Risicomanagementbeleid UWV

Documentbeheer

Versie historie

Versie	Datum	Aanpassing op verzoek van	Omschrijving van de aanpassing
0.1	01-07-2023	Manager KRB	Initiële opzet
0.6	25-08-2023	Adviseurs Risicomanagement	Aanpassingen op inhoud
0.76	22-09-2023	Adviseurs Risicomanagement	Aanpassingen op inhoud
0.9	30-10-2023	RM Community en staffuncties	Aanpassingen op inhoud en taal
0.91	11-12-2023	Directeur FEZ	Input bespreking 07-12-2023
0.93	18-12-2023	Reviewers versie 0.9	Aanpassingen op inhoud en taal
0.94	22-01-2024	Functioneel Overleg van hoofden BC&K	Aanpassingen op inhoud en taal
0.95/0.96	15-02-2024	Team KRB	Aanpassingen op inhoud en taal
0.97	15-04-2024	Review door AaC-leden en CPI	Aanpassingen op inhoud
0.98/0.99	23-05-2024	Team KRB	Aanpassingen op inhoud en taal
1.00	09-07-2024	RvB	Met goedkeuring RvB

Goedkeuring

Datum	Gremium	Rol	Status
09-07-2024	RvB	Goedkeurend orgaan	Goedgekeurd

Review en publicatie

Datum publicatie (locatie)	09-07-2024
Eerstvolgende reviewdatum	09-07-2025

Inhoud

1. Inleiding

'Elke dag spant UWV zich in voor een samenleving waarin iedereen kan meedoen. Dat doen we door mensen op een zo prettig mogelijke manier te helpen rond werk en inkomen. Mensen willen meedoen en een bijdrage leveren. Bij tegenslag, zoals werkloosheid, zoeken ze inkomenszekerheid. Wij maken werk en inkomen mogelijk. En zetten ons in om werkloosheid en arbeidsongeschiktheid te voorkomen. UWV werkt voor ons allemaal.'

Bron: Over UWV

Iedereen bij UWV draagt bij aan de doelen van de organisatie. In de uitvoering van het eigen werk maar ook in de veranderingen die we organiseren om de doelen van UWV steeds beter te realiseren. Doelen zijn daarmee een belangrijk onderdeel van de besturing van UWV.

Bij UWV hebben we te maken met doelen op verschillende niveaus. De organisatie-brede doelstellingen maar ook doelstellingen op het niveau van de klantketen, organisatieonderdelen en doelen op het niveau van processen, (verander)programma's en projecten. Het realiseren van doelen op het niveau van organisatieonderdelen, afdelingen en processen dragen bij aan het behalen van de organisatie-brede doelstellingen.

Doelstellingen zijn er in vele vormen. Er zijn, bijvoorbeeld, doelen die bijdragen aan een optimale dienstverlening aan cliënten (gezien, gehoord, geholpen) en aan een rechtmatige uitvoering van het werk. Doelen die misbruik of oneigenlijk gebruik helpen voorkomen, die ervoor zorgen dat we voldoen aan wet- en regelgeving (compliance) en die bijdragen aan een financieel gezonde bedrijfsvoering.

Op de weg naar het realiseren van al deze doelen worden we geconfronteerd met 'onzekerheden'. Dit kunnen zowel kansen als risico's zijn. Risico's maken het behalen van de doelen onzeker. Daarom is risicomanagement een onderdeel van de besturing van onze organisatie. Risicomanagement is een integraal onderdeel van de beheerste bedrijfsvoering die we bij UWV nastreven. Met risicomanagement zorgen we ervoor dat UWV structureel en procesmatig inzicht krijgt in de onzekerheden in de besturing en het geeft managers en medewerkers de mogelijkheid om tijdig en adequaat bij te sturen op de realisatie van de doelstellingen. Risicomanagement wordt toegepast op elk niveau binnen de organisatie.

Omdat alle doelen uiteindelijk bijdragen aan de realisatie van de UWV-brede doelstellingen passen wij integraal risicomanagement toe. Daarmee zijn alle relevante doelstellingen in de breedte van de organisatie en op alle niveaus afgedekt.

Bij risicomanagement hoort risicoleiderschap. Risicoleiderschap beschrijft de cultuur, de houding en het gedrag dat wordt gevraagd van elke medewerker om goed om te gaan met onzekerheden bij het realiseren van doelen. Met risicoleiderschap kunnen we bij UWV de dialoog over risico's en de beheersing daarvan bevorderen.

De bedoeling van deze cultuur is dat we tussen alle lagen van de organisatie het goede gesprek voeren over de doelstellingen, wat daarbij de onzekerheden (risico's en kansen)

zijn en hoe we daarmee omgaan (wat we eraan doen). In die gesprekken vervult de D-O-D aanpak een centrale rol. D-O-D staat voor Doel – Onzeker – Doen.

In dit document is het risicomanagementbeleid van UWV en de werkwijze op hoofdlijnen verder uitgewerkt. Het beleid heeft mede als doel een uniforme toepassing van risicomanagement binnen UWV te bewerkstelligen wat zorgt voor een integraal inzicht in alle onzekerheden (risico's en kansen) op elk niveau van de organisatie en de mate van beheersing van deze onzekerheden. Daarom is de werkwijze een integraal onderdeel van dit beleidsdocument gemaakt.

Het beleidsdocument is opgesteld onder regie van FEZ als stelselverantwoordelijke en in afstemming met vertegenwoordigers van de organisatieonderdelen van UWV. Zij werken samen in de risicomanagement community en andere afdelingen binnen UWV die verantwoordelijk zijn voor specifieke beleidsgebieden en raken aan risicomanagement. Laatstgenoemde zijn verzameld in de zogenaamde 'expertisetafel risicomanagement' van UWV die in paragraaf 3.3 verder wordt toegelicht.

2. Doel, doelgroep en reikwijdte van het beleid

2.1 Doel

Het doel van het UWV-brede risicomanagementbeleid is al benoemd in de inleiding maar wordt hier kort herhaald. Op weg naar het realiseren van de doelen van UWV worden we geconfronteerd met 'onzekerheden'. Dit kunnen zowel kansen als risico's zijn. Risico's maken het behalen van de doelen dus onzeker. Daarom is risicomanagement een onderdeel van de besturing van onze organisatie. Risicomanagement is een integraal onderdeel van de beheerste bedrijfsvoering die we bij UWV nastreven. Met risicomanagement zorgen we ervoor dat UWV structureel en procesmatig inzicht krijgt in de onzekerheden en het geeft managers en medewerkers de mogelijkheid om tijdig en adequaat bij te sturen op de realisatie van de doelstellingen. Risicomanagement wordt toegepast op elk niveau binnen de organisatie.

Bij risicomanagement hoort risicoleiderschap. Risicoleiderschap beschrijft de houding en het gedrag dat wordt gevraagd van elke medewerker van UWV om goed om te gaan met onzekerheden bij het realiseren van de doelen.

Het doel van dit document is om binnen UWV een organisatie-brede, uniforme, methodiek in te voeren om risico's, te identificeren, classificeren, beheersen, monitoren en te rapporteren. Dit is nodig om integraal risicomanagement te realiseren en zo een structurele bijdrage te leveren aan het behalen van de organisatiedoelen en aan een beheerste bedrijfsvoering bij UWV.

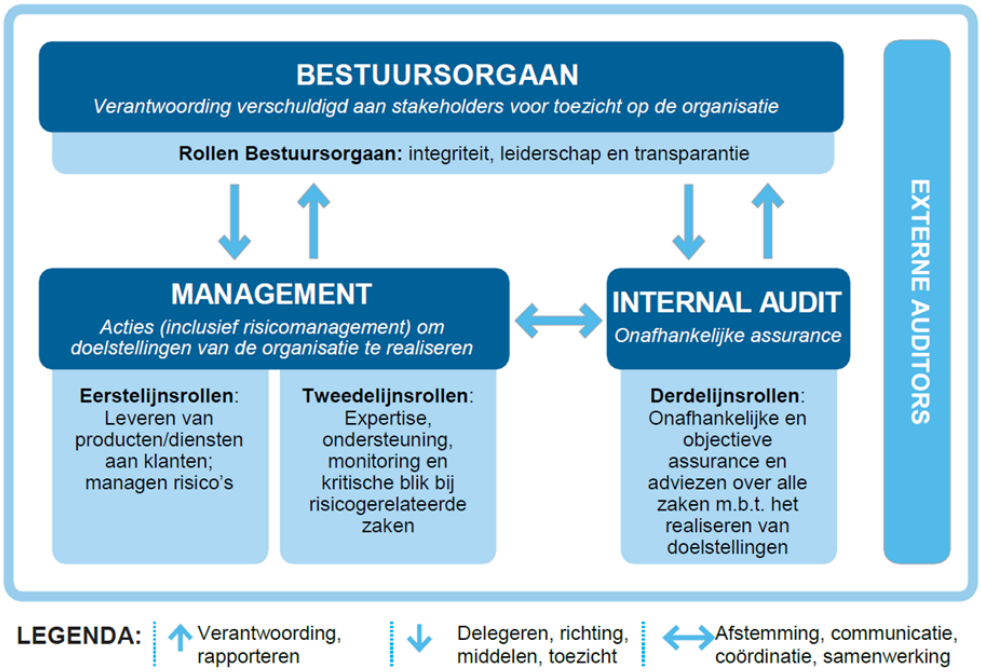
De methodiek van risicomanagement vormt daarvoor de basis en is daarom een integraal onderdeel van dit beleidsdocument.

2.2 Doelgroep

Elke medewerker van UWV heeft een rol in risicomanagement. Immers, alle medewerkers werken mee aan het behalen van de doelen, worden bij de uitvoering van hun werk geconfronteerd met onzekerheden en hebben een oplossing nodig om met

vertrouwen verder te kunnen werken. Daarom geldt het genoemde risicoleiderschap en het daaraan verbonden risicomanagement voor alle medewerkers van UWV.

