO past voor wat betreft de positionering van IA het internationaal gehanteerde '*3-lines of defence*' model toe (figuur 1):

- **1e lijn**
  Het lijnmanagement dat verantwoordelijk is voor de realisatie van de doelstellingen van NWO en de strategie die daaraan ten grondslag ligt. Dit omvat onder meer de verantwoordelijkheid voor de processen, projecten en de sturing en beheersing daarvan alsmede het afleggen van verantwoording daarover.
- **2e lijn**
  Risicomanagement- en *compliance* functies die de 1e lijn enerzijds ondersteunen en adviseren en anderzijds bewaken dat de 1e lijn haar verantwoordelijkheden neemt. Deze functies zijn binnen NWO bij diverse functionarissen belegd en worden soms gecombineerd met andere functies en taken. Voorbeelden zijn de *Chief Information Security Officer* (CISO), *compliance officer*, *risk managers* en *privacy officers*. NWO-D heeft sinds medio 2021 een *compliance officer* die vanuit een ingroeimodel inhoud aan deze functie aan het geven is. NWO-I heeft nog geen *compliance officer*.
- **3e lijn**
  Assurance functies van IA en de Functionaris Gegevensbescherming (FG) die het functioneren van de 1e en 2e lijn controleren, zich daarover objectief en onafhankelijk een oordeel vormen en mogelijkheden tot verbetering aangeven vanuit hun natuurlijke adviesfuncties.



Figuur 1: het 3-lines of defence model

De *compliance officer*, *risk managers*, CISO, FG, hoofd juridische zaken en het hoofd interne audit vormen tezamen de Audit & Risk Commissie (ARC). Deze is medio 2021 gevormd. Het doel is om een geïntegreerde visie op risico's te vormen, het risicoprofiel van NWO te bewaken, werkzaamheden met elkaar af te stemmen, prioriteiten te stellen, van elkaar te leren en samen te werken.

1.2 Taakopdracht

De taakopdracht van IA is nader uitgewerkt in een *audit charter*[1] dat, met advies van de Audit Commissie (AC) van de Raad van Toezicht (RvT), in 2018 is goedgekeurd door de RvB/SB. Dit *charter* zal in het najaar van 2021 worden geactualiseerd in verband met het aflopen van het ingroeimodel dat de eerste jaren is gehanteerd om de 2e lijn te ondersteunen en de afdeling vorm te geven. Met ingang van 2021 vormt IA een zuivere 3e lijn voor NWO-D. Voor NWO-I zal dat met ingang van 2022 aanvangen.

1.3 Kwaliteitsborging

Om de kwaliteit van interne audits te waarborgen beschikt de afdeling over een kwaliteitsbeheersingssysteem en -beleid[2]. Jaarlijks wordt een verantwoording opgesteld over de naleving daarvan. Conform *best practices* zal het functioneren van de afdeling om de 5 jaar extern worden getoetst in opdracht van de RvB/SB of de (AC van de) RvT. Dat zal voor het eerst in 2023 gaan plaatsvinden.

Naar aanleiding van een in 2020 uitgevoerde Europese Aanbesteding is KPMG geselecteerd als strategische partner voor kwaliteitsbeheersing. Indien gewenst of noodzakelijk kan IA een beroep op KPMG doen om een dossier review of Opdrachtgerichte KwaliteitsBeoordeling (OKB) uit te voeren. In 2021 is hier nog geen noodzaak toe geweest.

1.4 Planning

Voor de uit te voeren audits wordt jaarlijks een audit jaarplan opgesteld waarin de voor het komende jaar uit te voeren audits zijn opgenomen alsmede een doorkijk naar twee opvolgende jaren. Het plan wordt vooraf besproken met de vicevoorzitter van de RvB/SB. De goedkeuring van het jaarplan behoort, na een voorafgaand advies van de (AC van de) RvT, tot de verantwoordelijkheid van de RvB/SB. Het goedgekeurde jaarplan wordt gepresenteerd in het Directie Team (DT) van NWO-D en het Instituutsmanagers overleg (IM) en Directeuren Overleg (DO) van NWO-I. De instituutsmanagers en directeuren krijgen daardoor de mogelijkheid om met IA van gedachte te wisselen over het plan en een advies aan de RvB/SB te formuleren dat kan worden meegenomen in de besluitvorming. Voor iedere audit die in het jaarplan is opgenomen, wordt alvorens met de uitvoering te starten een gedetailleerd auditplan met onderliggend werkprogramma uitgewerkt. Ieder audit plan wordt in overleg met de vicevoorzitter van de RvB/SB en de voor het audit object verantwoordelijke bestuurder, directeur of manager (*auditee*) vastgesteld.

1.5 Reikwijdte

De reikwijdte van de uit te voeren audits betreft primair risico's die op NWO breed (concern) niveau als groot of zeer groot worden ingeschat, oftewel *risk-based auditing*. Dat wil zeggen dat de afdeling onderzoek doet op zowel concernniveau als bij de domeinen en instituten voor zover die dergelijke risico's lopen. Leidend voor het onderzoek naar de (zeer) grote risico's is dit audit jaarplan.

In aanvulling op audits die zijn opgenomen in dit jaarplan kunnen op verzoek van de 1e of 2e lijn secundair ook audits worden verricht naar kleinere risico's of specifieke onderwerpen waarover *assurance* gewenst is. Randvoorwaarde is dat dit in te passen is in de planning en capaciteit van IA. In dit kader is bijvoorbeeld onderzoek gedaan naar diversiteit, zijn *quality assurance* diensten op projecten verricht en zijn incidenten en vermoedens van fraude onderzocht. De ervaring heeft geleerd dat jaarlijks meer verzoeken voor ad hoc onderzoeken worden ontvangen dan waarvoor capaciteit

[1] Definitieve versie 1.1 d.d. 18 oktober 2018

[2] Definitieve versie 1.1 d.d. 18 oktober 2018

was gereserveerd. Daarom is in dit jaarplan additionele capaciteit vrijgemaakt om aan dergelijke verzoeken opvolging te kunnen geven.

Verzoeken voor ongeplande audits behoeven, voorzien van een advies van het hoofd IA[3], voorafgaande goedkeuring van de vicevoorzitter van de RvB/SB. Tot slot kan IA zelfstandig gedurende het jaar audits verrichten die niet in het audit jaarplan waren voorzien indien IA dat noodzakelijk acht en dit past binnen de capaciteitsplanning voor niet-geplande audits. Indien IA tot een dergelijke audit besluit zal zij de vicevoorzitter van de RvB/SB hierover vooraf en met redenen omkleed informeren. Bij vermoedens van fraude dient conform het fraudeprotocol van NWO altijd IA betrokken te worden.

NWO's strategie voor 2019-2022[4], het risicomanagement, bevindingen uit uitgevoerde interne audits, voorgevallen incidenten, het accountantsverslag en actuele ontwikkelingen zijn leidend voor de uit te voeren audits. Deze beslaan een breed terrein, waaronder begrepen:

1. Operationele audits naar de kwaliteit van de beheersing van processen, afdelingen of projecten, inclusief de betrouwbaarheid van de daartoe benodigde data en informatie;
2. *Compliance audits* naar de naleving van relevante wet- en (interne) regelgeving;
3. Audits op het gebied van integriteit en fraude;
4. *IT-audits* naar de *IT governance* en de beheersing van IT processen en –systemen;
5. Audits op het gebied van sociaal organisatorische beheersmaatregelen, oftewel *soft controls*;
6. Veiligheidsaudits, waaronder begrepen arbeidsomstandigheden;
7. Financiële audits, gericht op de betrouwbaarheid van de financiële informatie in samenspraak met de externe accountant.

Financiële audits (ad 7) worden in beginsel niet door IA uitgevoerd omdat deze tot het aandachtsgebied van de externe accountant behoren. Daar waar onderwerpen die door IA worden onderzocht financiële aspecten of gevolgen hebben, kunnen deze in de reikwijdte van de audit betrokken worden. De audit planning wordt jaarlijks met de externe accountant (EY) afgestemd.

1.6 Capaciteit

De capaciteit van de afdeling[5] is voor 2022 en opvolgende jaren vastgesteld op 4 auditors (3 FTE). Daarnaast wordt aan studenten via stageplaatsen de kans geboden om binnen de afdeling ervaring op te doen of af te studeren voor hun *bachelor* of *master*. De normatieve bezetting van de afdeling is eind 2021 in totaal 3,2 FTE:

- Hoofd interne audit als afdelingshoofd in een vast dienstverband (0,8 FTE);
- Senior auditor op inhuurbasis (0,8 – 1,0 FTE). In verband met onzekerheden ten gevolge van de Covid19-pandemie is deze functie in 2021 ingevuld vanuit de flexibele schil van IA. Najaar 2021 zal de werving starten om de functie vanaf 2022 vast in te gaan vullen;
- Medior auditor in een vast dienstverband (0,8 FTE);
- Junior auditor in een vast dienstverband (0,8 FTE).

De afdeling beschikt naar aanleiding van een in 2020 uitgevoerde Europese aanbesteding over een flexibele schil met Baker Tilly en Van Berkel Professionals als *preferred suppliers* voor het leveren van expertise of additionele capaciteit. KPMG is de strategische partner voor kwaliteitsbeheersing.

Streven ten aanzien van de bezetting van de afdeling is om een grote diversiteit op zoveel mogelijk aspecten te realiseren.

---

[3] Tot 2021 de senior internal auditor

[4] Verbinden van wetenschap en samenleving, NWO-strategie 2019-2022

[5] Exclusief de Functionaris Gegevensbescherming die met ingang van 2021 onderdeel van de 3e lijn is

1.7 Ervaringen en leerpunten

IA is inmiddels circa drie jaar operationeel. In die periode is de afdeling opgezet, zijn medewerkers en stagiaires geworven, is een *audit charter* en kwaliteitssysteem opgesteld, zijn audit jaarplannen gemaakt, zijn adviezen gegeven, zijn fraudesignalen en incidenten onderzocht, is het risicomanagement ondersteund, zijn trainingen gegeven, is *quality assurance* (QA) op projecten verricht, zijn de *preferred suppliers* gecontracteerd, zijn audits uitgevoerd en zijn rapporten naar aanleiding daarvan uitgebracht. Ten behoeve van de inbedding in de organisatie is in de eerste jaren daarbij prioriteit aan de adviesrol van IA gegeven. Inmiddels is sprake van een volwaardige afdeling in de 3e lijn. In dat kader is de FG in 2021 aan de afdeling toegevoegd met een functionele rapportagelijn aan het hoofd interne audit en een hiërarchische rapportagelijn aan de vicevoorzitter van de RvB/SB. De FG is geen auditor en heeft een eigen wettelijke taak maar maakt tezamen met de auditors onderdeel van de 3e lijn van NWO uit.

Het functioneren van IA is de afgelopen anderhalf jaar beïnvloed door de gevolgen van de Covid19-pandemie die de uitvoering van audits heeft bemoeilijkt. Dat geldt in het bijzonder voor de veiligheidsaudit naar chemie, gas en proefopstellingen die bij de instituten wordt uitgevoerd en waarbij bezoeken ter plaatse noodzakelijk zijn. In combinatie met de gevolgen van een systeem *hack* en ad hoc onderzoeken die niet in de planning waren opgenomen heeft dit tot achterstanden in de uitvoering van het audit jaarplan geleid. Daarentegen is door de uitvoering van de ad hoc onderzoeken voorzien in behoeften van directeuren en het bestuur, is zekerheid verstrekt en is kennis door IA opgebouwd.

Omdat de Covid19-pandemie het inwerken van auditors bemoeilijkt is ervoor gekozen beperkt additionele capaciteit vanuit de flexibele schil in te zetten. De prioriteiten en de inzet van capaciteit zijn in nauw overleg met vicevoorzitter van de RvB/SB bepaald. Hierdoor heeft de afdeling in 2020 en 2021 ruim onder het kostenbudget gewerkt. Een deel van het budget dat is bestemd voor de veiligheidsaudit naar chemie, gas en proefopstellingen is via een reservering doorgeschoven naar 2021 en zal voor een deel nogmaals moeten worden doorgeschoven (naar 2022).

Het aantal verzoeken voor ongeplande onderzoeken, zoals incidenten en vermoedens van fraude, is een leerpunt dat tot aanpassing van de allocatie van de capaciteit in dit jaarplan heeft geleid. In tegenstelling tot het vorige jaarplan zijn de uren van het hoofd van de afdeling niet meer gealloceerd aan de uitvoering van geplande audits maar is zijn capaciteit gereserveerd voor bijzondere onderzoeken, participatie in projecten, kwaliteitsbeheersing en leidinggevende taken.

Een ander leerpunt betreft de tijd die is benodigd voor audits die meerdere organisatieonderdelen omvatten. In de afgelopen jaren heeft standaardisatie van het primaire proces van de domeinen plaatsgevonden uit hoofde van project Vesalius en bij de instituten is een nieuw financieel systeem geïmplementeerd met standaardisatie van de financiële processen. Hierdoor zijn de verschillen tussen organisatieonderdelen kleiner geworden maar nog niet verdwenen. Deels bestaat nog eigen beleid, procedures en processen waardoor audits die meerdere organisatieonderdelen omvatten niet op basis van één normenkader uitgevoerd kunnen worden. In de capaciteitsplanning en allocatie van tijd aan audits is daar in dit jaarplan wederom rekening mee gehouden door additionele tijd te alloceren.