Voor de besturing van de organisatie gebruikt UWV het 'drie lijnen model' (Zie afbeelding 1). Ook dit model is van toepassing op risicomanagement omdat de collega's die de eerste, de tweede en de derde lijn vertegenwoordigen een rol hebben in risicomanagement. Elke lijn heeft een eigen rol die duidelijk is omschreven. In het hoofdstuk Governance worden de rollen nader toegelicht.



Afbeelding 1: het drie lijnen model

Het eigenaarschap van risico's ligt, per definitie, in de eerste lijn. De rol om de risico-eigenaar uit te dagen en (waar nodig) te faciliteren ligt nadrukkelijk bij de tweede lijn. Bij FEZ ligt het stelseleigenaarschap voor risicomanagement. Daarmee is FEZ verantwoordelijk voor de opzet, het bestaan en de werking van het door haar geformuleerde beleid dat in dit document is vastgelegd. De derde lijn doet de controle op de werking van het totale risicomanagementsysteem van UWV.

Daarmee heeft iedere lijn dus een eigen verantwoordelijkheid en rol in risicomanagement en behoort daarmee tot de doelgroep van dit beleid.

Het risicomanagementbeleid van UWV sluit aan bij het risicomanagementbeleid van het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) en de Sociale Verzekeringsbank (SVB). Zo wil UWV komen tot een breed bruikbare methodiek en een gemeenschappelijke taal die de samenwerking tussen de partijen bij (de verdere ontwikkeling van) risicomanagement kan bevorderen.

2.3 Reikwijdte

Dit risicomanagementbeleid vormt de basis voor de inrichting van integraal risicomanagement bij UWV en is daarom van toepassing op alle onderdelen en niveaus van de organisatie. De uitgangspunten voor risicomanagement, de werkwijze en de daarbij behorende gemeenschappelijke taal, vormen de basis zonder dat de eigen verantwoordelijkheden en rapportagelijnen van verschillende expertises worden overgenomen. Bij expertises kun je denken aan Informatiebeveiliging en Privacy (IB&P), Misbruik en Oneigenlijk Gebruik, Compliance en Integriteit. Zij hebben eigen beleid op het vlak van hun expertise en gebruiken mogelijk een eigen, afgeleide werkwijze met betrekking tot risicomanagement op de voor hen relevante inhoud. Wel wordt de uitkomst van hun werk geïntegreerd in een integraal beeld van risico's en de mate van beheersing van deze risico's voor UWV als gehele organisatie. Over deze aansluiting worden operationele afspraken gemaakt met de relevante expertises. Deze afspraken maken geen deel uit van het UWV-brede risicomanagementbeleid.

3. Het risicomanagementproces

3.1 Risicoleiderschap

Risicoleiderschap is het gedrag dat UWV van haar medewerkers verwacht als bijdrage aan goed risicomanagement. In essentie bestaat dit gedrag uit het bewust omgaan met onzekerheden (risico's en kansen). UWV heeft het gedachtengoed van risicoleiderschap, net als veel andere overheidsinstellingen, geadopteerd en verwerkt in de training en opleiding van medewerkers.

Het uitgangspunt bij risicoleiderschap is dat je risico's niet kan vermijden en er dus bewust mee om moet gaan. Dit noemen we risico-gestuurd werken. Risico-gestuurd werken wordt ingegeven door vraagstukken waar organisaties mee te maken krijgt die vaak complex zijn en waarvoor de oplossingen niet rechtlijnig zijn. We leven in een VUCA-wereld. VUCA staat voor *volatile, uncertain, complex & ambiguous*. In het Nederlands: veranderlijk, onzeker, complex en ambigu. Oplossingen voor problemen en/of risico's kunnen weer andere risico's opleveren. Tijdens de periode waarin we werken aan een oplossing kan de situatie zomaar veranderen.

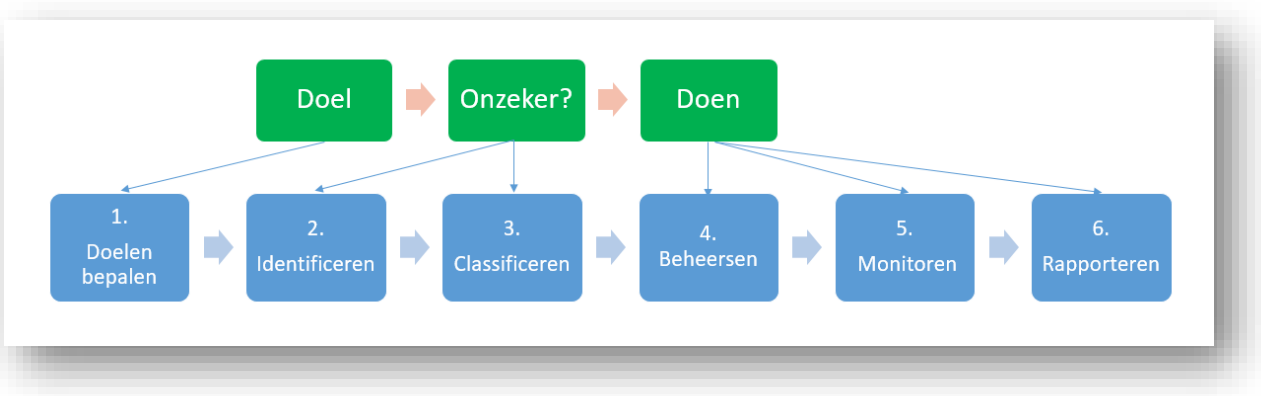
Risicoleiderschap is een essentieel onderdeel van risicomanagement. Het management zorgt voor de structuur waarlangs een dialoog over risico's met elkaar wordt aangegaan, de doelen worden afgestemd, onzekerheden (risico's en kansen) geanalyseerd en besluiten genomen (wat gaan we doen?).

Risicoleiderschap wordt in andere documenten uitgebreid beschreven en hier alleen herhaald omdat het een belangrijke basis vormt voor risicomanagement en het beleid in dit document.

3.2 Inleiding tot het risicomanagementproces

Het integraal risicomanagementproces van UWV bestaat uit 6 stappen. Dit zijn generieke stappen die overeenkomen met de verschillende, algemeen geaccepteerde, methodieken die binnen en buiten UWV in gebruik zijn. Daarmee hanteren we één overkoepelende en verbindende 'risicotaal', onafhankelijk van de methodieken die gebruikt worden voor specifieke risico-aspecten zoals de eerdergenoemde risico's met betrekking tot Informatiebeveiliging, Privacy en Misbruik & Oneigenlijk gebruik. Het generieke proces en de bijbehorende taal faciliteert het integrale risicomanagement van UWV.

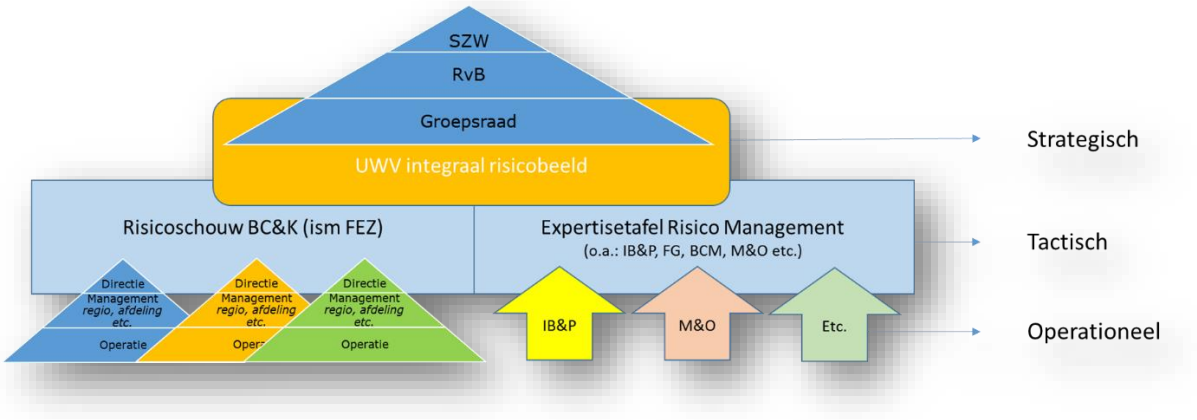
Daarnaast verbinden we ook de cultuur, de houding en het gedrag van risicoleiderschap aan dit proces. Risicoleiderschap beoogt risico-sturend gedrag te bevorderen waarbij de vragen 'wat is ons **d**oel?', 'wat is daarbij **o**nzeker?' en 'wat gaan we eraan **d**oen?' (D-O-D) centraal staan (zie afbeelding 2).



Afbeelding 2: De 6 stappen van het risicomanagement-proces verbonden aan de drie dagelijkse D-O-D-vragen van risicoleiderschap

Hoewel het proces hierboven lineair is weergegeven zijn deze processtappen ook cyclisch. De stappen worden periodiek herhaald. Hierbij wordt aangesloten bij de reguliere planning & control cyclus van UWV omdat risicomanagement een integraal onderdeel is van de besturing van de organisatie. Bij UWV gaan we uit van een jaarcyclus waarbij het jaarplan, en de daarin benoemde doelstellingen, de basis vormen van deze cyclus.

Verder is de verbinding tussen de verschillende onderdelen en niveaus van de organisatie ook een aspect van cyclische aard. Binnen dit proces voor integraal risicomanagement onderscheiden we drie niveaus: strategisch, tactisch en operationeel. Elk van deze niveaus is onderdeel van het risicomanagementproces. De niveaus zijn onderling met elkaar verbonden (Zie afbeelding 3).