De status van de audits die in 2021 opgestart of afgerond zouden moeten worden conform het vorige audit jaarplan is in onderstaande tabel weergegeven (peildatum 1 september 2021).

Audit volgens planning (iedere audit heeft een uniek referentienummer)	Planning	Werkelijk	Toelichting
5. Compliance AVG (NWO-D)	100%	95%	Audit is afgerond, rapport nog op te maken.
6. Belangenverstrengeling (NWO-D)	100%	100%	Volledig afgerond in 2021.

7. Veiligheid (NWO-I[6]) inzake chemie, gas en wetenschappelijke proefopstellingen	100%	35%	Wegens Covid19 beperkingen en ad hoc onderzoeken beperkte voortgang in 2021. Voor najaar 2021 is capaciteit aan deze audit gealloceerd met als streven de audit 1e halfjaar 2022 af te ronden. Doordat alle instituten in *scope* zijn is dit een arbeidsintensieve audit.
9. Declaratiegedrag (NWO-D, NWO-I)	100%	100%	Volledig afgerond in 2021.
10. Top wetenschappers (NWO-I)	100%	0%	Vertraagd. Afgesproken is een voorstudie uit te voeren alvorens te besluiten over de uitvoering van de audit.
12. Verbonden partijen (NWO-D, NWO-I)	100%	35%	Audit is in uitvoering, afronding wordt verwacht voor eind 2021.
13. Asset management wetenschappelijke infrastructuur (NWO-I)	100%	10%	Vooronderzoek naar het normenkader is uitgevoerd. De audit wordt naar verwachting begin 2022 opgestart.
15. Integriteitsklimaat (NWO-D, NWO-I)	100%	0%	Vertraagd. Het voornemen is de audit te combineren met het medewerkersonderzoek dat voor NWO-D in 2022 door de P&O afdeling wordt uitgevoerd.
18. Diversiteit en *gender pay-gap* (NWO-D, NWO-I)	100%	95%	Audit is afgerond, rapport nog af te ronden.
19. Subsidieproces (NWO-D)	100%	60%	Audit is in uitvoering, afronding wordt verwacht voor eind 2021.

Tabel 1: status audits volgens plan 2021-2023 ten opzichte van werkelijke status per 1 september 2021

Om te voorkomen dat teveel audits parallel in uitvoering zijn, zijn audits nummer 10, 13 en 15 niet in uitvoering genomen. Voor wat betreft de inzet van het hoofd interne audit en de medior auditor wordt najaar 2021 zoveel als mogelijk prioriteit gegeven aan de uitvoering van de veiligheidsaudit (audit nummer 7) bij NWO-I.

[6] Initiële scope betrof de instituten AMOLF, DIFFER en NIOZ. Dit is uitgebreid tot alle instituten.

2 Risk based audits

Doelstelling van de afdeling is onderwerpen die een groot tot zeer groot risicoprofiel representeren in een cyclus van 3 tot 5 jaar te onderzoeken op basis van *risk-based auditing*. Dat wil zeggen dat audit objecten op basis van een risicoanalyse worden geselecteerd. Voor wat betreft de analyse van risico's wordt daarbij aangesloten op het interne risicobeleid[7] van NWO. Een risico is in dat beleid gedefinieerd als een onzekere gebeurtenis die kan leiden tot het afwijken van doelstellingen en eisen. De zwaarte van een risico is bepaald door een combinatie van de waarschijnlijkheid dat een gebeurtenis plaatsvindt en de impact daarvan op de doelstellingen van NWO. Dit wordt gemeten in vier klassen en is nader uitgewerkt in een risicomatrix (matrix 1). Het risicobeleid waarin deze matrix is opgenomen wordt herzien door de *risk manager* maar het gedachtegoed zal niet wijzigen.

4	Klein	Groot	zeer groot	zeer groot
3	Klein	Groot	groot	zeer groot
2	zeer klein	Klein	groot	groot
1	zeer klein	zeer klein	klein	klein
Kans	**1**	**2**	**3**	**4**
	Gevolg			

Matrix 1: risicomatrix model NWO (heatchart)

De gevolgen van risico's zijn in het risicobeleid nader uitgewerkt naar de aspecten financiële- en reputatieschade (matrix 2). Uit een confrontatie van de gevolg-categorieën voor risico's met *best practices* is naar voren gekomen dat andere organisaties, in aanvulling op de toepassing bij NWO, de mogelijke gevolgen van risico's tevens relateren aan gevolgcategorieën zoals veiligheid, compliance en integriteit. In de aanpassing van het risicobeleid wordt dit meegenomen door de *risk manager*. Een geactualiseerd risicobeleid is echter nog niet definitief vastgesteld, zodat IA nog gebruikmaakt van onderstaande risicowaardering.

Klasse	Waardering	Gevolg in geld
1	zeer klein	< € 2 mio
2	klein	€ 2 – € 10 mio
3	groot	€ 10 - € 22 mio
4	zeer groot	> € 22 mio

Financiën – NWO-D en concern

Klasse	Waardering	Gevolg in geld
1	zeer klein	< € 0,5 mio
2	klein	€ 0,5 – € 3 mio
3	groot	€ 3 - € 6 mio
4	zeer groot	> € 6 mio

Financiën – NWO-I

Klasse	Waardering	Gevolg voor de reputatie
1	zeer klein	Zeer klein
2	klein	Klein
3	groot	Groot
4	zeer groot	Zeer groot

Reputatie – NWO breed

Matrix 2: risicowaardering NWO

Totdat een herzien risicobeleid definitief is vastgesteld betrekt IA meerdere gevolgcategorieën in haar risico-gerichte aanpak, waarbij rekening wordt gehouden met de gevolgen op het gebied van de financiën, reputatie, veiligheid, compliance en integriteit.

Om tot een onderbouwde en afgewogen selectie aan te onderzoeken onderwerpen te komen die een (zeer) hoog risico voor NWO vormen wordt gebruik gemaakt van een aantal bronnen en criteria:

- **Formele vereisten (§ 2.1)**
  Dit zijn onderwerpen die onderzocht dienen te worden op basis van wet- en regelgeving, intern beleid of contractuele afspraken. Ten aanzien van deze onderwerpen bestaat in beginsel geen keuze, uitvoering van een audit is immers verplicht voorgeschreven.
- **Interne risico-analyses (§ 2.2)**
  Dit betreffen onderwerpen die een (zeer) hoog risicoprofiel hebben volgens de interne risicoregisters van NWO-D en NWO-I en daardoor het realiseren van de doelstellingen van NWO kunnen

[7] Notitie: Risicomanagement bij NWO, 201801111

bedreigen. De opstelling van deze registers is voor concern en NWO-D begeleid vanuit Concern Control & Financieel Beleid en voor bureau NWO-I door Financiële Planning. De implementatie van risicomanagement is NWO-breed nog in uitvoering.

- **Benchmarks (§ 2.3)**
  De interne risicoanalyses (§ 2.2) zijn afgezet tegen een tweetal *benchmarks* (zie bijlagen A en B) om te bezien of daaruit risicogebieden naar voren komen die binnen NWO geen of minder aandacht hebben maar zich op basis van het daaruit volgende risicoprofiel wel kwalificeren voor een interne audit. Deze *benchmark* is gedeeld met de risicomanagers.
- **Maatschappelijke ontwikkelingen (§ 2.4)**
  Naast *benchmarks* kunnen ook uit maatschappelijke ontwikkelingen risico's naar voren komen die voor NWO relevant zijn, in het bijzonder omdat NWO een publieke organisatie is. De interne risicoanalyses zijn daarom afgezet tegen maatschappelijke ontwikkelingen. Hiervoor is gebruik gemaakt van berichten uit de media die door IA gedurende het jaar worden verzameld voor dit doel.
- **Interne audit bevindingen (§ 2.5)**
  Dit betreffen bevindingen uit hoofde van uitgevoerde interne audits die een (zeer) hoog risicoprofiel representeren. De audit rapporten en daarmede de bevindingen worden gedeeld met de *risk managers* zodat zij de risicoregisters op basis hiervan kunnen actualiseren waar dat nodig is. De *risk managers* volgen de voortgang van de 1e en 2e lijn met het opvolgen van audit bevindingen op. Indien bevindingen volgens de *risk managers* zijn opgelost zal IA dit toetsen om de bevinding te kunnen sluiten.
- **Bevindingen externe accountant (§ 2.6)**
  Dit betreffen openstaande bevindingen van de externe accountants van NWO-D en NWO-I die een hoog risicoprofiel representeren.
- **Incidenten en vermoedens van fraude (§ 2.7)**
  Aan incidenten en vermoedens van fraude kunnen risico's ten grondslag liggen die tot een ander inzicht in het risicoprofiel van NWO leiden. IA volgt daarom (grote) incidenten op en doet daar indien gewenst ad hoc onderzoek naar. Bij vermoedens van fraude wordt IA conform het fraudeprotocol van NWO altijd betrokken.
- **Spreiding (§ 2.8)**
  Bij de selectie van de te onderzoeken risicogebieden wordt tot slot gestreefd naar een zo evenwichtig mogelijke verdeling van audits tussen NWO concern, domeinen en instituten. In overleg met onder meer de instituten vindt na vaststelling van dit jaarplan een nadere allocatie plaats van de auditcapaciteit over de instituten en vestigingslocaties. Dit leidt tot zichtbaarheid van de IA afdeling en heeft daardoor een preventieve werking binnen de organisatie. Bovendien helpt dit de auditoren de NWO organisatie, haar processen, locaties, risico's en beheersmaatregelen beter te leren kennen, zodat verdere kennis binnen de afdeling kan worden opgebouwd.

2.1 Formele vereisten

Audits die op basis van formele vereisten uitgevoerd worden liggen vast in wet- en regelgeving, intern beleid of contractuele afspraken. Dit kunnen risico's met een (zeer) hoog risico betreffen maar dat hoeft niet. Het dwingende karakter vanuit de voorschrijvende bron is voor deze onderwerpen leidend.

Tot heden is alleen een auditverplichting uit hoofde van het interne privacy beleid[8] vastgesteld. Dit hangt samen met verplichtingen uit hoofde van de AVG[9]. In het beleid is opgenomen, *quote* - "Aanvullend hierop maken audits op de naleving van de privacywetgeving en het privacy beleid het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit" - *unquote*. Met "hierop" wordt verwezen naar het toezicht op de naleving van de AVG door de FG.

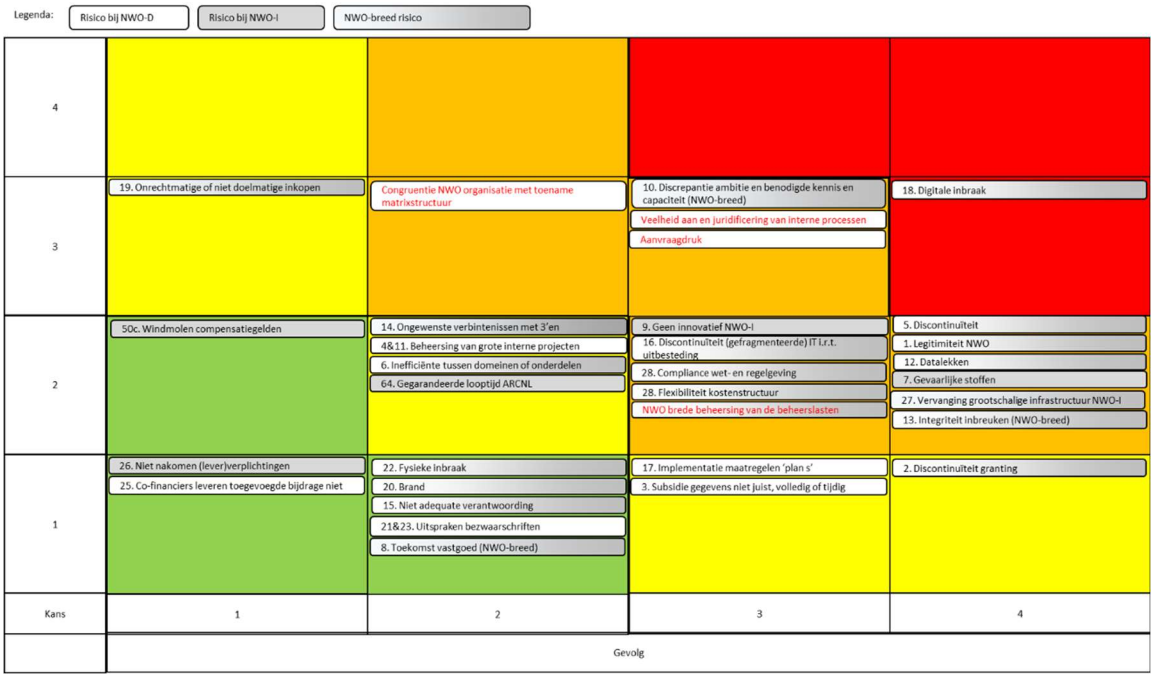
[8] Privacybeleid NWO 2018 – 2019 d.d. 23-5-2018

[9] Algemene Verordening Gegevensbescherming

Tot slot bestaat een verplichting tot controle van de jaarrekening. Dit valt niet onder de reikwijdte van de interne audit afdeling. De jaarrekeningcontrole wordt verricht door de externe accountant (4e lijn). Zowel de jaarrekeningen van de ZBO als die van Stichting NWO-I worden naar aanleiding van een openbare aanbesteding jaarlijks onderzocht door (gescheiden controleteams van) EY. De interne auditor en de externe accountants dienen jaarlijks de werkzaamheden op elkaar af te stemmen in een collegiaal overleg teneinde dubbel werk te voorkomen en waar mogelijk gebruik te maken van elkaars werkzaamheden. Met de accountant van NWO-D is dit jaarlijks georganiseerd en met ingang van najaar 2021 sluit ook de accountant van NWO-I hierbij aan. Maatschappelijk en binnen de beroepsvereniging van accountants is een roep ontstaan om meer gebruik te maken van elkaars werkzaamheden. De ervaringen tot heden zijn dat EY vooral gebruik maakt van onderzoeken van IA naar vermoedens van fraude en daarnaar geen dubbel onderzoek verricht. Door EY wordt niet gesteund op de werkzaamheden van IA omdat de verplichte toepassing van audit standaard 610[10] dat volgens EY inefficiënt maakt.