Afbeelding 3: de lagen in het risicomanagement-proces

Om de risico's op de verschillende niveaus te behandelen besteden we in alle lagen van de organisatie aandacht aan de eigen risico's. Zo maken we het dagelijkse risicoleiderschap ook expliciet en onderdeel van een (cyclisch) proces. Dit doen we in risicodialogen waarin de hiervoor beschreven processtappen worden doorlopen met het verantwoordelijke management en medewerkers van de 1e lijn. Desgewenst worden zij daarbij ondersteund door functionarissen uit de 2e lijn. De sessies (risicodialogen) richten zich op het verantwoordelijkheidsgebied van dat management en de doelstellingen die daaraan gekoppeld zijn. Dit kan, bijvoorbeeld, ook gaan over projecten, programma's en klantreizen die horizontaal georganiseerd zijn. Binnen UWV worden de risicodialogen op tactisch en strategisch niveau ook wel aangeduid met de term 'risicoschouw'.

Al deze elementen vormen samen de integrale risicomanagementwerkwijze van UWV die hierna in meer detail wordt uitgelegd.

3.3 Risicodialogen & Risicoschouw BC&K

Het risicobeeld stellen we vast in risicodialogen, waarbij - ten minste - de volgende vragen centraal staan:

- Wat zijn de doelstellingen? / Zijn de doelstellingen nog hetzelfde?
- Wat zijn de onzekerheden? / Zijn de onzekerheden nog hetzelfde? / Zien we nieuwe onzekerheden?
- Wat is de voortgang op de implementatie/ effectiviteit van de bestaande maatregelen en de status van de (extra) beheersmaatregelen die in de vorige sessie zijn vastgesteld?
- Wat betekent dit voor het netto risico (onder of boven de risico-bereidheid,-zie stap 4 beheersen)?
- Wat doen we met nieuwe onzekerheden?

Bij risicodialogen is de 1e lijn leidend. Zij zijn primair verantwoordelijk voor de doelstellingen en de beheersing van onzekerheden (risico's en kansen). De 2e lijn faciliteert de dialogen waar nodig.

Voor de werking van risicomanagement is het essentieel om de uitkomsten van de risicodialoog vast te leggen. Vastlegging gebeurt in het uniforme risicoregister. De

vastlegging bestaat uit de uitkomsten van de betreffende risicodialoog zoals de risico's die zijn geïnventariseerd, de beheersmaatregelen die zijn afgesproken en wie verantwoordelijk is voor de uitvoering van die beheersmaatregelen. Daarnaast wordt vastgelegd voor welke netto-risico's (rest-risico) escalatie naar een hoger niveau noodzakelijk is. Meer informatie over de vastlegging en alle aspecten daarvan zijn terug te vinden in het uniforme risicoregister (zie bijlage II).

Het lijnmanagement van de 1e lijn is verantwoordelijk voor het omgaan met de risico's en het implementeren en opvolgen van de gekozen maatregelen. In dit proces heeft de 2e lijn een faciliterende rol en vervult daarnaast een rol in het kritisch meedenken met en het uitdagen van de 1e lijn. Zij leveren, bijvoorbeeld, ondersteuning bij de processtappen en periodieke rapportages over de risicomanagementactiviteiten.

Risicodialogen worden gehouden bij alle organisatieonderdelen en op alle lagen van het onderdeel: bij de operatie, in het regio of districtsmanagement en met de directie.

De verzamelde toprisico's per organisatieonderdeel vormen de basis van de **Risicoschouw BC&K** die tenminste twee keer per jaar wordt georganiseerd in het Functioneel Overleg van de hoofden BC&K. In deze risicoschouw wordt besproken wat uit de toprisico's zijn voor UWV die voortkomen uit de risicoregisters en wat de status van de beheersing op deze top-risico's is . Dit wordt vervolgens aangevuld door de Expertisetafel Risicomanagement.

3.4 Expertisetafel Risicomanagement

De expertisetafel risicomanagement is het gremium waarin de expertises met een organisatie--brede risicoverantwoordelijkheid samenwerken om tot een integraal risicobeeld te komen. Een aantal van de expertises heeft ook eigen beleid en/of achterliggende wetgeving die hun werkwijze vormgeeft en een daaraan verbonden, eigen risicomanagement methodiek en/of vastlegging (register). Het is belangrijk dat deze risico's bij elkaar komen om een integraal beeld van de risico's en de mate van beheersings voor heel UWV te kunnen vormen. Veel van deze thema's zijn een subcategorie van de vier hoofdcategorieën die door UWV worden onderscheiden. De expertises die aan de risicotafel vertegenwoordigd zijn:

- Compliance
- Portfoliobureau
- Informatie Voorziening
- Juridische zaken
- Informatiebeveiliging en Privacy
- Misbruik en Oneigenlijk gebruik
- Business Continuity Management
- Bureau Integriteit
- Issue Management
- Human Resource Management
- Financieel Economische Zaken

Waar nodig wordt de tafel aangevuld met nieuwe expertises waar die ontstaan of met bestaande expertises voor zover die niet al onderdeel zijn van het risicomanagementproces.

3.5 Het risicomanagementproces in 6 stappen

Stap 1: Doelen bepalen

Het bepalen van doelen is een verantwoordelijkheid van de 1e lijn van UWV en vormt een belangrijk onderdeel van de besturing. Deze doelen hebben niet alleen betrekking op veranderingen maar ook op de reguliere uitvoering. Er zijn, bijvoorbeeld, kwalitatieve en kwantitatieve doelen. Het bepalen van doelen is geen specifiek risicomanagementproces maar vormen wel het startpunt voor risicomanagement. De 2e lijn heeft een belangrijke, ondersteunende rol. Zij dagen de 1e lijn uit op de kwaliteit (SMART) van de doelstellingen. Het jaarplan is de vastlegging van de (strategische) jaardoelen en (tactische en operationele) doelstellingen en daarmee is het jaarplanproces een belangrijke input van het risicomanagementproces.

Stap 2: Identificeren

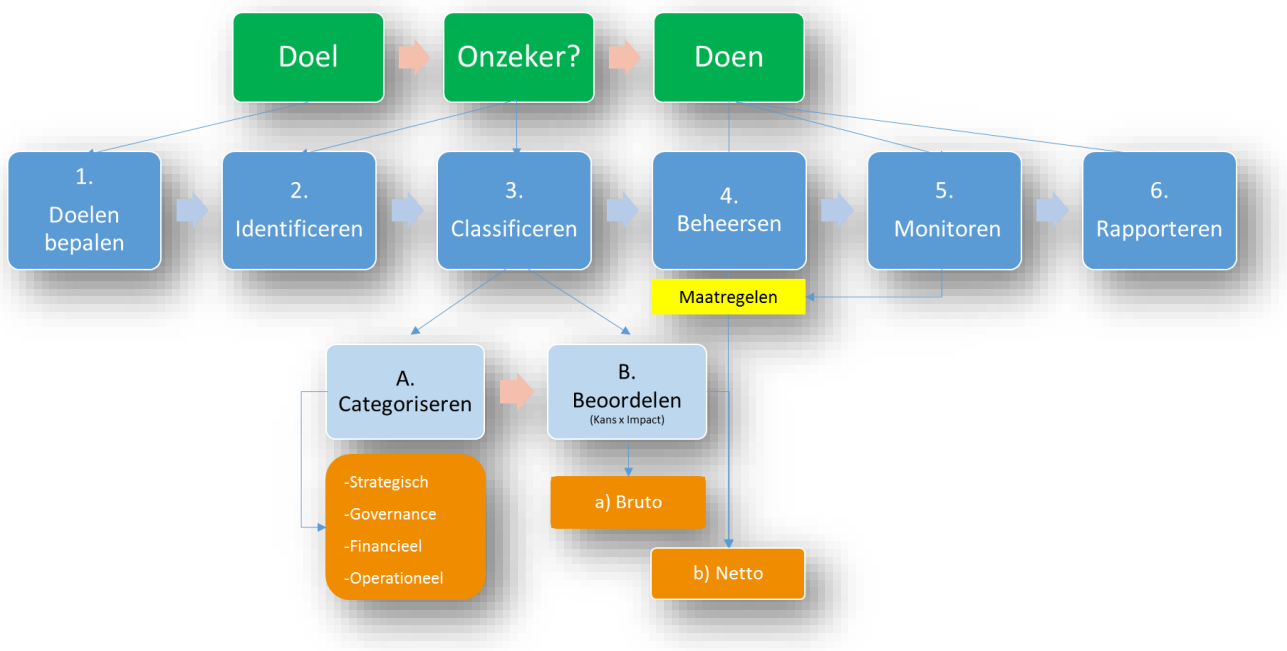
Het identificeren van risico's op de te realiseren doelen is een onderdeel van het risicomanagementproces en van risicoleiderschap. Ieder organisatieonderdeel houdt risicodialogen om te komen tot een overzicht van alle relevante risico's. Voor de dialoog over risico's zijn verschillende vormen (methoden en technieken) mogelijk. De 2e lijn begeleidt veelal de dialoog over risico's en vervult daarnaast een rol in het kritisch meedenken met en het uitdagen van de 1e lijn. Elk organisatieonderdeel van UWV houdt de dialoog over risico's met de medewerkers in de uitvoering en middel- en hoger management. Voor de relevante onderdelen (per laag) wordt geadviseerd om tenminste twee keer per jaar een volledige dialoogsessie over risico's te organiseren en één keer een update te geven, in lijn met de reguliere Planning & Control cyclus die loopt in tertalen. Het vastleggen van de uitkomsten van de risicosessies vindt plaats in het risicoregister. De 2e lijn faciliteert bij de vastlegging. De risicorapportages (stap 6 in het risicomanagementproces) hanteren de vastlegging van de risicosessies/ risicoregisters als basis.

Naast de periodieke dialogen kan ook gebruik worden gemaakt van risicomeldpunten die binnen bepaalde organisatieonderdelen zijn ingericht. Dit is een extra mogelijkheid om risico's te verzamelen buiten het bestaande, cyclische proces.

Urgente risico's moeten natuurlijk niet wachten op een cyclisch proces maar worden via de reguliere hiërarchie behandeld in lijn met risicoleiderschap en waar nodig omhoog gebracht via de lijn. Deze risico's worden opgenomen in het risicoregister.

Stap 3: Classificeren

Het classificeren van risico's is een wat uitgebreidere stap in het risicomanagementproces en is een verantwoordelijkheid van de 1e lijn. Het classificeren van risico's bestaat uit twee stappen: A) categoriseren en B) beoordelen zoals in afbeelding 4 (hieronder) te zien is en daarna verder wordt toegelicht in de tekst.



Afbeelding 4: Het volledige risicomanagementproces inclusief een verdieping op het proces van classificeren

Het classificeren van risico's bestaat uit het indelen van de risico's op het type risico (A) plus de beoordeling van de omvang van het risico. De omvang van het risico wordt bepaald aan de hand van de kans dat het risico zich voordoet en de impact die het risico heeft op het te realiseren doel (B), dat laat zich samenvatten in de formule:
Risico omvang = Kans $*$ Impact.

Stap 3A: Categoriseren

Het indelen van risico's in categorieën is bedoeld om de risico's met een gelijksoortig karakter te groeperen. Het biedt structuur en overzicht wat weer bijdraagt aan goed risicomanagement, zeker binnen een omvangrijke en complexe organisatie als UWV. Het is nu mogelijk om de risico's tussen de organisatieonderdelen, binnen een organisatieonderdeel, op verschillende niveaus en per categorie te bekijken en de belangrijke thema's in de breedte en diepte van het bedrijf te herkennen.

Er is een zekere mate van overlap in de indeling van risico's. Een operationeel risico kan, bijvoorbeeld, door de impact die het risico heeft op de reputatie van de organisatie een strategisch risico worden. Ook daarom blijft het goede gesprek over risico's noodzakelijk.

De indeling helpt ook in het controleren of je volledig bent. Is bij het identificeren van risico's aan alle categorieën gedacht?

De veronderstelling is juist dat de indeling van risico's een zeker verband heeft met de doelstellingen van de organisatie. Risico's houden rekening met de mogelijkheid dat de gestelde organisatiedoelstellingen niet worden behaald.

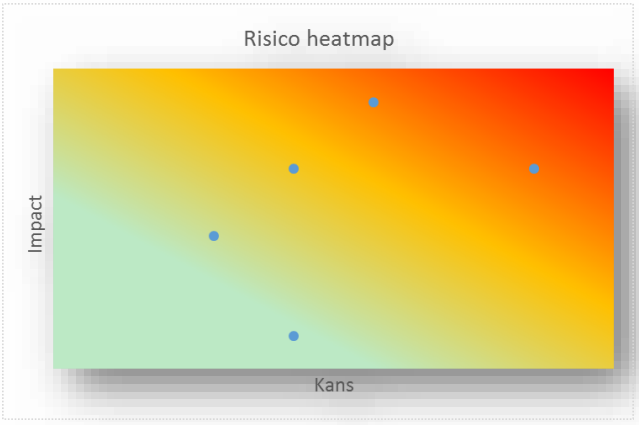
De indeling in (hoofd)categorieën is gebaseerd op de indeling die het ministerie van SZW en de ketenpartners gebruiken. Door aan te sluiten bij deze indeling kunnen we op dat niveau helder en eenduidig over de categorieën communiceren. Op subcategorieniveau

is de indeling aangepast aan de situatie bij UWV. Risico's worden binnen UWV ingedeeld in de volgende vier hoofdcategorieën:

Strategisch	Het risico dat UWV strategische doelstellingen niet realiseert omdat we niet of in onvoldoende mate op (significante) veranderingen binnen en buiten de organisatie reageren.
Governance	Het risico dat UWV strategische doelstellingen niet realiseert door onduidelijke of conflicterende taken en/of besturing, binnen (onderdelen van) UWV of tussen UWV en ketenpartners. Het risico op het niet voldoen aan de geldende wet- en regelgeving (compliance).
Financieel	Het risico van ineffectieve en/of inefficiënte beheersing van de financiële opzet, financiering en liquiditeitsrisico's. Ook de financiële gevolgen van operationele risico's worden onder deze categorie geschaard. Rechtmatigheid is daar een voorbeeld van.
Operationeel	Het risico van het niet behalen van operationele doelstellingen in brede zin door tekortschietende of falende (interne) processen, middelen, mensen en/of systemen, of door externe factoren.

Stap 3B: Beoordelen

Om de gesignaleerde risico's tegen elkaar af te wegen en in te delen naar prioriteit is een onderlinge beoordeling nodig. Dit doen we door, voor elk risico, de kans dat het risico voorkomt en de dan optredende impact voor de organisatie in te schatten en deze twee factoren met elkaar in verband te brengen. Dit wordt aangeduid als 'Kans maal Impact'. Op deze manier brengen we alle soorten risico's binnen hetzelfde wegingskader. Vaak wordt dit grafisch weergegeven in een heatmap (Afbeelding 5). Daarbij worden de grootste risico's rechts bovenin (rood) weergegeven. De blauwe stippen in de grafiek zijn voorbeelden van de risicoweergave op een heatmap. In principe gebeurt dit allereerst voor de voorkomende risico's, zonder inachtneming van eventuele beheersmaatregelen die zijn getroffen. Dit zijn de inherente risico's of bruto-risico's.



Afbeelding 5: Risico heatmap

Kans

Om een geïdentificeerd risico te meten moet de kans dat een risico zich voordoet worden ingeschat. Dit gebeurt veelal door een inschatting te maken van de waarschijnlijkheid of frequentie dat het risico zal optreden in de toekomst. Voor het inschatten van de waarschijnlijkheid of frequentie houdt UWV de onderstaande vijfpuntschaal aan:

Omschrijving	Getal	Indicatie op basis van frequentie	q
Zeer klein	1	Komt de komende 10 jaar waarschijnlijk niet voor want heeft zich in meer dan 10 jaar niet voorgedaan.	0-20
Klein	2	Komt waarschijnlijk binnen 5-10 jaar voor want heeft zich in de afgelopen 10 jaar voorgedaan.	20-40
Redelijk	3	Komt waarschijnlijk binnen 1-5 jaar voor want heeft zich in de afgelopen 5 jaar voorgedaan.	40-60
Groot	4	Komt meerdere keren per jaar voor want heeft zich in het afgelopen jaar voorgedaan.	60-80
Zeer groot	5	Komt meerdere keren per kwartaal voor want heeft zich in het afgelopen kwartaal voorgedaan.	80-100

De indicatie bij deze vijfpuntsschaal voor de Kans is nog niet voor alle soorten risico's even passend, op basis van voortschrijdend inzicht en in samenwerking met de interne en externe ketens gaan we op dit punt verder ontwikkelen. Er moet benadrukt worden dat het gaat om een referentietabel en geen wiskundige indicatie. Het expertoordeel blijft een belangrijk element om tot een juiste weging te komen.

Impact

De impact van een risico voor de organisatie (zie bijlage IV) wordt, afhankelijk van het soort risico, uitgedrukt in mogelijke gevolgen. Om tot een uniforme weging voor de impact van risico's op UWV te komen is een wegingskader opgesteld. Dit is een referentietabel waarbij het expertoordeel een belangrijk element vormt om tot een juiste weging te komen. Hierna volgt een samenvatting van de categorieën van het wegingskader en de beoordelingsaspecten die daarbij relevant zijn. Een meer gedetailleerde versie vind je in bijlage IV.

Hoofdcategorieën	Beoordelingsaspecten
Strategisch *continuïteit, omgeving, publieke opinie, keten-afhankelijkheid*	• Uitvoering kerntaken UWV. • Uitvoering veranderagenda UWV. • Impact op publieke opinie mbt UWV en politieke gevolgen.
Governance *sturing, cultuur, verantwoording en compliance*	• Inrichting organisatie versus gewenste besturing UWV. • Volledigheid en juistheid van stuur- en verantwoordingsinformatie versus geformuleerde doelstellingen. • Volledige en juiste vertaling van relevante wet- en regelgeving naar UWV-beleid (compliance).
Financieel *financiële opzet, financiële rechtmatigheid, liquiditeit, financiële verantwoording*	• Juiste en volledige verantwoording van rechten en plichten. • Solvabiliteit en liquiditeit. • Rechtmatigheid van vergoedingen. • Juistheid, volledigheid en tijdigheid van betalingen.
Operationeel *proces, uitbesteding, juridisch, integriteit, IT, HR, M&O, calamiteit*	• Procesuitvoering is juist, tijdig en volledig, conform beleidsregels en uitkomsten Meting Operationele Kwaliteit (MOK). • Proceskwaliteit[1] - score klanttevredenheid en kans op klachten. • Kleine geldstroom - mogelijk efficiencyverlies en mogelijke claims en boetes. • Kans op misbruik en oneigenlijk gebruik. • Kwantiteit personeel - bezetting versus budget en beschikbaarheid back-ups voor essentiële functies. • Kwaliteit personeel - uitkomsten periodieke schouw. • IT-aspecten beschikbaarheid (continuïteit), integriteit en vertrouwelijkheid - gerelateerd aan, onder andere, de geldende BIO-normen. [1] *gerelateerd aan de vraag of de klant zich gezien, gehoord en geholpen voelt*

Kans maal Impact

Risico's bestaan uit een factor Kans en een factor Impact. Om praktische redenen wordt aan beide factoren een getal toegekend en met elkaar vermenigvuldigd om de grootte van de risico's te bepalen. De hoogste getallen geven de grootste risico's weer. De hoogste getallen komen meer rechtsboven in de heatmap.

De uitkomst is een indicatie van de grootte van het risico en geen exacte, mathematische meting. Vaak worden kans en impact uitgedrukt in een oneven serie getallen waarbij een indeling in drie en vijf het meest voorkomen. Binnen UWV hanteren wij zowel voor Kans als voor Impact een vijfpuntschaal.