2.2 Interne risico analyses

Door de *risk managers* van NWO worden risicoregisters bijgehouden die de basis vormen voor het opstellen van risicomatrices voor enerzijds NWO-D en anderzijds NWO-I. Deze matrices worden door de *risk manager* van NWO-D vanuit zijn concernrol geconsolideerd tot een NWO-breed overzicht (matrix 3). Voor wat de risico's betreft zijn er, afgezien van verschuivingen in de *rating*, ten opzichte van vorig jaar een aantal nieuwe inzichten (in rood weergegeven in de matrix).



Matrix 3: NWO-brede risicomatrix 2021

Uit de interne risicomatrix blijkt dat de volgende risico's een hoog[11] (oranje) of zeer hoog (rood) risicoprofiel hebben en daarom verderop in dit auditplan betrokken dienen te worden:

- congruentie NWO organisatie met toename matrixstructuur (NWO-D);
- discrepantie ambitie en benodigde kennis en capaciteit (NWO-breed);
- veelheid aan en juridisering van interne processen (NWO-D);
- aanvraagdruk (NWO-D);
- geen innovatief NWO-I (NWO-I);

[10] NV COS 610 "Gebruik maken van de werkzaamheden van interne auditors"

[11] Er zijn geen zeer hoog (rood) gekwalificeerde risico's

- discontinuïteit (gefragmenteerde) IT in relatie tot uitbesteding (NWO-D);
- compliance met wet- en regelgeving (NWO-breed);
- flexibiliteit kostenstructuur (NWO-breed);
- NWO-brede beheersing van de beheerslasten (NWO-breed);
- digitale inbraken (NWO-breed);
- discontinuïteit NWO (NWO-breed);
- legitimiteit NWO (NWO-breed);
- datalekken (NWO-breed);
- gevaarlijke stoffen (NWO-I);
- vervanging grootschalige infrastructuur NWO-I (NWO-breed)[12];
- integriteit inbreuken (NWO-breed).

In de risicomatrix komt één risico met een zeer hoog risicoprofiel voor, namelijk het risico op een digitale inbraak (*hacking*).

2.3 Benchmarks

Vanuit haar eigen verantwoordelijkheid heeft IA de interne risicoanalyses (§ 2.2) evenals vorig jaar professioneel kritisch beoordeeld en de risico's afgestemd op een tweetal *benchmarks*:

- de *Hot Topics* 2021 rapportage van het IIA[13]. Dit is een jaarlijkse gezaghebbende publicatie van onderwerpen die IA afdelingen wereldwijd bezighouden en waarnaar zij audits uitvoeren (bijlage A);
- een in 2021 door IA geactualiseerde beoordeling van de risicoparagrafen van vergelijkbare instellingen zoals de onderzoeksafdelingen van Nederlandse universiteiten, Hogescholen en instituten zoals TNO (bijlage B).

Uit de afstemming komen de volgende onderwerpen naar voren die niet in de interne risicoanalyses zijn opgenomen maar wel in de *benchmarks* prominent[14] aandacht krijgen:

- ***Corporate governance* en verslaggeving**
  De *governance* van NWO is grondig herzien op basis van een transitie. Een uitgevoerde interne audit daarnaar uit 2019 heeft geen grote risico's naar voren gebracht. Dat geldt ook voor een in 2020 in opdracht van de Minister uitgevoerde externe evaluatie door de commissie Rinnooy Kan[15]. Daarnaast is NWO een Organisatie van Openbaar Belang (OOB), hetgeen wil zeggen dat de financiële verslaggeving door de externe accountant op basis van de meest strikte audit standaarden wordt onderzocht. Enige aandachtspunt voor NWO is het voornemen van de Europese Commissie (EC) om strikte verslaggevingseisen te introduceren op het gebied van niet-financiële informatie. NWO dient daar tijdig op voorbereid te zijn.
- **Klimaatrisico's en duurzaamheid**
  Dit is enerzijds een kans voor de wetenschap om onderzoek te doen en de maatschappij te informeren. Anderzijds is het voor NWO een reputatie risico indien de eigen bedrijfsvoering niet duurzaam is. Intern zijn initiatieven genomen om daaraan invulling te geven, waardoor dit niet als potentieel onderwerp voor een interne audit wordt beschouwd.
- **Management en reputatie**
  Dit risico richt zich op het voorbeeldgedrag en ethisch handelen van het (top)management. Jaarlijks wordt op basis van de beroepsregels van de auditors in het kader van de kwaliteitsbeheersing de integriteit van het bestuur geëvalueerd. Dit wordt afdoende geacht, er zijn geen indicaties dat dit binnen NWO een (groot) risico is.

---

[12] Dit wordt als NWO-breed risico bezien vanuit de *intercompany* relatie en financiering

[13] *Institute of Internal Auditing*

[14] Voor wat betreft de vergelijkbare instellingen zijn daarbij de risico's gehanteerd die door meerdere instellingen worden gerapporteerd. Van eenmalig gerapporteerde risico's is geabstraheerd.

[15] Evaluatierapport "De nieuwe weg van NWO" d.d. september 2020

- **Corruptie en fraude**
  Subsidieverstrekking is een activiteit die een risico voor omkoping en fraude met zich meebrengt. Daarnaast is fraude door wetenschappers bij onderzoek een aandachtspunt. Een trend is dat fraude meer en meer digitaal plaatsvindt, waaronder begrepen *hacking*. De afgelopen jaren zijn vermoedens van fraude conform het fraudeprotocol aan IA gemeld en onderzocht. Fraude is in zijn diverse verschijningsvormen daarmee een significant risico voor NWO. In alle interne audits wordt rekening gehouden met frauderisico's, alhoewel interne audits niet primair gericht zijn op het opsporen en ontdekken van fraude.
  Witwassen en financiering van terrorisme wordt een minder waarschijnlijke risico voor NWO geacht, alhoewel zeker bij internationaal onderzoek alertheid geboden blijft. De organisatie hanteert strikte gedragscodes en een fraudeprotocol maar geen standaard *due diligence* procedures t.a.v. subsidie-aanvragers.
- **Fusies en overnames**
  NWO is een ZBO waardoor een overname niet van toepassing is. Er zijn geen indicaties voor een fusie met een andere organisatie. Een voorbereiding op een samengaan met ZonMW is in 2018 stopgezet. De Minister heeft in antwoord op kamervragen[16] in 2021 herbevestigd dat van een samengaan met ZonMW geen sprake is. Dit is hierdoor geen onderwerp voor een audit.
- **Werkdruk**
  Dit is een risico dat door meerdere vergelijkbare instellingen wordt gerapporteerd. Uit MedewerkersOnderZoeken (MOZ) binnen NWO en uit een interne audit naar de transitie is naar voren gekomen dat dit ook bij NWO een aandachtspunt is. Een te hoge werkdruk kan naast verzuim tevens leiden tot ongewenst verloop, ontevredenheid en het kan een factor zijn om fraude te rationaliseren. Op basis van het MOZ is het thema intern opgepakt.
- **Imago en reputatie**
  Dit wordt binnen NWO niet als risico gezien maar als een mogelijk gevolg van risico's. In het risicobeleid van NWO is reputatie een gevolgcategorie. Dit wordt door IA onderschreven.

Bovenstaande is besproken en afgestemd met de risicomanager.

2.4 Maatschappelijke ontwikkelingen

Door gedurende het jaar voor NWO relevante maatschappelijke ontwikkelingen te monitoren heeft IA een aantal ontwikkelingen geïdentificeerd die potentiele risico's voor NWO kunnen (gaan) vormen. Dit betreft veelal strategische onderwerpen die bij een verkeerde of ontbrekende invulling voor NWO tot reputatieschade kunnen gaan leiden:

- **Diversiteit**
  Diversiteit is een aandachtspunt voor de wetenschap, in het bijzonder voor wat betreft de ondervertegenwoordiging van vrouwen en onderzoekers met een niet-westerse migratieachtergrond. De EC pakt daarop door met een *Gender Equality Plan* dat onderzoeksinstellingen met ingang van 2022 dienen in te voeren. NWO besteed aandacht aan het onderwerp via het eigen interne diversiteitsbeleid en extern met haar financieringsinstrumenten en voorwaarden in *calls*. Een interne audit naar de interne aspecten van dit onderwerp is recent afgerond en momenteel wordt het rapport opgemaakt. Ondanks de aandacht en maatregelen is ook bij NWO sprake van een onbalans in het personeelsbestand.
- **Werk-, aanvraag- en publicatiedruk wetenschappers**
  Op het competitiemodel voor het toekennen van subsidies aan wetenschappers bestaat kritiek omdat het kan leiden tot werk-, aanvraag- en publicatiedruk. Wetenschappers besteden uren aan het schrijven van voorstellen die voor een deel uiteindelijk niet tot een subsidie leiden. Deze uren hadden aan onderzoek besteed kunnen worden. NWO werkt aan maatregelen om de aanvraagdruk te verlagen en wordt daar door de evaluatiecommissie[17] verder in aangespoord. Desalniettemin kan de kritiek op het competitiemodel een risico vormen voor de legitimiteit van NWO, hetgeen als risico in het interne risicoregister is opgenomen.

[16] Antwoord op schriftelijke vragen van lid Bruins d.d. 11-5-2021

[17] Commissie Rinnooy Kan - 2020

- **Duurzaamheid**
  De Nederlandse overheid streeft naar energieneutraal en volledig circulair werken in 2050. Om dit te realiseren is een grote inspanning nodig. NWO heeft de eerste stappen gezet met een werkgroep voor Maatschappelijk Verantwoord Ondernemen (MVO) die werkt aan een duurzaamheidsbeleid. Daarnaast zijn in de kantoren maatregelen geïmplementeerd zoals gescheiden afvalsystemen. Het initiatief van de EC om niet-financiële rapportage verplicht te gaan stellen kan ertoe leiden dat NWO met ingang van 2023 over duurzaamheid dient te gaan rapporteren. Indien daaruit onvoldoende voortgang blijkt kan NWO worden aangesproken door belanghebbenden.
- ***Open science***
  Open science betreft een transitie naar een nieuwe, meer open en inclusieve manier van het uitvoeren, publiceren en evalueren van wetenschappelijk onderzoek. NWO heeft zich hieraan verbonden, onder meer voor wat betreft het *open access* publiceren. Indien dit niet op het gewenste tempo kan worden gerealiseerd of onvoorziene negatieve gevolgen voor wetenschappers blijkt te hebben vormt dit een risico voor NWO. In 2024 is een interne audit naar dit onderwerp voorzien.
- **Publiek private samenwerking**
  De wetenschap werkt steeds vaker samen met bedrijven en andere private partijen voor wat betreft de financiering van onderzoek. Dit sluit aan bij de strategie van NWO met betrekking tot de Nexus rol. Naast de onmiskenbare voordelen hiervan brengt dit een risico met zich mee met betrekking tot de onafhankelijkheid van het onderzoek en daarmee het vertrouwen van het publiek in de wetenschap.
- **Fraude met onderzoek(saanvrag)en**
  Fraudecases bij universiteit Leiden[18] met vervalste subsidieaanvragen en gemanipuleerde onderzoeksresultaten, bij de universiteit van Tilburg met vervalste onderzoeksgegevens[19] en onderzoeksresultaten die volgens reproductieonderzoek te rooskleurig zijn gepresenteerd in tijdschriften zoals *Nature* en *Science* leiden tot verlies van maatschappelijk vertrouwen in de wetenschap en misbruik van publiek geld voor onderzoek. Door het financieren van replicatie- en reproductieonderzoek draagt NWO bij aan het herstel van vertrouwen. Fraude door onderzoekers is een financieel en reputatierisico voor NWO indien de onderzoeken door NWO worden gefinancierd.
- **Wetenschappelijke infrastructuur(projecten)**
  Voor het behouden van een vooraanstaande positie dienen investeringen in de wetenschappelijke infrastructuur plaats te vinden. Dergelijke investeringen kunnen een hoog risicoprofiel hebben indien instituten of NWO-D hierin participeren of volledig voor eigen rekening investeren in infrastructuur, zoals bijvoorbeeld de schepen van NIOZ. Aan investeringen in infrastructuur zijn diverse risico's verbonden zoals financiële risico's, fiscale risico's, aanbestedingsrisico's en reputatierisico's. Een interne audit naar het asset management van wetenschappelijke infrastructuur was voorzien voor 2021 maar zal in 2022 worden uitgevoerd.
- **Cybercriminaliteit**
  Uit diverse publicaties blijkt dat cyber risico's toenemen. In 2021 is ook NWO hierdoor getroffen via een netwerk *hack* met *ransomware*. Uit in 2019 en 2020 uitgevoerde interne IT audits bij NWO-D, NIKHEF en NSCR bleek dat met name NWO-D op dit gebied een hoger risicoprofiel had. Maatregelen om dit te verlagen zijn uitgevoerd of nog in uitvoering. Cyber risico's zijn volgens het IIA het grootste risico voor organisaties, in het bijzonder omdat vanwege de Corona pandemie veelvuldig op afstand wordt gewerkt. De afhankelijkheid van de IT is daardoor verder toegenomen terwijl medewerkers gebruik maken van veelal minder goed beveiligde internetverbindingen thuis. Volgens het IIA vormen *phishing* en *malware* de grootste subrisico's. Het Rathenau Instituut doet daarom een beroep op organisaties om encryptie toe te passen, zodat eventueel buitgemaakte data voor criminelen niet leesbaar zijn. Voor ZBO's geldt in dat kader dat zij op basis van de kaderwet dienen te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Tussen NWO en het Ministerie van OCW zijn echter geen afspraken gemaakt over de verant-

[18] Cases "Adriana Bus" en "Lorenza Colzato"

[19] Casus "Diederik Stapel"

woording daarover. Wij hebben de CISO erop geattendeerd dat andere ZBO's jaarlijks verantwoording afleggen aan hun 'moederdepartement' en sommigen interne audits laten uitvoeren ter onderbouwing daarvan.
Naast financiële motieven vormen ook spionage en diefstal van kennis en technologie een motief. De Nederlandse regering roept universiteiten en onderzoeksinstellingen in dat kader op voorzichtig te zijn in de samenwerking met bepaalde landen. In 2023 worden nadere regels van overheidswege verwacht.
Tot slot is door de beroepsvereniging van IT-auditors een oproep gedaan om naast de jaarlijkse verklaring van de externe accountant bij de jaarrekening ook een jaarlijkse verklaring over de continuïteit en berouwbaarheid van de IT voor organisaties verplicht te stellen. Dit voorstel is met gemengde reacties ontvangen. Onduidelijk is of de Minister van Financiën in het kader van de herziening van de audit wetgeving het advies op gaat volgen.

- **Covid-19 pandemie**
  De (midden)lange termijn gevolgen van de Covid-19 pandemie zijn nog onduidelijk. Dit betreft onder meer de invloed op de gezondheid en vitaliteit van medewerkers, de budgetkeuzes van de overheid als de stimuleringsmaatregelen terugbetaald moeten worden, vertragingen die zijn opgelopen in wetenschappelijke onderzoeken en het vertrouwen van het publiek in de wetenschap. Vanuit NWO is pro-actief op de pandemie gereageerd en wordt op de gevolgen gestuurd door een *taskforce*.

2.5 Interne audit bevindingen

Bevindingen die uit interne audits naar voren zijn gekomen vormen eveneens een bron voor risicogericht auditen omdat aan bevindingen risico's ten grondslag liggen. In de afgelopen periode zijn de volgende audits uitgevoerd (tot en met in ieder geval een concept rapportage) waaruit bevindingen naar voren zijn komen:

- audit nr. 1: logische toegangsbeveiliging UBW en ISAAC (NWO-D);
- audit nr. 2: primair proces (NWO-D);
- audit nr. 3: IT security (NWO-D, NIKHEF en NSCR);
- audit nr. 4: inkoopproces (NWO-D, ASTRON en SRON);
- audit nr. 5: compliance AVG (NWO-D);
- audit nr. 6: belangenverstrengeling (NWO-D);
- audit nr. 8: transitie (NWO-D);
- audit nr. 9: declaratiegedrag (NWO-I en NWO-D);
- audit nr. 18: diversiteit en *gender pay gap* (NWO-I en NWO-D).

Uit de bevindingen van deze audits komen samengevat als meest relevante risicogebieden, exclusief *non-compliances*, naar voren:

- een middelmatig tot hoog risicoprofiel van de IT van NWO-D, waaronder begrepen de *IT security* en de afhankelijkheid van uitbestedingspartners. Na uitvoering van de audits heeft in februari 2021 een *hack* met *ransomware* plaatsgevonden waardoor de systemen van NWO enige weken niet operationeel zijn geweest. Verbeterpunten uit de audits waren ten tijde van de *hack* nog niet geïmplementeerd. Op dit moment wordt nog gewerkt aan de implementatie van verbeterpunten;
- effectiviteit en efficiëntie van het primaire proces van NWO-D, waaronder begrepen harmonisatie van het proces en datakwaliteit. Harmonisatie van het proces dient op basis van het Vesalius project gerealiseerd te zijn. Momenteel wordt dit voor een aantal processtappen getoetst via een interne audit. Datakwaliteit heeft de aandacht van een in 2020 gestarte informatiemanager;
- naleving van de AVG, waarbij diverse *non-compliances* bestaan. Deze zijn opgevoerd in het risicoregister en onder de aandacht gebracht van de nieuwe FG die op 1 september 2021 in dienst is getreden.

De interne audit rapporten worden gedeeld met de risicomanagers, zodat de risicoregisters op basis van de audit bevindingen aangescherpt kunnen worden. *Non-compliances* met wet- en regelgeving

worden in het kader van de NOCLAR[20] verordening voor NWO-D gedeeld met de *compliance officer* (NWO-I heeft nog geen *compliance officer*). Samengevat betreft het de volgende *non-compliances*:

- aanbestedingsregels: hierin is verbetering aangebracht door versterking van de inkoopfunctie. Daarnaast wordt hier jaarlijks door de externe accountant onderzoek naar gedaan. Uit zowel interne rapportages van de inkoopafdeling als van de externe accountant blijkt dat de rechtmatigheid aan het verbeteren is. De externe accountant van NWO-D rapporteert geen noemenswaardige bijzonderheden te hebben geconstateerd;
- tijdig betalen inkoopfacturen: op grond van artikel BW6-119a dienen inkoopfacturen tijdig betaald te worden. Uit de inkoopaudit kwam naar voren dat circa 20% van de facturen niet tijdig door NWO-D worden voldaan. Dit heeft de aandacht van afdeling Financiën;
- privacy: uit de AVG audit en audits naar het primaire proces van NWO-D zijn diverse verbeterpunten naar voren gekomen. Dit omvat onder meer de omgang met ongestructureerde data, het (niet) uitvoeren van Privacy Impact Analyses (PIA) op verwerkingen waarvoor dit wel geïndiceerd is en verwerkingen met gebruikmaking van de ISAAC applicatie voor subsidieverwerking van NWO-D terwijl die applicatie niet volledig AVG-*proof* is. Deze onderwerpen komen grotendeels overeen met de jaarlijkse rapportages van de FG aan het bestuur. De *non-compliances* worden zijn de auditors onder de aandacht gebracht van de nieuwe FG die per 1 september 2021 in dienst van NWO is gekomen;
- participatiewet: NWO voldoet niet aan de quota voor het bieden van werk aan personen met een arbeidsbeperking. Hierop wordt beleid gevoerd vanuit de P&O afdelingen maar dit resulteert nog niet in voldoende arbeidsplaatsen.

2.6 Bevindingen externe accountant

De externe accountant richt zich op de getrouwheid van de jaarrekening. Daardoor richt de accountant zich vooral op risico's die deze getrouwheid kunnen bedreigen.

Uit de *management letter*[21] (ML) van NWO-D blijken geen hoge risicogebieden. De ML bevat wel diverse middelhoge aanbevelingen. Het merendeel daarvan is inmiddels geïmplementeerd of in een vergevorderd stadium van implementatie, zoals project Vesalius voor de harmonisatie van het primaire proces en het inrichten van een batenregister. Het meest relevante resterende middelhoge risicogebied is naar onze inschatting de onvoldoende zichtbare tussentijdse monitoring door NWO-D op de naleving van subsidievoorwaarden door subsidieontvangers.
Kanttekening bij de ML is dat door de externe accountant niet formeel is gerapporteerd over de geautomatiseerde gegevensverwerking. De daaraan verbonden risico's ontbreken derhalve, terwijl deze significant zijn in navolging van de uitkomst van de interne audits naar de IT en de systeem *hack*.

Uit de ML van de externe accountant[22] met betrekking tot NWO-I zijn de volgende risico's als meest belangrijk af te leiden:

- ontbreken van procesdocumentatie en een gezamenlijke financiële administratie. Door de implementatie van een nieuw financieel systeem en een handboek AO wordt dit grotendeels opgelost;
- handmatige handelingen binnen het financiële consolidatieproces en fiscale aandachtspunten. Dit zijn risico's die geen onderdeel van door IA uitgevoerde operationele audits vallen;
- *security*, AVG *compliance* en continuïteit van de decentraal georganiseerde IT;
- onvolledige en niet uniforme decentrale contractenregisters.

Ten aanzien van de werkzaamheden van de externe accountant dient opgemerkt te worden dat deze bij beide organisatieonderdelen gegevensgericht zijn en dat niet wordt gesteund op de *general* en *application controls*.

---

[20] Non Compliance with Laws And Regulation, nadere verordening van de NBA

[21] 2e concept versie d.d. 5-11-2020

[22] Definitieve versie d.d. 9-12-2020

2.7 Incidenten en vermoedens van fraude

Een laatste bron voor risico's die richting kan geven aan interne audits betreft incidenten en vermoedens van fraude. De twee meest revelante risicogebieden die hieruit naar voren zijn gekomen betreffen:

- cybercriminaliteit, onder andere naar aanleiding van de systeem *hack* bij NWO-D en een poging tot digitale fraude;
- kwetsbaarheid van de bepaling van de rangorde van onderzoek aanvragen. Dit deelproces berust op het gebruik van kwetsbare *end-user-computing* toepassingen. Daarin zijn bij een organisatieonderdeel van NWO-D omissies geconstateerd die na ontdekking zijn hersteld. Dit is reden geweest de interne audit naar het primair proces in 2021 expliciet op deze risico's te richten teneinde een totaalbeeld van het risico te krijgen. Deze audit is nog in uitvoering.

2.8 Selectie risicogebieden

De risico's uit de voorgaande paragrafen zijn in tabel 2 samengevat als risicogebieden weergegeven. Daarbij is in de koptekst per risicogebied tussen haakjes aangegeven of dit betrekking heeft op NWO-D, NWO-I of op de gehele organisatie (NWO-breed). Daarnaast is in de opvolgende kolommen door middel van een "√" aangegeven uit welk bron het risicogebied afkomstig is: uit formele eisen (§ 2.1), het risicomanagement van NWO (§ 2.2), *benchmarks* (§ 2.3), relevante maatschappelijke ontwikkelingen (§ 2.4), bevindingen uit uitgevoerde interne audits (§ 2.5), rapportages van EY (§ 2.6) of uit incidenten of vermoedens van fraude (§ 2.7).

Risicogebieden	For-meel	Risico man.	Bench-mark	Pu-bliek	IA	EY	I/F
Compliance (NWO-breed) In het bijzonder met betrekking tot de privacy (AVG), inkopen (aanbestedingswetgeving en tijdig betalen) en de participatiewet.	√	√			√	√	√
Continuïteit (NWO-breed) Het *going concern* zijn van NWO, waaronder begrepen het negatieve eigen vermogen van de ZBO.		√					
Legitimiteit NWO (NWO-breed) Het bestaansrecht van NWO, waaronder begrepen het realiseren van doelstellingen zoals *open access* publicatie (plan "S") en het tijdig toekennen van onderzoeksgelden (discontinuïteit *granting*).		√		√			
Vernieuwing (NWO-I) Het innovatieve vermogen van de instituten om het bestaansrecht te waarborgen.		√					
Personeel (NWO-breed) Personeel gerelateerde deelrisico's: • werkdruk; • verandervermogen; • congruentie met de matrixstructuur; • kwaliteit management; • discrepanties tussen de ambitie van NWO en de benodigde kennis en capaciteit; • schaarste aan talent; • diversiteit.		√	√	√	√		

Primair proces (NWO-breed) Dit omvat: • effectiviteit en efficiëntie van het primaire proces (NWO-D); • juridisering van het primaire proces; • publiek private samenwerking (NWO-breed); • werk-, aanvraag- en publicatiedruk bij wetenschappers (NWO-breed); • calamiteiten bij samenwerkingspartners, zoals co-financiers (NWO-breed); • *open access* (laten) publiceren van onderzoeksresultaten (NWO-breed); • het waarborgen van de juistheid, tijdigheid en volledigheid van subsidiegegevens (zie ook risicogebied "verslaggeving") (NWO-breed); • datakwaliteit ISAAC (NWO-D); • monitoring naleving van subsidievoorwaarden (NWO-D); • kwetsbaarheid deelproces bepalen rangorde subsidieaanvragen (NWO-D); • kennisveiligheid (NWO-I).		√	√	√	√	√	√
Integriteit en fraude (NWO-breed) Dit betreft het mogelijk niet integer handelen van medewerkers, referenten, commissieleden, onderzoekers of andere derden, waaronder begrepen fraude met onderzoeksgelden en onderzoeksgegevens of corruptie.		√	√	√			
Veiligheid (NWO-I) Arboveiligheid en milieu gerelateerde risico's bij wetenschappelijke onderzoeken.		√	√				
Asset management (NWO-breed) Het behoud van - en investeren in – een hoogwaardige wetenschappelijke infrastructuur. Hieronder valt de vernieuwing van de onderzoekvloot van NIOZ en de financiering daarvan maar ook het onroerend zaak. Daarnaast is duurzaamheid van de infrastructuur een aandachtspunt.		√	√	√			
ICT (NWO-breed) Cybercriminaliteit, datalekken en de continuïteit van de (gefragmenteerde) ICT, waaronder begrepen de afhankelijkheid van uitbestedingspartners. Ook *non-compliance* met eisen die aan informatiesystemen worden gesteld uit hoofde van informatiebeveiliging en dataprotectie vormen onderdeel van dit risicogebied.		√	√	√	√	√	√
Verslaggeving (NWO-breed) Getrouwheid van de jaarrekening en de juistheid, tijdigheid en volledigheid van subsidiegegevens en –verantwoordingen (zie ook risicogebied "primair proces"). Daarnaast vormt aanstaande regelgeving over niet-financiële informatie zoals duurzaamheid een aandachtspunt.		√	√			√	
Kostenefficiëntie (NWO-breed) Dit betreft zowel de flexibiliteit van de kostenstructuur om mee te kunnen bewegen met budgettaire politieke sturing als de beheersing van de beheerslasten.		√					