De risico's, uitgedrukt als cijfermatige vermenigvuldiging van Kans en Impact, ziet er als volgt uit:

Risico						
Kans		1	2	3	4	5
Impact		Zeer laag	Laag	Gemiddeld	Hoog	Zeer hoog
5	Zeer groot	5	10	15	20	25
4	Groot	4	8	12	16	20
3	Redelijk	3	6	9	12	15
2	Beperkt	2	4	6	8	10
1	Minimaal	1	2	3	4	5

Een goede categorisering en beoordeling van het risico is belangrijk om ook het vervolg van het proces goed uit te kunnen voeren. Ondersteuning en facilitering door de 2e lijn kan hier een belangrijke bijdrage aan leveren. Met name voor de toprisico's, de risico's die niet op het eigen niveau beheerst kunnen worden, is dit essentieel. De risico's die de organisatieonderdelen aanleveren voor de risicoschouw met FEZ en BC&K worden in lijn met deze methode beoordeeld.

Stap 4: Beheersen

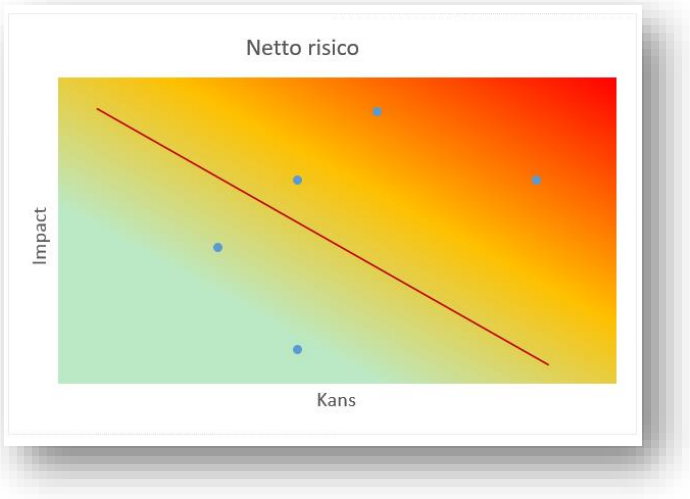
Hoe er wordt omgegaan met een risico is aan de 1e lijn. In eerste instantie wordt vastgesteld hoeveel risico acceptabel is. Met andere woorden: Wat is de risicobereidheid?

Risicobereidheid

De uitkomst van het netto-risico wordt vergeleken met de risicotolerantie die de organisatie heeft. Deze tolerantie noemt men 'risk appetite' of risicobereidheid. Als het netto-risico minder is dan de risicobereidheid wordt het risico geacht afdoende te zijn beheerst. Om beide met elkaar te kunnen vergelijken wordt de risicobereidheid in dezelfde termen vermeld als de uitkomst van het netto-risico.

Als voorbeeld: Als met behulp van de cijfermatige benadering is bepaald dat de maximale risicotolerantie 12 bedraagt dan zijn alle netto-risico's die hoger scoren onacceptabel. Dat moeten we dan aandacht geven, bijvoorbeeld in de vorm van extra of andere beheersmaatregelen.

Schematisch kan dat er zo uitzien:



Afbeelding 6: Risicobereidheid in de risico heatmap

De rode lijn geeft aan hoe de risicobereidheid is bepaald binnen een organisatie. De risicobereidheid wordt vastgesteld door het hoogste orgaan. Bij UWV is dat de Raad van Bestuur. Binnen UWV wordt de risicobereidheid periodiek vastgesteld en waar nodig ook periodiek bijgesteld.

Afhankelijk van de risicobereidheid verloopt de grens meer naar rechtsboven (meer risicobereid) of naar linksonder (minder risicobereid – risico avers) en worden er daarmee grotere, respectievelijk kleinere risico's geaccepteerd.

In dit voorbeeld valt een drietal risico's buiten de tolerantie omdat ze groter zijn dan de risicobereidheid (boven de lijn). Deze risico's vragen dus aanvullende aandacht.

Risicoreactie

In de theorie van risicomanagement wordt vaak gesproken over vier T's die helpen bij het kiezen van de juiste reactie op een risico. De vier T's zijn: Treat (mitigeren), Transfer (overdragen), Tolerate (accepteren) en Terminate (vermijden). De 1e lijn kijkt in haar risicoreactie naar deze vier T's en maakt vervolgens een keuze uit:

- De behandeling (Treat) van het risico, waarbij zowel het beperken (mitigeren) van de kans als het beperken van de impact mogelijk is. Dit wordt gedaan door het treffen van beheersmaatregelen.
- De overdracht van het risico (Transfer) waarbij zij (een deel van) de impact van het risico naar een andere partij overdragen.
- De acceptatie (Tolerate) van het risico waarbij de uitkomst van de weging valt binnen de risicobereidheid; het risico is te gering om er nadere aandacht aan te besteden. Valt het risico buiten de grenzen van de risicobereidheid, waarbij de beheersmaatregelen het risico onvoldoende mitigeren, dan accepteert het hoger liggend management het risico.

- Het laten vervallen (Terminate) van een doelstelling waarbij de conclusie is dat de doelstelling op basis van het vastgestelde en gewogen risico niet langer haalbaar is of het behandelen van het risico niet opweegt tegen de waarde van de doelstelling.

Van bruto- naar netto-risico

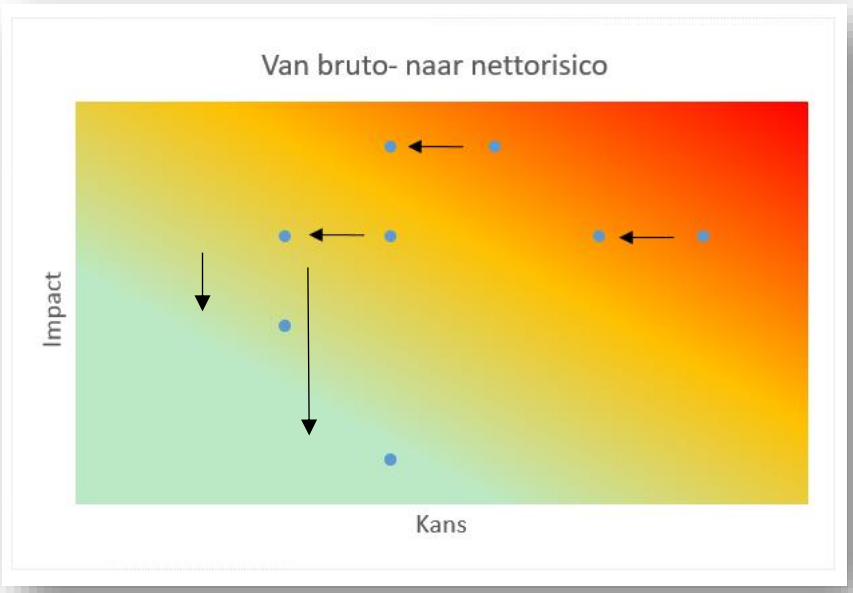
De beredenering van risicomanagement is om eerst het bruto (of: inherente) risico in te schatten. Dit risico doet zich voor zonder aantoonbare werking van beheersmaatregelen (of: controls) die het betreffende risico mitigeren. Daarna maakt de 1e lijn, met ondersteuning van de 2e lijn, een analyse van de getroffen beheersmaatregelen en bepaalt bij de aantoonbare werking van de beheersmaatregelen het verwachte netto-risico.

Wat dan nog moet gebeuren is het vaststellen dat de maatregelen zijn ingevoerd en aantoonbaar effectief zijn om het bruto-risico daadwerkelijk te mitigeren. Tenzij het bruto-risico is geaccepteerd zoals het is.

Wat overblijft is het netto-risico (of rest-risico). Het is de verantwoordelijkheid van de 1e lijn om aan te tonen dat de afgesproken maatregelen aantoonbaar effectief zijn. De 2e lijn beoordeelt de effectiviteit van de maatregelen. Deze beoordeling kan BC&K uitvoeren maar kan ook door andere 2e lijnfunctionarissen worden gedaan. Bijvoorbeeld voor specifieke onderwerpen zoals cybersecurity, integriteit, privacy, compliance etc.

Effectief werkende maatregelen kunnen een risico verkleinen door de kans te verminderen en/of de impact te beperken. Een cijfermatig voorbeeld: als de bruto-kans dat een risico zich voordoet op 4 wordt ingeschat, en de impact is dan ook 4, dan komt het bruto-risico uit op 16. Als er maatregelen zijn ingesteld die de kans verkleinen naar 2 dan wordt het netto-risico 8.

De volgende heatmap (Afbeelding 7) geeft de beweging weer van bruto- naar netto-risico van de drie bruto-risico’s die zich buiten de risicobereidheid bevinden. Bij één risico wordt duidelijk gemaakt dat kan worden ingezet op reductie van de kans, reductie van de impact of een combinatie van beide. De mogelijkheden voor reductie zijn afhankelijk van de aard van het risico. Van de twee minder grote bruto-risico’s wordt aangenomen dat deze dermate beperkt zijn dat er geen extra beheersmaatregelen nodig zijn (Tolerate).



Afbeelding 7: risicobeheersing (verschuiving van bruto naar netto) in de risico heatmap

De werking van beheersmaatregelen is belangrijk om te zorgen dat het netto-risico op een acceptabel niveau komt ten opzichte van de risicobereidheid. De keuzes die hierin worden gemaakt zijn de verantwoordelijkheid van het management van de 1e lijn.

Stap 5: Monitoren

Het monitoren van de werking van maatregelen is een belangrijke activiteit om te beoordelen of het netto-risico daadwerkelijk binnen de risicobereidheid valt of daar komt binnen de daarvoor gestelde termijn. Het eigenaarschap van de aantoonbare werking van maatregelen ligt, per definitie, bij de 1e lijn. Het monitoren van de werking van maatregelen is een taak van de risico-eigenaar. De risico-eigenaar is degene die verantwoordelijk is voor de doelstelling waarop het risico van toepassing is. Het uitdagen op de status van de genomen maatregelen in zowel de opzet, het bestaan en de werking is een verantwoordelijkheid van de 2e lijn. Daarbij spreekt voor zich dat de 2e lijn het eigenaarschap van de maatregelen niet overneemt. De status van de maatregelen en het effect op het netto-risico legt BC&K vast in het risicoregister.