Covid-19 (NWO-breed) Dit omvat de (middel)lange termijn effecten van de pandemie op onder meer personeelsleden, budgetten en internationale samenwerkingen.			√	√			

Tabel 2: hoog risicogebieden voor NWO

In vergelijking met het vorige audit jaarplan[23] kwalificeren de volgende risicogebieden niet meer als (zeer) hoog risicogebied en zijn daarom niet in tabel 2 opgenomen:

- Uitbestedingen. Voor NWO betreft dit vooral de leverancier van de ISAAC applicatie, waardoor dit risico bij de IT gerelateerde risico's is gevoegd;
- Inkopen. Dit betreft *compliance* met de aanbestedingsregels, hetgeen is opgenomen onder het bredere risicogebied van *compliance* met wet- en regelgeving waarvan het een subrisico is.

Ten opzichte van het vorige audit jaarplan zijn de volgende risico's breder gedefinieerd:

- *Compliance*. Hieronder is het handelen in overeenstemming met alle relevante wet- en regelgeving opgenomen;
- Primair proces. Hieraan is als apart deelrisico datakwaliteit binnen de ISAAC applicatie toegevoegd alsmede de juridisering van het proces;
- ICT. Hieronder is het risico met betrekking tot de uitbesteding van ISAAC opgenomen;
- Verslaggeving. Hieronder is opgenomen dat NWO op tijd klaar dient te zijn voor aanstaande regelgeving inzake niet-financiële rapportage.

[23] Audit jaarplan 2021-2023 d.d. 26-11-2020

3 Audit capaciteit

De IA afdeling bestaat uit een formatie van 4 medewerkers (3 FTE). Zij worden ondersteund door een flexibele schil die in 2020 via een Europese aanbesteding invulling heeft gekregen en bestaat uit een drietal van elkaar onafhankelijke *preferred suppliers*:

- twee organisaties die op aanvraag specifieke expertise of additionele capaciteit kunnen leveren;
- één organisatie die de kwaliteitstoetsing of opdrachtgerichte kwaliteitsbeoordeling (OKB) kan uitvoeren.

De *preferred suppliers* zijn onafhankelijk van de externe accountant van NWO.

Ten aanzien van de bezetting bestaat 1 vacature voor een senior auditor die vanwege de beperkingen van Covid-19 conform de planning tijdelijk is ingevuld vanuit de flexibele schil. Voornemen is om najaar 2021 de werving voor een vaste invulling te gaan starten.

Naast de vaste bezetting en flexibele schil blijft IA stageplaatsen aanbieden voor studenten. Bij gebleken geschiktheid en voldoende budgettaire ruimte kunnen de studenten na afronding van hun stage als tijdelijke kracht in de vorm van een bijbaan of vakantiewerk de afdeling blijven ondersteunen.

In de bepaling van de voor audits beschikbare uren wordt met ingang van 2022 de capaciteit van het hoofd interne audit niet meer aan geplande audits gealloceerd. Argument hiervoor is de ervaring dat zijn capaciteit vooral wordt ingezet op ongeplande ad hoc onderzoeken, het participeren in projecten, kwaliteitsbeheersing en leidinggevende taken. De voor audits beschikbare uren van de overige medewerkers zijn als volgt bepaald: (260 dagen * 8 uur per werkdag – 338 verlofuren) * aanstellingspercentage * 70%[24] productiviteit. De stagiaires zijn voor nihil uren (PM) meegenomen in de capaciteitsplanning omdat zij enerzijds capaciteit bieden maar anderzijds ook capaciteit vragen voor de begeleiding. Dit leidt tot onderstaande audit capaciteit (zie tabel 3) in uren voor de komende jaren op basis van de formatieplaatsen zoals die in het afdelingsbudget zijn opgenomen.

	2022	2023	2024
Hoofd interne audit (80%)	PM	PM	PM
Senior auditor (80%)	975	975	975
Medior auditor (80%)	975	975	975
Junior auditor (80%)	975	975	975
Stagiaires	PM	PM	PM
Aftrek: inhaal van in 2020 en 2021 minder opgenomen vakantie uren t.g.v. Covid-19 (ingeschat op 250 uur per medewerker voor het hoofd, de medior en de junior)	-750	n.v.t.	n.v.t.
Totaal beschikbare uren op jaarbasis (transporteren) – interne capaciteit	**2.175**	**2.925**	**2.925**

[24] Uitgangspunt is 70% productiviteit en 30% indirecte activiteiten zoals scholing, planning, overleggen, participatie in projecten, kwaliteitsbeheersing en het monitoren van de opvolging van audit bevindingen

Transport (beschikbare uren op jaarbasis)	**2.175**	**2.925**	**2.925**
Bij: capaciteit vanuit het budget voor de flexibele schil[25]	395	395	395
Niet-gealloceerde capaciteit (20%) t.b.v.: • additionele verzoeken voor niet begrote interne audits; • ad hoc interne audit verzoeken van RvB/SB en/of AC; • fraude onderzoeken indien intern fraude is geconstateerd of een wezenlijk vermoeden van fraude bestaat; • opvolging van openstaande audit bevindingen (i.s.m. *risk management*)	-435	-585	-585
Beschikbare uren t.b.v. geplande audits. Deze inzet is nader uitgewerkt in hoofdstuk 5.	**2.135**	**2.735**	**2.735**

Tabel 3: audit capaciteit IA

Het aantal beschikbare uren voor geplande audits is lager dan hetgeen was begroot in het voorgaande jaarplan omdat op basis van de ervaringen uit de afgelopen jaren is besloten de capaciteit van het hoofd interne audit niet planmatig mee te nemen. Zijn tijd wordt hoofdzakelijk besteed aan ad hoc onderzoeken, participatie in projecten, kwaliteitsbeheersing en leidinggevende taken. Daarnaast is de capaciteit in 2022 eenmalig verlaagd doordat in 2020 en 2021 vanwege de Covid-19 pandemie en diverse bijzondere ongeplande onderzoeken het verlofsaldo van alle medewerkers van interne audit is opgelopen tot een ongewenst hoog niveau. In de capaciteitsplanning is rekening gehouden met een afbouw daarvan in 2022.

Uitgaande van een gemiddelde doorlooptijd van een audit van ongeveer 400 uur kunnen in 2022 vijf audits worden uitgevoerd en vanaf 2023 circa zes tot zeven audits per jaar. Het gaat bij de capaciteitsbepaling om indicaties omdat sommige audits vanwege complexiteit of omvang meer of minder tijd zullen vergen dan andere audits. Daarnaast is in de inschatting van de benodigde uren rekening gehouden met ervaringen die zijn opgedaan in de afgelopen jaren.

[25] Totale budget is € 75.000 voor externe capaciteit, expertise en kwaliteitsbeheersing. Stelpost is hiervan € 50.000 te alloceren aan capaciteit. Tegen een gemiddeld uurtarief van € 105 exclusief 21% btw geeft dat een capaciteit voor audits vanuit de flexibele schil van 395 uur (50.000/105*1,21).

4 Audit planning

Deze paragraaf bevat een meerjaren audit planning voor de *assurance* diensten van IA. De bedoeling is de planning voor 2022 goed te laten keuren en de planning voor 2023 en 2024 indicatief vast te stellen. Crises zoals de Covid-19 pandemie en de systeem *hack* hebben duidelijk gemaakt dat lange termijn planningen met onzekerheden omgeven zijn en tussentijdse bijstelling kunnen behoeven. Dat geldt ook voor dit audit plan. Jaarlijks - en indien nodig tussentijds - zal de planning worden geactualiseerd en opnieuw vastgesteld conform de procedure die in het *audit charter* is vastgelegd.

Iedere audit heeft binnen NWO een uniek en doorlopend nummer. Een overzicht van de tot heden uitgevoerde audits is opgenomen in bijlage C.

De verwachting is dat in 2021 de volgende audits nog geheel of grotendeels worden uitgevoerd en afgerond:

- nr. 5 compliance AVG (NWO-D)
- nr. 12 Verbonden partijen (NWO-D en NWO-I)
- nr. 18 Diversiteit en *gender pay gap* (NWO-D en NWO-I)
- nr. 19 Subsidieproces (NWO-D)

De volgende audits waren overgelopen uit 2020 of voor 2021 in de planning opgenomen maar zullen vanwege de impact van Covid-19, de systeem *hack*, diverse ad hoc onderzoeken en het uitbreiden van de *scope* van de veiligheidsaudit naar verwachting niet voor eind 2021 worden afgerond of opgestart:

- nr. 7 Veiligheid en gezondheid bij gevaarlijke stoffen (alle instituten NWO-I)
- nr. 10 Topwetenschappers (NWO-I)
- nr. 13 Asset management (NWO-I)
- nr. 15 Integriteitsklimaat (NWO-D en NWO-I)

Als basis voor de audit planning is het audit jaarplan van de periode 2021-2023 gebruikt. Dat plan is nader uitgewerkt, verdiept en geactualiseerd op basis van de grootste risicogebieden (hoofdstuk 2), de beschikbare capaciteit (hoofdstuk 3) en leerpunten (hoofdstuk 1).

Audit onderwerp Onderliggend risicogebied	Toelichting	C/ D/ I [26]	V/ R [27]	Urenbegroting per audit		
				2022	2023	2024
Subsidieproces (nr. 26) *Compliance* (NWO-wet) Legitimiteit NWO Primair proces	Jaarlijkse audit naar de kernactiviteit van NWO-D gericht op de beoordeling van de beheersing van (nader te bepalen elementen van) de subsidieverstrekking aan onderzoeksprojecten. Waar mogelijk zal in overleg met EY *process mining* worden ingezet t.b.v. *conformance checking*.	D	R	300[28]	300	300
Transporteren				**300**	**300**	**300**

[26] **C**oncern, NWO-**D**omeinen of NWO-**I**nstituten

[27] **V**erplicht onderwerp of **R**isicogericht onderwerp

[28] T.o.v. het vorige audit jaarplan is het aantal uren per jaar teruggebracht. De scope van de audit zal namelijk beperkter worden om de doorlooptijden beter beheersbaar te houden.

Transport				**300**	**500**	**500**
Onderzoeksproces (nr. 22) *Compliance* (subsidievoorwaarden) Legitimiteit NWO Primair proces	Jaarlijkse audit naar de kernactiviteit van NWO-I gericht op de beoordeling van de beheersing van (nader te bepalen elementen van) wetenschappelijke onderzoeksprojecten. Omdat het innovatieve karakter van deze onderzoeken vanuit adviesraden, visitaties en het competitiemodel voor de verwerving van subsidies wordt beoordeeld zal daar beperkt op worden ingegaan. Voor 2022 is afgesproken de audit vooral te richten op de borging van kennisveiligheid binnen het primair proces.	I	R	385[29]	300	300
Compliance AVG (nr. 27) *Compliance* ICT (datalekken)	Jaarlijkse verplichte audit o.b.v. paragraaf 5.3 van het interne privacy beleid van NWO. In 2022 zal de audit zich in ieder geval op NWO-I richten omdat in 2021 onderzoek bij NWO-D is gedaan.	D I	V	250	250	200
Top wetenschappers (nr. 10) Vernieuwing Legitimiteit NWO Personeel	Onderzoek naar de mate waarin de instituten (top) wetenschappers aan zich weten te binden om de strategische ambities te kunnen realiseren en leidend te blijven in onderzoek (deze audit was voorzien voor 2020 en 2021 maar loopt over naar 2022). Deze audit zal zich focussen op het *talent management* en voor aanvang van de audit zal een voorstudie worden uitgevoerd.	I	R	400	-	-
***Asset management* – wetenschappelijke infrastructuur (nr. 13)** Vernieuwing *Asset management*	Beoordeling van het asset management v.w.b. de wetenschappelijke infrastructuur zoals telescopen en de onderzoekvloot. Dit omvat zowel de beheersing van het onderhoud van de huidige activa als toekomstige behoeften en investeringsprogramma's. Een vooronderzoek naar normatieve kaders is reeds uitgevoerd.	I	R	400	-	-
Transporteren				**1.735**	**1.050**	**1.000**

[29] T.o.v. het vorige audit jaarplan is het aantal uren teruggebracht en daarnaast is het een jaarlijkse audit geworden. Voor 2022 zijn meer uren begroot dan voor opvolgende jaren omdat dit het eerste jaar zal zijn waarin de audit wordt uitgevoerd en nog geen efficiëntie u.h.v. de herhaalfrequentie kan worden behaald

Transport				**1.735**	**1.050**	**1.000**
Integriteitsklimaat (nr. 15) Personeel Integriteit en fraude	Onderzoek van het integriteitsklimaat binnen NWO. Een goed integriteitsklimaat (*soft control*) voorkomt fraude en is een randvoorwaarde voor de werking van formele beheersmaatregelen *(hard controls*). Aansluiting wordt gezocht bij het MOZ[30] dat in 2022 opnieuw zal worden uitgevoerd bij NWO-D.	C D I	R	400	-	-
Personele bezetting domeinen (nr. 11) Legitimiteit NWO Personeel	Onderzoek naar de vraag in hoeverre de personele bezetting van de domeinen aansluit op de strategische ambities. De verwachting is dat de strategische personeelsplanning in 2023 volledig is geïmplementeerd en kan worden getoetst op haar werking.	D	R	-	450	-
***Asset management* – huisvesting (nr. 14)** *Asset management*	Beoordeling van het asset management v.w.b. de huisvesting (kantoren) op korte en (middel)lange termijn. Hierin zal tevens de grondpositie van NWO-D op het Science Park in Amsterdam betrokken worden. Merk op dat kantoren door NWO-D worden gehuurd en bij NWO-I in eigendom zijn. De ervaring van de andere *asset management* audit (nr. 13) zal worden meegenomen.	D I	R	-	400	-
Cyber security (nr. 24) ICT	Uitvoering van een gesimuleerde cyberaanval om de robuustheid van de IT *security* te toetsen. Uit de IT audit van 2020 en de systeem *hack* is gebleken dat het risicoprofiel bij NWO-D gemiddeld tot hoog is.	D	R	-	435	-
***Compliance* wet- en regelgeving (nr. 16)** *Compliance*	Onderzoek naar *compliance* met wet- en regelgeving buiten de reeds onderzochte AVG, aanbestedingswet en NWO subsidieregeling. Hiertoe zal ieder jaar in nauw overleg met de *compliance officer* een andere wet (of wetten) worden geselecteerd. De WNT wordt niet onderzocht omdat een gespecialiseerd team van EY daar jaarlijks onderzoek naar doet.	C D I	R	-	400	350
Transporteren				**2.135**	**2.735**	**1.350**

[30] MedewerkersOnderZoek

Transport				**2.135**	**2.735**	**1.350**
Open Access (nr 23) Legitimiteit NWO Primair proces	Beoordeling van de naleving van het *open access* beleid en de implementatie van plan "S".	D I	R	-	-	350
Werkdruk en psychosociale arbeidsbelasting (nr. 21) Personeel Veiligheid Covid-19 (impact op personeel en werk)	Beoordeling van de psychosociale arbeidsbelasting (PSA) en de effectiviteit van maatregelen om de werkdruk te verminderen. Hierbij zal worden aangesloten op metingen die in het kader van het MOZ zijn uitgevoerd. PSA is buiten scope als risicogebied in de veiligheidsaudit (nr. 7).	D I	R	-	-	300
EU projecten (nr. 17) Compliance (EU subsidievoorwaarden) Primair proces Integriteit en fraude	Beoordeling compliance met subsidievoorwaarden EU, in het bijzonder v.w.b. het tijdschrijven.	I	R	-	-	250
(In)flexibiliteit kostenstructuur (nr 20) Legitimiteit NWO Kostenefficiëntie Covid-19 (bezuinigingen overheid en EU)	Beoordeling mate van flexibiliteit van de kostenstructuur om mee te kunnen bewegen met fluctuaties in de subsidiestroom. Deze audit was voorzien voor 2022 maar is om capaciteitsredenen doorgeschoven naar 2023.	C D I	R	-	-	250
Uitbestedingsrelaties (nr. 25) ICT	Verkennend onderzoek naar de afhankelijkheid van NWO van uitbestedingspartners en de beheersing van risico's dienaangaande.	C D I	R	-	-	235
Totaal geplande audit uren				**2.135**	**2.735**	**2.735**

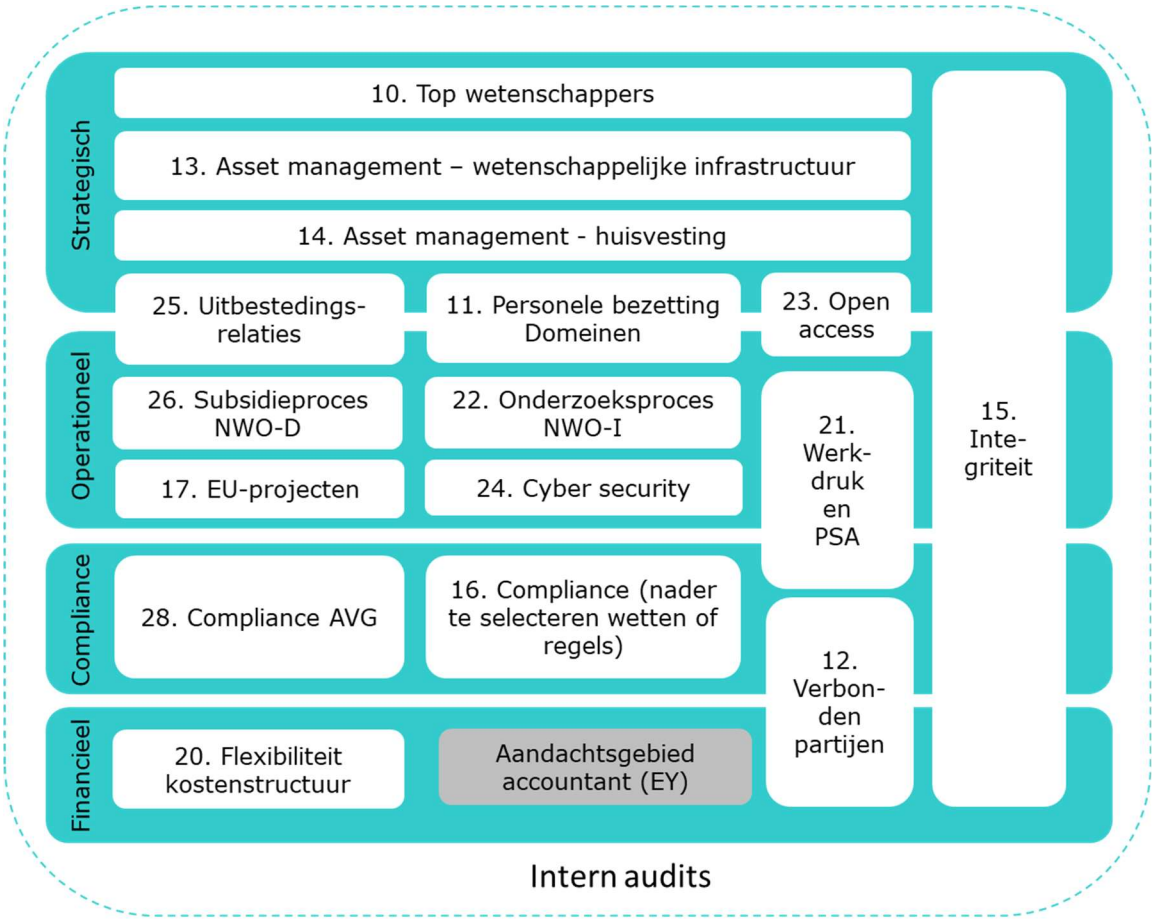
Tabel 4: audit planning en allocatie capaciteit 2022-2024

De audits zoals uitgewerkt in tabel 4 zijn primair risicogericht bepaald, zodat de grootste risico's de meeste audit-aandacht krijgen. Daarnaast is voor zover mogelijk rekening gehouden met een evenwichtige verdeling tussen enerzijds concern, domeinen en instituten en anderzijds tussen de risicocategorieën voor wat betreft de doelstellingen zoals opgenomen in het risicomanagement beleid (figuur 3). Aanvullend wordt het van belang geacht jaarlijks een significant deel van de audit capaciteit in te zetten op het primaire proces, oftewel subsidieverstrekking (NWO-D) en wetenschappelijk onderzoek (NWO-I). Audits 26 en 27 hebben rechtstreeks betrekking op het primaire proces en representeren 25% van de totale audit capaciteit in de komende drie jaren. Naar de risicogebieden continuïteit en verslaggeving wordt geen onderzoek gedaan. Dat is omdat op het negatieve eigen vermogen (continuïteit) nagenoeg geen invloed door NWO kan worden uitgeoefend en omdat de verslaggeving primair onder het aandachtsgebied van de externe accountant valt. Enige uitzondering kan voortkomen uit het EC initiatief om niet-financiële verslaggeving met ingang van 2023 verplicht te stellen. Indien de EC die planning gaat halen en NWO binnen de reikwijdte van de regelgeving gaat vallen zal dit in de volgende update van het audit jaarplan meegewogen worden.

Voor wat betreft NWO-I zullen de audits in 2022 in de volgende prioriteitsvolgorde worden uitgevoerd:

- (afronden van de) veiligheidsaudit;
- asset management wetenschappelijke infrastructuur;
- compliance AVG;
- integriteitsklimaat.

Voor wat betreft de audit naar top wetenschappers (*talent management*) zal eerst een vooronderzoek worden uitgevoerd om te concretiseren welke toegevoegde waarde een interne audit naar dit onderwerp kan opleveren in aanvulling op de externe (o.a. SEP) evaluaties dienaangaande. Indien dit tot de conclusie gaat leiden dat een interne audit hiernaar toegevoegde waarde heeft, zal deze opvolgend worden uitgevoerd.



Figuur 3: verdeling audits over de doelstellingen conform het risicobeleid

Hieronder (tabel 5) is inzichtelijk gemaakt welke risicogebieden uit paragraaf 2.7 de komende drie jaar conform dit audit jaarplan worden onderzocht, dan wel recent zijn onderzocht (bijlage C). Hieruit blijkt dat de (zeer) grote risico's van NWO in audits zijn of worden betrokken en IA de RvB/ SB en AC/RvT derhalve relevante additionele zekerheid gaat verstrekken over deze onderwerpen.

Risicogebieden	Toelichting
Compliance (NWO-breed)	*Compliance* met de aanbestedingswet is in 2019 onderzocht (audit nr. 4) en in 2021 is zowel *compliance* met de AVG (audit nr 5) als de naleving van de (oude) code belangenverstrengeling (audit nr. 6) onderzocht. In uitvoering is een audit naar de naleving van de interne richtlijn rechtspersonen in het kader van de audit naar verbonden partijen (audit nr. 12). De komende 3 jaren worden de volgende *compliance* audits uitgevoerd: • jaarlijkse audit naar de AVG conform de eis daartoe uit het interne privacybeleid (audit nr. 27); • een tweetal nog nader te selecteren wetten in 2023 en 2024 (audit nr. 16); • EU subsidieregels in 2022 (audit nr. 17). *Compliance* met de WNT wordt niet onderzocht omdat dit jaarlijks door een gespecialiseerd team van EY wordt gecontroleerd. *Compliance* met verslaggevingsregels valt ook onder de scope van EY.