Stap 6: Rapporteren

Rapportage betreft alle communicatie met betrekking tot risico's (onzekerheden) en de maatregelen die worden getroffen om de onzekerheden te beheersen. Dat kan in een formele vorm zoals hieronder staat beschreven in de P&C-cyclus maar ook alle informele communicatie die van toepassing zijn bij risicoleiderschap.

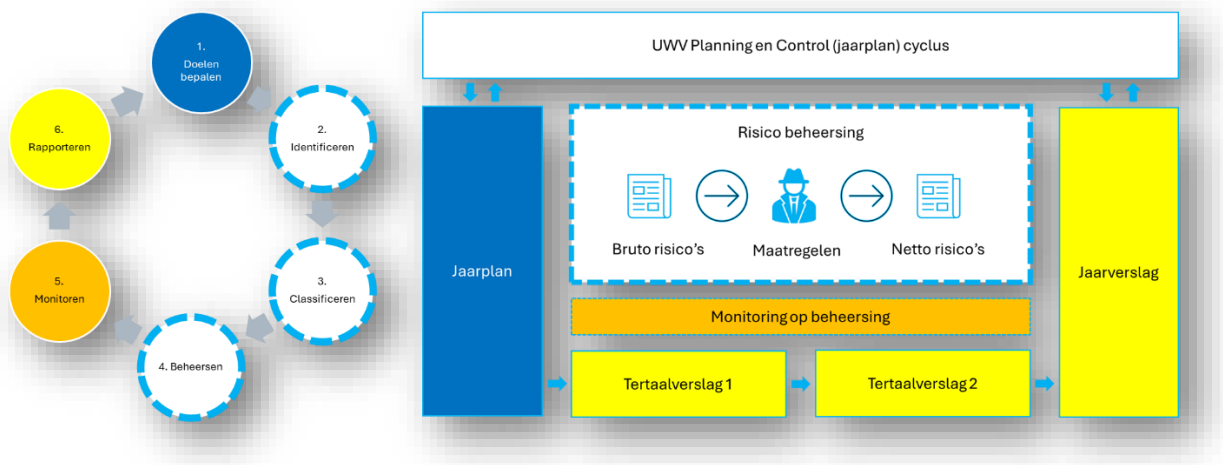
Planning & control cyclus

Binnen de planning en control-cyclus van UWV wordt periodiek gerapporteerd over risicomanagement. Een belangrijk startpunt is het jaarplan waarin ook structureel een risicoparagraaf opgenomen is en natuurlijk de doelstellingen benoemd zijn waarop de risico's van toepassing zijn. De organisatieonderdelen (1e lijn) rapporteren maandelijks aan FEZ (2e lijn). Elke vierde maand (tertaal) wordt door het organisatieonderdeel gerapporteerd over de voortgang op de beheersing van de risico's (in de tertaalrapportage van het onderdeel). Daarnaast wordt ook elk tertaal ook verantwoording afgelegd over de algehele beheersing van de risico's door UWV in de UWV tertaalrapportage.

Het lijnmanagement rapporteert over de gevoerde beheersing van de risico's binnen het eigen organisatieonderdeel. De 2e lijn rapporteert over de uitkomsten van de risicodialoog en de beoordeling en toetsing van de werking van de beheersmaatregelen. Daarnaast leveren de onderdelen elk tertaal hun (bijgewerkte) risicoregister aan bij FEZ Risicomanagement.

Verder zijn er diverse expertises die een eigen risicoregister hanteren zoals Informatiebeveiliging & Privacy (CISO-Office), voor Misbruik & Oneigenlijk gebruik (afdeling R&I van Handhaving) en voor de fiscale aspecten (HRM). Zij rapporteren elk tertaal aan de eigen managementlijn en aan FEZ.

Op basis van de risicoregisters stelt FEZ een integraal risico-overzicht samen van de top-risico's van UWV. Dit overzicht is onderdeel van de tertaalrapportages, het jaarverslag en de periodieke rapportages van UWV aan het Ministerie van SZW. Tevens vormt de inhoud van het integraal risico-overzicht de basis voor de halfjaarlijkse risicodialoog in de Groepsraad.



Afbeelding 8: risicomanagement en de planning en control cyclus van UWV

Uniform risicoregister

De status van risico's en de voortgang van beheersmaatregelen houden de BC&K-afdelingen van UWV bij in een risicoregister. Dit risicoregister wordt UWV-breed op uniforme wijze opgesteld. Daarvoor is een template beschikbaar (zie bijlage II). Het register dient als basis voor de risicomanagementrapportage binnen de planning en control cyclus van UWV en wordt ook ieder tertaal aangeleverd aan FEZ.

3.6 Issues, incidenten en de kwaliteitscyclus

Ondanks de inrichting van een risicomanagementproces en een cultuur van risicoleiderschap kunnen risico's ongeïdentificeerd blijven of realiteit worden. Er kan ingezet zijn op mitigerende maatregelen op de impact in plaats van maatregelen op de kans dat het risico zich voordoet waarmee de kans dat het risico zich manifesteert dus gelijk gebleven is. Ook kan het voorkomen dat de gekozen maatregelen op het beheersen van de kans (nog) niet effectief waren. Wat de reden ook is, zelfs bij een goed werkend risicomanagementproces zullen zich incidenten en issues manifesteren.

Het afhandelen van issues en incidenten is geen onderdeel van dit beleid, dat zich richt op de beheersing van risico's, maar wordt afgedekt in specifiek beleid en onderliggende processen voor deze thema's.

Een issue of incident geeft aanleiding om zowel terug te kijken als vooruit te kijken. Enerzijds kan dit, in overeenstemming met het kwaliteitsmanagementbeleid, leiden tot aanpassing van processen, systemen en producten. Anderzijds, om daadwerkelijk een lerende organisatie te zijn, kunnen issues of incidenten worden ingezet om het risicomanagementproces op basis van deze ervaringen te verbeteren. Denk dan aan de vraag waarom issues of incidenten niet als risico's geïdentificeerd waren of als ze wel geïdentificeerd waren waarom maatregelen niet of onvoldoende effectief waren. Alleen als deze vragen structureel beantwoord worden, wordt er voldoende invulling gegeven aan de kwaliteitsmanagementcyclus met betrekking tot risicomanagement.

4. Governance risicomanagement UWV

4.1 Drie lijnen model

De verantwoordelijkheden voor de interne beheersing zijn belegd in lijn met het drie lijnen-model dat UWV hanteert.

De 1e lijn in het besturingsmodel van UWV is de lijn van de Raad van Bestuur, directie, (staf)management en medewerkers. In beginsel is de 1e lijn er verantwoordelijk voor dat de organisatiedoelen van UWV worden bereikt en er sprake is van een goede beheersing van de belangrijkste risico's.

De 2e lijn (onder andere FEZ/BC&K en CISO/BSO) ondersteunt de 1e lijn en heeft daarin meerdere rollen. Zij zorgen ervoor dat:

- de 1e lijn geëquipeerd is om haar rol in risicomanagement adequaat uit te voeren;
- het risicomanagementproces goed is ingericht voor de organisatie;

- de stuurinformatie beschikbaar is en deze informatie binnen de organisatieonderdelen op de juiste plek terecht komt.

Daarnaast heeft de 2e lijn een bewakingsrol. Zij signaleren zaken die aan de aandacht van de 1e lijn zijn ontsnapt, analyseren de mogelijke consequenties en zorgen dat de signalen worden besproken aan de juiste overlegtafels. De 2e lijn van UWV wordt in de eerste plaats gevormd door de BC&K-afdelingen. Elk uitvoerend organisatieonderdeel heeft een BC&K-afdeling.

De stelselverantwoordelijkheid voor risicomanagement en de regie daarover is belegd bij de directie FEZ. Het zwaartepunt van de uitvoering van de 2e lijns-rol ligt in principe belegd bij de BC&K-afdeling van de organisatieonderdelen.

De 3e lijn in dit besturingsmodel heeft een belangrijke taak in het vaststellen of de 1e en de 2e lijn er samen in slagen om de organisatiedoelen op een juiste, tijdige en volledige manier te bereiken en velt daarmee, in dit geval, een oordeel over de werking van het totale risicomanagement. Bij UWV wordt de 3e lijn gevormd door de Auditdienst UWV en, voor privacyaspecten, ook door de Functionaris Gegevensbescherming (FG).

Hieronder zijn de taken en verantwoordelijkheden van de 1e en de 2e lijn weergegeven, per stap van het risicomanagement-proces[1]:

	1e lijn	2e lijn
Algemeen	Bepalen van de risicobereidheid (dit doet de hoogste leiding van de organisatie). Risico-eigenaarschap.	Adviseren en ondersteunen (zonder eigenaarschap over te nemen) bij alle stappen van het risicomanagementproces. Onder andere door het bijhouden van het risicoregister.
1. Doelen bepalen	Doelstellingen formuleren.	Het uitdagen van de, door de 1e lijn, geformuleerde doelstellingen.
2. Identificeren	Identificeren en wegen van de bruto-risico's.	Het faciliteren en uitdagen van de 1e lijn bij de risico-identificatie.
3. Classificeren		Het faciliteren en uitdagen van de 1e lijn bij de risico-classificatie.
4. Beheersen	Bepalen van de risicoreactie (mitigeren, overdragen, vermijden of accepteren). Implementeren en uitvoeren van beheersmaatregelen.	Beoordelen van en adviseren over de opzet en het bestaan van de, door de 1e lijn ingestelde, beheersmaatregelen.