Continuïteit (NWO-breed)	Naar de continuïteit worden geen interne audits verricht omdat dit door het ministerie wordt bepaald en een audit hier beperkt toegevoegde waarde heeft. Het negatieve eigen vermogen en het *going concern* vraagstuk hebben jaarlijks de aandacht van EY.
Legitimiteit NWO (NWO-breed)	Het bestaansrecht van NWO hangt sterk samen met de kwaliteit van de medewerkers. Het kunnen realiseren van de strategische ambities en leidend te blijven in onderzoek wordt voor NWO-I in 2022 onderzocht via een audit naar het vinden en binden van top wetenschappers (audit nr. 10) en voor NWO-D in 2023 via een onderzoek naar de personele bezetting (audit nr. 11). In 2024 wordt de stand van zaken ten aanzien van plan "S" (*open access*) beoordeeld (audit nr. 23) omdat NWO zich hieraan heeft gecommitteerd. Tot slot wordt in 2024 de flexibiliteit van de kostenstructuur (audit nr. 20) beoordeeld om vast te stellen wat de beïnvloedbaarheid is van het percentage beheerskosten. Dit percentage staat in de publieke belangstelling.
Vernieuwing (NWO-I)	Voor het innovatieve karakter van de onderzoeksprojecten van de instituten is veel aandacht vanuit onder meer adviesraden, visitaties en het competitiemodel via welke subsidies voor onderzoek verworven worden. Daarom zal in de audits naar het onderzoeksproces (audit nr. 22) vooral worden ingaan op de beheersing van de uitvoering van onderzoeksprojecten en zal beperkt aandacht worden besteed aan het innovatieve karakter ervan.
Personeel (NWO-breed)	Dit wordt voor NWO-I in 2022 onderzocht in de audit naar top wetenschappers (audit nr. 10), voor NWO-D in 2023 met de audit naar de personele bezetting en NWO-breed in 2022 voor wat betreft het integriteitsklimaat, oftewel de *soft controls* (audit nr. 15). Daarnaast zal in 2024 onderzoek worden gedaan naar de werkdruk en psycho sociale arbeidsbelasting (audit nr. 21).
Primaire proces (NWO-breed)	Het primaire proces van zowel NWO-D als NWO-I wordt jaarlijks onderzocht (audits nr. 22 en 26). Daarnaast wordt in 2024 onderzoek gedaan naar *compliance* met de voorwaarden van EU-subsidies bij NWO-I (audit nr. 17).
Integriteit en fraude (NWO-breed)	In 2020 is het declaratiegedrag (audit nr. 9) als integriteitsrisico onderzocht en in 2021 belangenverstrengeling (audit nr. 6). In 2022 wordt het integriteitsklimaat in samenloop met het MOZ onderzocht (audit nr. 15). Een goed integriteitsklimaat wordt beschouwd als een belangrijke beheersmaatregel (*soft control*) ter voorkoming van fraude. Daarnaast versterkt het de werking van formele beheersmaatregelen (*hard controls)*.
Veiligheid (NWO-breed)	In 2020 is aangevangen met een naar de Arboveiligheid bij de instituten t.a.v. het werken met chemicaliën en gassen in laboratoria alsmede de veiligheid van wetenschappelijke proefopstellingen. De uitvoering van deze audit loopt wegens omstandigheden nog door tot begin 2022. In 2024 volgt een NWO-brede audit naar de werkdruk en psychosociale arbeidsbelasting (audit nr. 21). Daarin kunnen eventuele (middellange) termijneffecten van Covid-19 worden meegenomen als aandachtspunt.
Asset management (NWO-breed)	In 2022 wordt het *asset management* t.a.v. de wetenschappelijke infrastructuur (audit nr. 13) onderzocht en in 2023 t.a.v. de huisvesting (audit nr. 14).
ICT (NWO-breed)	De ICT is de afgelopen jaren uitgebreid onderzocht voor wat betreft de logische toegangsbeveiliging van UBW en ISAAC bij NWO-D (audit nr. 1) en de *IT security* van NWO-D, NIKHEF en NSCR (audit nr. 3). In de *compliance* audit naar de AVG van 2021 (audit nr. 5) is bovendien aandacht aan de informatiebeveiliging besteed vanuit het risico op datalekken. In 2021 is een extern onderzoek gedaan naar de systeem *hack* en heeft de IAF onderzoek gedaan naar een vermoeden van cybercriminaliteit. Daarnaast dient EY jaarlijks aandacht te besteden aan de *IT governance* en de *IT general controls* in het kader van de jaarrekeningcontrole. Om de organisatie de tijd te geven bevindingen uit bovengenoemde interne audits en het onderzoek naar de systeem *hack* op te lossen wordt een nieuwe IT audit in 2023 voorzien. Deze zal zich dan richten op *cyber security* risico's (audit nr. 24). Een audit in 2022 wordt minder zinvol geacht omdat de implementatie van veel verbeteringen op dit moment nog in uitvoering is.

	Voor 2024 is een verkennend onderzoek naar de afhankelijkheid van uitbestedingspartijen en samenwerkingspartners voorzien (audit nr. 25). Vooralsnog is alleen de uitbesteding van de ISAAC applicatie van NWO-D hiervoor in beeld.
Verslaggeving (NWO-breed)	De financiële verantwoording wordt primair onderzocht door EY. Interne audits die hieraan bijdragen zijn: • onderzoek naar het primaire proces van NWO-D in 2018 en 2019 (audit nr. 2), 2021 (audit nr. 19) en 2022 en opvolgende jaren (audit nr. 26); • onderzoek naar het primaire proces van NWO-I met ingang van 2022 (audit nr. 22); • onderzoek naar de naleving van de richtlijn rechtspersonen bij NWO-I in 2021 (audit nr. 12) uit hoofde van de beheersing van verbonden partijen; • onderzoek in 2024 naar *compliance* met EU-subsidieregels bij NWO-I (audit nr. 17). Indien aanstaande regelgeving vanuit de Europese Commissie (EC) over verplichte niet-financiële verslaggeving ook voor NWO gaat gelden ontstaat een risico om daar tijdig aan te kunnen voldoen. Streven van de EC is de regelgeving met ingang van boekjaar 2023 in te laten gaan.
Kostenefficiëntie	Voor 2024 is een audit naar de mate van flexibiliteit van de kostenstructuur voorzien (audit nr. 20). Daarbij kunnen tevens de beheerslasten betrokken worden.
Covid-19	De (middel)lange termijneffecten van de Covid-19 pandemie op wetenschappelijk onderzoek, de daarvoor beschikbare budgetten, het personeel en internationale samenwerkingen zijn nog onduidelijk. Duidelijk is dat er een impact is op de primaire processen van zowel NWO-D als NWO-I en dat er mogelijk psychosociale gevolgen bij personeelsleden kunnen spelen. De gevolgen voor de financiering zijn nog onduidelijk, alhoewel in de EU begroting de onderzoeksgelden zijn gekort ten gunste van stimuleringsmaatregelen. De audit naar de flexibiliteit van de kostenstructuur van NWO (audit nr. 20) gaat een bijdrage leveren aan het inzicht in de mate waarin NWO mee kan bewegen in fluctuaties in de subsidiestroom.

Tabel 5: onderzoek van (zeer) hoge risicogebieden via interne audits

Naast de hiervoor uitgewerkte audits naar specifieke onderwerpen zal de afdeling tevens de volgende overige activiteiten uitvoeren:
- afstemmen van de werkzaamheden met EY (jaarlijks);
- actualiseren van het audit jaarplan, afstemmen met DT, IM, DO, RvB/SB en (AC van de) RvT (jaarlijks);
- rapportage over uitgevoerde audits en bevindingen aan RvB/SB (per uitgevoerde audit) en (AC van de) RvT (jaarlijks);
- audits op verzoek van concern, domeinen en instituten alsmede ad hoc verzoeken (na afstemming conform *audit charter*);
- fraude onderzoek indien intern een vermoeden van fraude wordt geconstateerd, e.e.a. conform het fraudeprotocol (ad hoc);
- monitoren van de opvolging op bevindingen die uit audits naar voren zijn gekomen (continu);
- bijdragen aan de effectiviteit en efficiency van de FG door het geven van (functionele) leiding aan de FG door het hoofd IA;
- bijdragen aan de beroepsontwikkeling door actief te participeren in de beroepsvereniging (Koninklijke NBA[31]).

[31] Nederlandse Beroepsorganisatie van Accountants

Om de geplande interne audits uit te kunnen voeren dient de afdeling over voldoende deskundigheid te beschikken. Voor wat betreft de volgende onderwerpen is de verwachting dat additionele expertise ter ondersteuning noodzakelijk zal zijn of verkregen moet worden door de auditors:

- *asset management* (audit nr. 13 in 2022 en audit nr. 14 in 2023);
- integriteitsklimaat (audit nr. 15, 2022);
- psychosociale arbeidsbelasting (audit nr. 21 in 2024);
- *cyber security* (audit nr. 24 in 2023).

Indien een investering in additionele expertise noodzakelijk blijkt zal dit in het gedetailleerde audit plan van de desbetreffende audit worden uitgewerkt, zodat hierop besluitvorming plaats kan vinden. Hierbij kan gedacht worden aan training of opleiding van medewerkers van IA of inhuur van externe expertise vanuit de flexibele schil van *preferred suppliers*.

5 Audit techniek en software

De aanpak van audits is door de afdeling nader uitgewerkt in een *audit charter* en een kwaliteitsbeheersingssysteem en -beleid. In het 4e kwartaal van 2021 worden beide documenten geactualiseerd.

Per audit wordt een gedetailleerd audit plan en onderliggend werkprogramma uitgewerkt waarin de toe te passen audit technieken en (eventueel) gebruik van audit software zal worden uiteengezet.

De afdeling beschikt, mede vanwege haar korte bestaan (sinds medio 2018), niet over audit software. De dossiervorming vindt daarom plaats op basis van digitale vastleggingen op de afdelingsschijf (G-schijf). Een wens is om op termijn een elektronisch dossier te gaan voeren, zodat het dossier beter ontsloten kan worden voor de risicomanagement functie, de *compliance officer* en de externe accountant. In het afdelingsplan is een verkennend onderzoek naar de mogelijkheden opgenomen. Daarbij zal tevens gebruik worden gemaakt van de kennis en ervaring van de *preferred suppliers*. Voor een eventuele aanschaf en implementatie is geen budget beschikbaar en dit wordt op korte termijn ook niet voorzien.

Voor data-analyse beschikt de afdeling over een licentie van Caseware IDEA. De licentie voor de *process mining* software van Perceptive is verlopen en door een overname van het softwarehuis is het ondanks diverse inspanningen niet mogelijk gebleken deze te verlengen. Vergelijkbare software is aanzienlijk duurder en past niet binnen het budget van de afdeling. Voornemen is te onderzoeken of *shareware* van universiteit Eindhoven bruikbaar is.

6 Rapportage

6.1 Audit rapportage

Per uitgevoerde interne audit wordt een concept audit rapport opgesteld en uitgebracht. Deze wordt voorbesproken met de vicevoorzitter van het bestuur om vervolgens te worden voorgelegd aan de in het audit plan vastgelegde *auditees*. De *auditees* geven inhoudelijke terugkoppeling op het concept rapport en management commentaar bij de bevindingen. De afdeling verwerkt het management commentaar in het rapport, waarna het conform het *audit charter* wordt aangeboden aan de vicevoorzitter, het DT of DO en de voltallige RvB/SB.

Jaarlijks stelt de afdeling een samenvattende rapportage op over de uitgevoerde audits en de belangrijkste bevindingen. Deze rapportage wordt conform de procedure uit het *audit charter* uitgebracht aan de (AC van de) RvT.

Op de middellange termijn kan de behoefte ontstaan om de afdeling een samenvattend oordeel over de interne beheersing te laten geven en daarover te rapporteren. Vaktechnisch zal dit de komende jaren niet mogelijk zijn omdat jaarlijks 'slechts' deelonderwerpen worden onderzocht en niet de totale interne beheersing. Een samenvattend oordeel zal samenhangen met een '*in control*' verklaring van de RvB/SB van NWO in het jaarverslag. Een dergelijke verklaring is tot heden geen onderdeel van het jaarverslag van NWO en er zijn nog geen processen en procedures, zoals *key-control testing*, die in een onderbouwing daarvoor voorzien.

6.2 Verspreiding rapportages

Rapportages worden door IA opgesteld voor interne doeleinden. Het is daarnaast op basis van de beroepsregels van de auditors niet toegestaan om audit rapporten zonder voorafgaande toestemming van de afdeling buiten NWO aan derden te verspreiden.

Omdat aan audit bevindingen risico's ten grondslag liggen worden audit rapporten gedeeld met de risicomanagers van NWO-I en/of NWO-D alsmede in voorkomende gevallen met de FG.

Bijlage A – Vergelijking IIA hot topics met NWO

Onderstaande tabel betreft een vergelijking van het jaarlijkse gezaghebbende IIA *hot topic* rapport[32] met het geconsolideerde NWO risicoregister. De risico's en eventuele verschillen zijn waar dat zinvol is geacht voorzien van een korte nadere toelichting.

IIA hot topic	NWO risicoregister	Toelichting
Cyber- en informatie-beveiliging	Datalekken (nr. 12) Digitale inbraak (nr. 18) Discontinuïteit IT i.r.t. uitbesteding (nr. 16)	Uit het IIA onderzoek blijkt dit als grootste risico voor organisaties naar voren te komen met *phishing* en *malware* als meest relevante bedreigingen. NWO heeft een CISO die toeziet op deze risico's.
Regulering en *compliance*	Datalekken (nr. 12 m.b.t. AVG) Compliance wet- en regelgeving (nr. 28) Onrechtmatig inkopen (nr. 19 m.b.t. aanbestedingsregels) Juridificering van processen (geen nr.)	NWO heeft geen '*regulator'* maar als ZBO wel een politiek risico. Daarbij zijn veel wetten van toepassing op NWO. In 2021 is een *compliance officer* aangesteld die voor NWO-D gaat toezien op de naleving. De instituten hebben nog geen *compliance officer*. De FG functioneert voor de gehele organisatie voor wat betreft *compliance* met de AVG.
Digitalisering en nieuwe technologie	Legitimiteit NWO (nr. 1) Geen innovatief NWO-I (nr. 9)	Voor NWO-D is dit vooral een kans om de dienstverlening aan wetenschappers te verbeteren. Indien niet wordt geïnnoveerd kan het op termijn de legitimiteit van NWO bedreigen. Voor diverse instituten van NWO-I is digitalisering en nieuwe technologie zowel een kans als een risico.
Financiële beheersing	Subsidiegegevens niet juist, volledig of tijdig (nr. 3) Co-financiers leveren bijdrage niet (nr. 25) Beheersing beheerskosten (geen nr.)	Financiële (verslaggevings)risico's worden primair onderzocht door de externe accountants van EY. De interne audit afdeling richt zich op operationele risico's. Een aandachtspunt zijn de *overhead*-kosten van NWO, die politiek en maatschappelijk de aandacht hebben.
Marco economische en (geo)politieke onzekerheden	Discontinuïteit *granting* (nr. 2) Flexibiliteit kostenstructuur (nr. 28) Beheersing beheerskosten (geen nr.)	Nationaal protectionisme en diefstal van kennis zijn aandachtspunten die onderzoeken en NWO kunnen raken. Daarnaast speelt in Nederland politieke onzekerheid met een voortslepende formatie en wereldwijd speelt de vraag hoe de overheidstekorten uit de Covid-19 periode terug moeten worden betaald. De vraag is wat beide voor de onderzoeksbudgetten gaan betekenen.
Organisatiecultuur	Integriteit inbreuken (nr. 13)	Een sterk integriteitsklimaat is essentieel om reputatie en *compliance* risico's te borgen.
Human resources en talentmanagement	Discrepantie ambitie en benodigde kennis en capaciteit (nr. 10)	Het IIA verwacht schaarste aan goed personeel. Maatschappelijke relevantie, diversiteit, inclusie en hybride werken zijn