[1] In lijn met de Basic risicomanagement, 2023

5. Monitoren	Monitoren van de voortgang van de implementatie van de beheersmaatregelen.	1e lijn uitdagen op de werking van de ingestelde beheersmaatregelen. Oordeel geven over de werking van beheersmaatregelen.
6. Rapporteren	Rapporteren over risico's als een regulier onderdeel van de planning en control-cyclus.	Het uitdagen van de 1e lijn bij het geschetste netto-risicobeeld zoals dat, per tertaal, gerapporteerd wordt door de organisatieonderdelen.

Risicomanagement Community

Daarnaast heeft UWV een risicomanagement community die een belangrijke rol heeft in de verbinding binnen de 2e lijn op de inhoud van risicomanagement en in de verbinding van de 1e en 2e lijn op deze inhoud.

Per organisatieonderdeel neemt tenminste één medewerker deel aan de risicomanagement community, daar waar er een BC&K afdeling is zal het een medewerker zijn van die afdeling.

Daarnaast nemen ook vertegenwoordigers van de expertises (in lijn met de deelnemers aan de Expertisetafel Risicomanagement) deel aan de risicomanagement community. Daarmee is er een brede vertegenwoordiging op zowel de verticale as (organisatieonderdelen) als de horizontale as (organisatie-brede expertises).

De community zorgt voor zowel verbinding op inhoud en voor de ontwikkeling van risicomanagement tussen de organisatieonderdelen en expertises en FEZ als stelselverantwoordelijke. De deelnemers aan de risicomanagement community hebben een belangrijke dubbelrol, in de community vertegenwoordiger ze hun onderdeel of expertise en binnen hun onderdeel of expertise vertegenwoordigen ze risicomanagement. Zij dragen de verantwoordelijkheid hun kennis actief te delen in zowel de community als in hun eigen omgeving en dan zowel richting de tweede lijn waarin zij veelal werken als vanuit die tweede lijn naar hun eigen eerste lijn. De risicomanagement community wordt gefaciliteerd door FEZ.

4.2 Risicomanagement als onderdeel van besluitvorming[2]

Ter voorbereiding op de besluitvorming beschrijft de 1e lijn de risico's en kansen die verbonden zijn aan de doelen van het besluit. De 2e lijn voorziet de voorstellen die ter besluitvorming worden aangeboden aan het directieteam (DT) of managementteam (MT) van een gevraagd (of ongevraagd) advies voor het management. De 2e lijn (in dit geval FEZ en BC&K) heeft daarbij aandacht voor het budgetbeheer, het te volgen beleid, de bevoegdheden, de consistentie van voorstellen, de risicobeheersing, de informatievoorziening, de financiële gevolgen, de rechtmatigheid en doelmatigheid, de administratieve organisatie/ interne controle (AO/IC) en de compliance.

[2] Bron: Position paper FEZ en BC&K, 2023

Ook wordt aandacht gegeven aan de risico's, als onderdeel van de interne besluitvorming. Dit kan op verschillende manieren. Bijvoorbeeld door risico's als vast onderdeel op te nemen in de voorlegger die standaard wordt meegeleverd met stukken voor besluitvorming door DT of MT.

Om de, voor besluitvorming aangeboden, voorstellen te kunnen beoordelen en te adviseren bij de besluitvorming is het nodig dat FEZ en/of BC&K betrokken zijn bij alle besluitvormende overleggen van UWV. Onder besluitvormende overleggen wordt, in ieder geval, verstaan:

a) Vergaderingen van de Raad van Bestuur van UWV;
b) Overleggen van directie(team) en overleggen van het district/rayon;
c) Overleggen van stuurgroepen (van projecten).

4.3 Risicomanagement als onderdeel van projectuitvoering[3]

Veel doelen van UWV worden gerealiseerd in projecten. Daarmee zijn projecten een integraal onderdeel van risicomanagement binnen UWV. We relateren de uitvoering van risicomanagement op projecten en op andere soorten van grootschalige veranderingen bij voorkeur aan beslismomenten. De projectstart wordt als een belangrijk beslismoment gezien. Het centrale Portfoliobureau van UWV monitort de levenscyclus van alle centraal gecoördineerde projecten binnen de organisatie en adviseert de Raad van Bestuur en de directie op basis van de verschillende projectstuurdocumenten die in de projectmethodiek worden opgesteld. Daarnaast zijn er ook decentrale portfoliobureaus ingericht binnen UWV.

Binnen ieder projectplan schenken we, op basis van de projectmethodiek, aandacht aan de risico's van het project. Deze worden ook periodiek (tenminste 3x per jaar) binnen de stuurgroep besproken.

Bij het aanbieden van projectplannen geeft het portfoliobureau een integraal advies. Het portfoliobureau geeft dit advies in de voorlegger.

Dit is ook van toepassing bij het aanbieden andere projectstuurdocumenten zoals het projectvoorstel, de afwijkingsrapportage en het dechargerapport. Indien het project niet de expliciete aandacht heeft van de Raad van Bestuur, dan geeft het portfoliobureau haar advies aan de opdrachtgevende directeur. Het kwaliteitskader van het portfoliobureau geldt daarbij als leidraad en niet als checklist. Er wordt vooral gekeken of er sprake is van een adequate projectbeheersing voor het realiseren van de gestelde projectdoelen.

Aan elk project van UWV is capaciteit vanuit BC&K toegekend, in lijn met de reguliere bedrijfsvoering. Daarmee ligt ook expliciet de 2e-lijns rol met betrekking tot risicomanagement voor het project bij BC&K. Overkoepelend is deze rol belegd bij het portfoliobureau.

[3] Bron: Kwaliteitskader Portfoliobureau, 2021

Vanuit haar centrale rol heeft het Portfoliobureau daarmee ook de verantwoordelijkheid om risico's over de projecten uit de portfolio heen te registreren (portfolio risicoregister), de voortgang van de realisatie van de maatregelen te monitoren en daarover te rapporteren. Dus stappen 5 en 6 van het risicomanagementproces met betrekking tot centrale portfolioprojecten ligt in de 2e lijns-rol van het Portfoliobureau. Voor decentrale projecten geldt dat voor de decentrale projectbureaus.

Een algemene regel is dat bij, zowel de start van een project als bij de overdracht naar de reguliere organisatie, een risicosessie wordt uitgevoerd. Verdere details zijn uitgewerkt in de UWV-projectmanagement methode (UPM).

Bijlage I – Begrippenlijst

Beheersmaatregelen (controls)	Procedures, richtlijnen, processtappen en overige afspraken en activiteiten die zijn gericht op het beheersen van risico's. Beheersmaatregelen zijn gericht op het verminderen van het bruto-risico. *Zie ook risicoreactie.*
BIO	Baseline Informatiebeveiliging Overheid: Het minimale basisniveau van informatiebeveiliging waar UWV aan moet voldoen.
Bruto-risico (inherent risico)	Risico's zonder rekening te houden met beheersmaatregelen die al zijn getroffen.
Governance	Governance betekent het uitvoeren van beleid, de controle op deze uitvoering, de verdeling van taken, bevoegdheden en verantwoordelijkheden en de gedragsregels en principes binnen een organisatie.
Heatmap	Manier om risico's grafisch weer te geven in relatie tot elkaar.
Mitigeren	Risico's verkleinen, door de kans en/of impact te verminderen.
Netto-risico (rest-risico)	Risico's rekening houdend met getroffen beheersmaatregelen. Netto-risico = bruto-risico minus werkende beheersmaatregelen. Ook wel restrisico genoemd.
Risico	Mogelijk nadelig effect op het bereiken van een doelstelling. Risico's kunnen worden gezien als een combinatie van kans en impact.
Risicobereidheid (risk appetite)	Mate waarin een organisatie bereid is om risico te accepteren.
Risicocategorie	Groep waarin op vergelijkbare wijze te meten risico's worden samengevoegd.
Risicoleiderschap[4]	Een risicoleider is een formele of informele leider, die doelgericht en realistisch durft om te gaan met onzekerheden, de daaruit voortkomende relevante risico's en kansen.
Risicomanagement	Het stelsel van afspraken, processen en procedures aan de hand waarvan een organisatie haar risico's beheerst.

[4] Iedereen risicoleider - waarde realiseren én behouden in een onzekere wereld, Martin van Staveren, 2020

Risicoreactie	De reactie die een organisatie heeft op een risico gelinkt aan de risicobereidheid van de desbetreffende organisatie. Er zijn 4 risicoreacties: accepteren, mitigeren, overdragen en vermijden. *Zie ook beheersmaatregelen.*
Risicoregister	Vastlegging van relevante geïdentificeerde risico's waarin bruto-risico, beheersmaatregelen en netto-risico worden weergegeven.
Expertisetafel Risicomanagement	Verzameling (veelal centraal gepositioneerde) specialisten met regie-voerende taken op hun expertisegebied. Vooralsnog betreft het o.a. de volgende afdelingen: • DHH/R&I (misbruik & oneigenlijk gebruik, SUWI) • CISO-Office (informatiebeveiliging & privacy) • FG (privacy) • Bureau Integriteit (integriteit, interne frauderisico's) • FEZ (financieel-administratieve organisatie) • JZ (juridische aspecten en compliance) • HRM (personele aspecten, fiscale aspecten) • Issue Management (communicatieve aspecten van reputatiemanagement) • SBK (algemene beleidsonderwerpen, afstemming met SZW) • Compliance (niet SUWI wetgeving). Voor de regie op het onderwerp compliance algemene wet- en regelgeving staan verschillende directeuren opgesteld, maar die zullen waarschijnlijk niet worden verzameld aan deze tafel.
Wegingskader	Systematiek om risico's met elkaar te vergelijken.
Werking (van maatregelen)	Ook wel: effectiviteit. Mate waarin beheersmaatregelen (controls) effectief zijn in het verminderen van het bruto-risico.