[32] Risk in focus 2021 report

	Congruentie organisatie met toename matrixstructuur (geen nr.)	daarbij aandachtspunten. Strategische personeelsplanning wordt als essentieel beschouwd.
Uitbesteding	Discontinuïteit IT i.r.t. uitbesteding (nr. 16)	NWO heeft een beperkt aantal uitbestedingen waardoor dit risico beperkt lijkt. Op basis van de interne *IT security* audit lijkt de uitbesteding van ISAAC het meest risicovol met de grootste afhankelijkheid.
Corporate governance en verslaggeving	Congruentie organisatie met toename matrixstructuur (geen nr.)	De *governance* van NWO is grondig herzien n.a.v. de transitie. Dit is in 2019 door een interne audit onderzocht. Voor NWO worden op dit aspect geen grote risico's verwacht. De (financiële) verslaggeving is een onderwerp dat buiten de *scope* van de interne audit functie valt. Een aandachtspunt vormen initiatieven van de EC op het gebied van standaarden voor niet-financiële rapportages.
Klimaatrisico's en duurzaamheid	-	NWO loopt geen directe klimaatrisico's. Klimaatverandering is wel een onderwerp van wetenschappelijk onderzoek. Binnen NWO wordt nagedacht over de duurzaamheid van de eigen bedrijfsvoering. Vanuit de EC wordt een richtlijn voorbereid die rapportage verplicht over niet-financiële aspecten zoals duurzaamheid.
Crisis- en herstelmanagement	Discontinuïteit (nr. 5) Discontinuïteit IT i.r.t. uitbesteding (nr. 16)	Het belang van crisis- en herstelmanagement is door de Covid-19 crisis en cyber incidenten vergroot.
Management en reputatie	-	Dit risico gaat over voorbeeldgedrag van het bestuur en de mogelijke gevolgen daarvoor door de reputatie. Binnen NWO zijn geen aanwijzingen dat dit risico aandacht behoeft.
Corruptie en fraude	Integriteit inbreuken (nr.13)	Subsidieverstrekking is een activiteit die een risico voor omkoping en fraude met zich meebrengt. Fraude vindt meer en meer digitaal plaats, waaronder begrepen *hacking*. Witwassen en financiering van terrorisme zijn minder waarschijnlijke risico's voor NWO. De organisatie hanteert strikte gedragscodes en een fraudeprotocol maar geen standaard *due diligence* procedure jegens subsidie-aanvragers.
Gezondheid en arbeidsomstandigheden	Gevaarlijke stoffen (nr. 7)	Dit risico heeft door de Covid-19 pandemie meer aandacht gekregen. Bij de instituten wordt een, wegens omstandigheden meermalen uitgestelde, interne audit uitgevoerd naar de veiligheid van het werken met chemicaliën, gassen en proefopstellingen.
Fusies en overnames	-	NWO is een ZBO waardoor een overname niet van toepassing is. Er zijn geen signalen voor fusies met andere organisaties.

Bijlage B – Vergelijking risicoparagrafen soortgelijke instellingen met NWO

Onderstaande tabel betreft een in de zomer van 2021 door IA geactualiseerd *benchmark* onderzoek waarin de risicoparagrafen inzake de onderzoeksactiviteiten van een aantal Nederlandse Universiteiten en Hogescholen (Haagse Hogeschool, Hogeschool Utrecht, RijksUniversiteit Groningen[33], Technische Universiteit Delft[34], Universiteit Utrecht[35] en Universiteit van Amsterdam[36]) alsmede die van KNAW[37] en TNO[38] zijn vergeleken met het geconsolideerde risicoregister van NWO. Een dergelijke analyse is in 2018 voor het eerst gemaakt. De analyse is uitgewerkt in onderstaande tabel, waarbij verschillen tussen NWO en de soortgelijke instellingen zijn voorzien van een toelichting. Voornemen van IA is om het *benchmark* onderzoek minimaal om het jaar te actualiseren.

Merk op dat de soortgelijke instellingen een diversiteit aan risico's rapporteren. Dit is mogelijk te verklaren door verschillen in risico-inschatting, specifieke omstandigheden en het volwassenheidsniveau van het risicomanagement. Onderstaande tabel is daarom gesplitst in een tabel met risico's die meerdere organisaties beschrijven en een tabel met risico's de eenmalig zijn gerapporteerd.

Tabel met meermalig gerapporteerde risico's:

Risicoparagraaf soortgelijke instelling	NWO risicoregister	Toelichting
Onzekerheid geldstromen en tekorten dekking *overhead*[39]	Discontinuïteit *granting* (nr. 2) Vervanging grootschalige infrastructuur (nr. 27) Beheersing beheerslasten (geen nr.)	Universiteiten rapporteren dit voor zowel de 1e, 2e als 3e geldstroom. Door de Covid-19 pandemie worden extra bezuinigingen verwacht bij zowel de overheid als het bedrijfsleven.
Hoge werkdruk medewerkers (o.a. verzuim en verloop)[40]	-	Door de Covid-19 pandemie is dit verder toegenomen. Verlies van sociale binding tussen medewerkers wordt mede als oorzaak voor verzuim gezien. Daarnaast wordt uitputting van het adaptief vermogen verwacht.
Capaciteitstekort en schaarste aan talent[41]	Discrepantie ambitie en benodigde kennis en capaciteit (nr. 10)	Betreft zowel docenten als wetenschappelijk personeel. Dit risico heeft een relatie met de werkdruk (zie hiervoor).

[33] RUG
[34] TU
[35] UU
[36] UvA
[37] Koninklijke Nederlandse Akademie Wetenschappen
[38] Nederlandse organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
[39] KNAW 2020 / TNO 2020 / RUG 2020 / TU 2020 / UU 2020 / UvA 2020
[40] HH 2020 / HvU 2020 / KNAW 2020 / TU 2020 / UvA 2020
[41] RUG 2020 / TU 2020 / UU 2020 /UvA 2020

AVG[42], data(lekken) en cyberveiligheid[43]	Datalekken (nr. 12) Digitale inbraak (nr. 18) Discontinuïteit IT (nr. 16)	Hieronder worden kennisspionage en *compliance* met de AVG genoemd als deelrisico's. Daarnaast wordt verwezen naar *ransomware* aanvallen op de Universiteit Maastricht en NWO alsmede de risico's in relatie tot thuiswerken.
Schending wetenschappelijke integriteit[44]	Integriteitsbreuken (nr. 13)	-
Imago en reputatie[45]	-	Bij NWO wordt dit niet als separaat risico gezien maar als een gevolg van risico's. TNO benoemd in dit kader het risico dat de meerwaarde van de portfolio aan instituten niet wordt gezien.
Veiligheid (fysiek en mentaal) [46]	Gevaarlijke stoffen (nr. 7) Brand (nr. 20)	Veiligheid is breder dan alleen de gevolgen van een brand en schadelijke stoffen. De RUG besteed specifiek aandacht aan aardbevingsrisico's. Dit is mogelijk eveneens relevant voor SRON met een vestiging van circa 50 medewerkers in Groningen.
Non-compliance met wet- en regelgeving[47]	Datalekken (nr. 12 m.b.t. AVG) Onrechtmatig inkopen (nr. 19 m.b.t. aanbestedingsregels) Compliance wet- en regelgeving (nr. 18) Juridificering processen (geen nr.)	-
Huisvesting i.c.m. onvoldoende hoogwaardige onderzoeksfaciliteiten[48.]	Toekomst vastgoed (nr. 8) Beheersing van grote interne projecten (nr. 4 & 11) Ongewenste verbintenissen met derden (nr. 14)	De RUG en UU rapporteren grote investerings- en onderhoudsprojecten in uitvoering te hebben (*asset management*).

Op de volgende pagina volgt een tabel met risico's die eenmalig door een organisatie zijn gerapporteerd.

[42] RUG 2020 / UU 2020 / UvA 2020
[43] KNAW 2020 / RUG 2020 / TU 2020 / UU 2020 / UvA 2020
[44] KNAW 2020 / RUG 2020 / TU 2020 / UU 2020
[45] HvU 2020 / KNAW 2020 / RUG 2020 / TU 2020
[46] KNAW 2020 / RUG 2020 / TU 2020 / UvA 2020
[47] HvU 2020 / KNAW 2020 / TNO 2020
[48] RUG 2020 / UU 2020 / UvA 2020

Risicoparagraaf soortgelijke instelling	NWO risicoregister	Toelichting
Onjuiste financiële verantwoording of stuurinformatie onbetrouwbaar[49]	Subsidiegegevens niet juist, volledig of tijdig (nr. 3)	-
Onvoldoende verzekerd[50]	-	Dit wordt door NWO niet als een risico gezien maar als een onjuiste uitvoering van een beheersmaatregel (verzekeren) .
Vernieuwing bedrijfsvoeringssystemen[51]	-	Dit betreft de RUG die werkt aan de implementatie van een overstijgend bedrijfsvoeringssysteem.
Brexit[52]	-	Dit betreft onder meer lastiger uitwisseling van wetenschappers. De UK blijft participeren in het EU Horizon programma.
Kwaliteit onderzoek/wetenschap[53]	Vervanging grootschalige infrastructuur (nr. 27)	Dit wordt door de UU gerapporteerd en betreft risico's om hoogwaardige onderzoeksfaciliteiten te realiseren.
Samenwerking en onderzoeksveiligheid[54]	Co-financiers leveren toegezegde bijdrage niet (nr. 25) Niet nakomen (lever)verplichtingen (nr. 26)	Dit omvat het risico op calamiteiten bij samenwerkingspartijen alsmede diefstal van kennis.

Tot slot worden een aantal risico's t.o.v. voorgaande jaren niet meer gerapporteerd door de onderzochte organisaties. Dat betreft:

- Inflexibiliteit kostenstructuur: het vast zijn van kosten in plaats van variabel, zodat niet op korte termijn kan worden bijgestuurd op het kostenniveau[55];
- Positie afbakening, positionering en zichtbaarheid: dit betreft de legitimiteit van de betrokken organisaties[56];
- Beleid overheid: dit onderwerp richtte zich op de commissie Van Rijn en ombuigingen in de EU begroting[57].

[49] TNO 2020
[50] TNO 2020
[51] RUG 2020
[52] UvA 2020
[53] UU 2020
[54] UU 2020
[55] TNO strategisch plan 2018-2021
[56] KNAW 2019 / TNO strategisch plan 2018-2021
[57] RUG 2018 / UvA 2018

Bijlage C – Overzicht uitgevoerde interne audits

Audit nr[58].	Jaar	Onderwerp	Scope
1.	2018-2019	**Toegangsbeveiliging UBW en ISAAC** Onderzoek naar de mate waarin de logische toegangsbeveiliging van de applicaties ISAAC en UBW waarborgen dat deze applicaties niet toegankelijk zijn voor onbevoegden.	NWO-D
2.	2019-2020	**Primair proces (subsidieverstrekking)** Onderzoek naar de effectiviteit en efficiëntie van het primaire proces van subsidieverstrekking, waaronder begrepen de in dit proces opgenomen beheersmaatregelen. Met ingang van 2021 wordt het primaire proces of elementen daarvan jaarlijks onderzocht.	NWO-D
3.	2019-2020	**IT security** Onderzoek naar de mate waarin de beschikbaarheid, integriteit en vertrouwelijkheid van data in de geautomatiseerde systemen is gegarandeerd.	NWO-D, NSCR en NIKHEF
4.	2019	**Inkoopproces** Onderzoek naar de mate waarin het inkoopproces wordt beheerst, waaronder begrepen de rechtmatigheid met betrekking tot aanbestedingsregels.	NWO-D, ASTRON en SRON
5.	2020-2021	**Compliance AVG** Onderzoek naar de mate waarin wordt voldaan aan de eisen vanuit de AVG.	NWO-D
6.	2020-2021	**Belangenverstrengeling** Onderzoek naar de mate waarin de code belangenverstrengeling (medio 2020 opgevolgd door de code persoonlijke belangen) wordt nageleefd.	NWO-D
8.	2019	**Realisatie doelstellingen transitie** Onderzoek naar de vraag in hoeverre de doelstellingen van een in de periode 2016-2018 uitgevoerde organisatieverandering (transitie) zijn bereikt.	NWO-D
9.	2020	**Declaratiegedrag** Onderzoek naar de rechtmatigheid en tijdigheid van declaraties van onkosten door medewerkers en derden alsmede vacatiegelden door derden.	NWO-D en NWO-I (alle instituten)
18.	2020-2021	**Diversiteit en *gender pay gap*** Onderzoek naar de status van diversiteit, inclusie en een eventuele *gender pay gap* binnen NWO.	NWO-D en NWO-I (alle instituten)

[58] Iedere audit binnen NWO heeft een uniek eigen referentienummer.