Bijlage II – Uniform risicoregister

Ten behoeve van de registratie van de beheersing van risico's wordt gebruik gemaakt van een risicoregister (op dit moment in Excel).

Het template bevat de volgende elementen:

- Identificatienummer
- Datum risico-identificatie
- Categorie
- Proces/Onderwerp
- Doelstelling (Doel)
- IT-systeem (indien van toepassing)
- Risico (Onzekerheid): het risico dat …
- Oorzaak: doordat …
- Gevolg: met als gevolg dat …
- Kans
- Impact
- Bruto-risico (kans * impact)
- Risico-reactie
- Beheersmaatregelen (Doen)
- Kans
- Impact
- Netto-risico (kans * impact)
- Oordeel over de werking van de beheersmaatregelen
- Eigenaar beheersmaatregel(en)
- Datum laatste herijking risicoregister
- Eventuele opmerkingen

Bijlage III – De risicomanagement-kalender van UWV

Risicomanagement heeft een voortdurend karakter, maar vindt plaats in cycli die aan de planning & control cyclus zijn gekoppeld. De generieke planning ziet er als volgt uit:

Inhoud	Eigenaar	Januari	Februari	Maart	April	Mei	Juni
Risicoregister	Onderdeel	15e				15e	
Risicoparagraaf in jaarplan / tertaal verslagen / jaarverslag per onderdeel	Onderdeel	Conform P&C cyclus				Conform P&C cyclus	
Risicoparagraaf in jaarplan / tertaal verslagen / jaarverslag centraal UWV	FEZ		FEZ				FEZ
Risicoschouw BC&K	FEZ		BC&K				BC&K
Risicodialoog RvB/GR	FEZ						RVB
Expertisetafel Risicomanagement	FEZ		Expertise				Expertise
Community	FEZ			Community		Community	
Jaarlijkse evaluatie	FEZ				Evaluatie beleid		
Trainigen	FEZ/Academie				Training		

Inhoud	Eigenaar	Juli	Augustus	September	Oktober	November	December
Risicoregister	Onderdeel			15e			
Risicoparagraaf in jaarplan / tertaa lverslagen / jaarverslag per onderdeel	Onderdeel			Conform P&C cyclus			
Risicoparagraaf in jaarplan / tertaal verslagen / jaarverslag centraal UWV	FEZ				FEZ		
Risicoschouw BC&K	FEZ				BC&K		
Risicodialoog RvB/GR	FEZ				RvB		
Expertisetafel Risicomanagement	FEZ				Expertise		
Community	FEZ			Community		Community	
Jaarlijkse evaluatie	FEZ						
Trainigen	FEZ/Academie					Training	

Deze planning is globaal opgezet en wordt jaarlijks aangepast aan de planning & control cyclus waar nodig. De onderdeelplanning wordt lokaal gemaakt op dusdanige wijze dat de centrale planning op de juiste manier gevoed kan worden met relevante informatie.

Bijlage IV – Wegingskader UWV

Referentietabel Classificatie Risico's - voorbeeld beoordeling impact per categorie

	1 – Minimaal	2	3 - Redelijk	4	5 – Zeer groot
Strategisch *continuïteit, omgeving, publieke opinie, keten-afhankelijkheid*	Uitvoering kerntaken UWV volledig gerealiseerd		Kerntaken grotendeels gerealiseerd *(> 95% realisatie)*		Uitvoering kerntaken UWV ernstig belemmerd *(< 90% realisatie)*
	Uitvoering verandering UWV volledig gerealiseerd *(bijvoorbeeld werkagenda 2021-2025, Integrale Klantreis etc.)*		Verandering UWV grotendeels gerealiseerd *(bijv. werkagenda 2021-2025, Integrale Klantreis etc.)*		Uitvoering verandering ernstig belemmerd *(bijv. werkagenda 2021-2025, Integrale Klantreis etc.)*
	Problemen met incidentele/geringe impact in media en/of geen reactie vanuit SZW		Problemen met meervoudige/enige verwachte impact in media en/of mogelijk doorvragen vanuit SZW *(bijv. meerdere krantenartikelen of TV programma's)*		Problemen met langdurige/aanzienlijke verwachte impact in media of op ministerie/minister SZW *(bijvoorbeeld Parlementaire Enquête)*
Governance *sturing, cultuur, verantwoording en compliance*	Inrichting organisatie past volledig bij gewenste besturing		Inrichting organisatie past niet (meer) geheel bij gewenste besturing		Inrichting organisatie past niet (meer) bij gewenste besturing
	Stuur- e/o verantwoordingsinfo dekt geformuleerde doelstellingen nagenoeg volledig af		Dekt geformuleerde doelstellingen deels af *(< 90% van de geformuleerde doelstellingen)*		Serieus hiaat in stuur- e/o verantwoordingsinfo info *(< 80% van de geformuleerde doelstellingen)*
	Vertaling van toepassing zijnde wet- en regelgeving en beleid hierop is volledig		Vertaling van toepassing zijnde wet- en regelgeving en beleid hierop is grotendeels gerealiseerd		Vertaling van toepassing zijnde wet- en regelgeving en beleid hierop is niet adequaat
Financieel *financiële opzet, financiering, liquiditeit, rechtmatigheid, financiële verantwoording*	Rechten en plichten zijn volledig in zicht en betrouwbaar verwerkt		Rechten en plichten zijn grotendeels in zicht en betrouwbaar verwerkt		Rechten en plichten onvolledig in zicht en/of niet betrouwbaar verwerkt
	Solvabiliteit en liquiditeit inzichtelijk en op orde		Solvabiliteit en liquiditeit inzichtelijk zijn grotendeels op orde		Solvabiliteit en liquiditeit niet inzichtelijk en/of op orde

	1 – Minimaal	2	3 - Redelijk	4	5 – Zeer groot
	Rechtmatigheid is nagenoeg volledig *(0% van vergoedingssoort onrechtmatig vastgesteld)*		Rechtmatigheid is grotendeels gerealiseerd *(± 0,5% van vergoedingssoort onrechtmatig vastgesteld)*		Rechtmatigheid is onvolledig *(> 1% van vergoedingssoort onrechtmatig vastgesteld)*
	Juiste en volledige betaling *(afwijking 0% van vergoedingssoort)*		Geringe onjuiste of onvolledige betaling *(afwijking < 0,5% van vergoedingssoort)*		Onjuiste of onvolledige betaling *(afwijking > 1% van vergoedingssoort)*
	Grotendeels tijdige betaling *(kleine groep klanten < 1 werkdag)*		Beperkte te late betaling *(grotere groep klanten ± 2 werkdagen te laat betaald)*		Te late betaling *(grote roep klanten > 3 werkdagen te laat betaald)*
Operationeel *proces, , uitbesteding, juridisch, integriteit, IT, HR, M&O, calamiteit*	Procesuitvoering conform beleid *(bijvoorbeeld: Meting Operationele Kwaliteit hoger dan 95%)*		Procesuitvoering grotendeels conform beleid *(bijvoorbeeld: Meting Operationele Kwaliteit hoger dan 90%)*		Procesuitvoering niet conform beleid *(bijvoorbeeld: Meting Operationele Kwaliteit lager dan 90%)*
	Proceskwaliteit: gering effect op score klanttevredenheid en kleine kans op klachten *(klant voelt zich nog steeds gezien, gehoord en geholpen)*		Proceskwaliteit: beperkt effect op score klanttevredenheid en stijging op klachten *(klant voelt zich beperkt gezien, gehoord en geholpen)*		Proceskwaliteit: groot effect op score klanttevredenheid en substantiële groei klachten *(klant voelt zich niet gezien, gehoord en geholpen)*
	Kleine geldstroom: geen efficiencyverlies of boete *(0% productiviteitsverlies of lager dan € 50.000)*		Kleine geldstroom: gering efficiencyverlies of boete *(± 0,5% productiviteitsverlies of ± € 500.000)*		Kleine geldstroom: groter efficiencyverlies of boete: *(> 1% productiviteitsverlies of > € 1 mln)*
	Kwantiteit personeel: bezetting op gepland niveau en back-ups voor essentiële functies beschikbaar		Kwantiteit personeel: bezetting ± 5% onder gepland niveau en/of niet voor alle essentiële functies back-ups beschikbaar		Kwantiteit personeel: bezetting > 10% onder gepland niveau en/of vrijwel geen back-ups beschikbaar voor essentiële functies
	Kwaliteit personeel: uitkomst periodieke schouw bevredigend		Kwaliteit personeel: uitkomst periodieke schouw onvoldoende		Kwaliteit personeel: uitkomst periodieke schouw alarmerend

	1 – Minimaal	2	3 - Redelijk	4	5 – Zeer groot
	IT: aspecten beschikbaarheid, integriteit en vertrouwelijkheid voldoen *(bijvoorbeeld: compliant aan de geldende BIO-normen)*		IT: aspecten BIV voldoen beperkt aan UWV-doelstellingen *(bijvoorbeeld: compliance BIO-normen op UWV planning)*		IT: aspecten BIV voldoen niet aan UWV-doelstellingen *(bijvoorbeeld: compliance BIO loopt achter op UWV planning)*

Referentietabel beoordeling Kans - deze indeling is met name bruikbaar voor operationele risico's aangezien deze op frequentie gebaseerd is (processen)

Omschrijving	Getal	Indicatie
Zeer klein	1	Komt waarschijnlijk de komende 10 jaar niet voor, heeft zich meer dan 10 jaar of nog nooit voorgedaan
Klein	2	Komt waarschijnlijk binnen 5-10 jaar voor, heeft zich de afgelopen 5 jaar voorgedaan
Redelijk	3	Komt waarschijnlijk binnen 1 of 2 jaar voor, heeft zich de afgelopen 2 jaar voorgedaan
Groot	4	Komt meerdere keren per jaar voor en heeft zich het afgelopen jaar voorgedaan
Zeer groot	5	Komt meerdere keren per kwartaal voor en heeft zich afgelopen half jaar voorgedaan