Dechargerapport project Sonar IB&P

Opdrachtgever: 5.1 lid 2 sub e

12 januari 2023

Projectmanagers	5.1 lid 2 sub e 5.1 lid 2 sub e
Projectcode	UN0929
Versie:	1.0

Managementsamenvatting

Het project Sonar IB&P is succesvol afgerond; de 77 KPMG-bevindingen zijn allen opgelost, binnen de geplande tijdslijnen en ook (ruim) binnen het (bijgestelde) budget. Oplossen betekent hier dat het risico volledig is gemitigeerd of dat er sprake is geweest van een formele (gedeeltelijke) risicoacceptatie. Om dit te bereiken zijn 142 verbeteracties uitgevoerd, waarmee een zeer omvangrijke risicoreductie is gerealiseerd. De restrisico's zijn helder in kaart gebracht, behandeld door onafhankelijke experts (in de Quality Assurance Commissie) en formeel geaccepteerd op het juiste niveau (alle restrisico's zijn behandeld in de Stuurgroep en afgestemd met de Domeinhouders, 2 restrisico's zijn eveneens behandeld bij het DT WB, en de op voorhand voorziene restrisico's waren reeds behandeld bij de Regiegroep en hoeven daarom niet nogmaals langs de Stuurgroep te gaan). Er zijn nog twee overdrachtspunten: deze acties zijn voorbereid en in gang gezet, maar de afronding is overgedragen aan de lijnorganisatie, omdat het moment van uitvoering in de tijd afhankelijk is van externe invloeden. De opvolging van deze acties is gepland in de eerste helft van 2023. De vanuit dit project gecreëerde rol 'IB&P Risicomanager' is een belangrijke factor in het toezicht op de restrisico's en restpunten, ondersteund middels het geïmplementeerde GRC-systeem.[1] Daarnaast heeft dit project bijgedragen aan een belangrijke verschuiving van eigenaarschap van het IB&P-thema binnen het WERKbedrijf. Het onderwerp is niet enkel meer "van IV en de BSO", maar wordt nu Directie-breed opgepakt. Waarbij ook de Domeinen en Uitvoering in hun rol zijn bekrachtigd.

Alle projectresultaten zijn binnen de gestelde termijn afgerond: de laatste bevinding is op 20 december 2022 gedechargeerd (waarbij de planning voor het afronden van de "middellange termijn-oplossingen", i.e. het oplossen van alle 77 bevindingen, eind 2022 was. De totale projectkosten bedragen € 4.785K (dit betreft de realisatie tot en met november en een prognose voor de komende periode) tegen een initiële kostenschatting van € 4.753K (inclusief een risico-opslag van € 500k). Deze initiële kostenschatting is in latere herijkingen nog (naar boven) bijgesteld; de details zijn beschreven in hoofdstuk Financiële consequenties.

Eind 2021 heeft adviesbureau EY in opdracht het projectmanagement de projectopzet beoordeeld, om te valideren dat de geplande acties tezamen het gewenste resultaat zouden bereiken (namelijk: het oplossen van alle 77 bevindingen). EY had enkele (relatief geringe) suggesties tot verbetering, welke reeds in de herijking van begin 2022 zijn opgenomen. Daarnaast heeft Accountantsdienst eind 2022 een onafhankelijk onderzoek gedaan naar de kwaliteitsborging in dit project (procesmatig, met steekproefsgewijze dossiercontroles). Alsmede de mate waarop de organisatie in staat is om continuïteit te geven aan de gerealiseerde verbeteringen. Hieruit zijn geen bevindingen naar voren gekomen die decharge van dit project in de weg staan. Daarbij stelt de Accountantsdienst voor om in de tweede helft van 2023 een vervolgonderzoek uit te voeren, gericht op de duurzaamheid van de verbetermaatregelen. De inhoud van de resultaten van dit onderzoek is beschreven in de rapportage van de Accountantsdienst.

Bijdrage aan organisatiedoelstelling

Met de inwerkingtreding van de AVG is vastgelegd dat er binnen UWV aan de aanvullende eisen uit de AVG ten opzichte van de Wbp (Wet bescherming persoonsgegevens) voldaan werd (de zogenaamde delta tussen de AVG en de Wbp). Tegelijkertijd werd erkend dat er nog grote stappen gezet moesten worden ten aanzien van de eisen die de Wbp al stelde, en die nu ook onder de AVG onverkort van toepassing zijn. Deze tekortkomingen zijn destijds ook in de u-toets AVG aan SZW gemeld.

Het (nog) niet volledig voldoen aan de Wbp/AVG kan (hoge) privacy risico's met zich meebrengen ten aanzien van de bescherming van persoonsgegevens van betrokkenen. Tevens kan UWV-sancties opgelegd krijgen voor deze tekortkomingen. Het is daarom van belang dat UWV kan aantonen in control te zijn op de bescherming van persoonsgegevens door het verbinden van acties aan de geïdentificeerde tekortkomingen, en door het bieden van een perspectief over wanneer de tekortkomingen in voldoende mate zijn opgelost.

[1] Voor de rol van "IB&P risicomanager" is geen aparte functie gecreëerd. Het verdient aanbeveling deze functie – UWV-breed – te standaardiseren en formaliseren. Zie verder ook punt 2 onder het kopje 'Adviezen en leerpunten' (p. 7).

Dit project heeft de gap tussen (het gebruik van) Sonar en de AVG (die is vertaald in het UWV-privacybeleid) verder gedicht. Het project levert daarmee een concrete en wezenlijke bijdrage aan het adequaat beschermen van persoonsgegevens van betrokkenen en daarmee het voldoen aan privacywet- en regelgeving.

Groep	Meerwaarde	Akkoord divisie (als eindgebruiker of namens klant)
Klant	De privacy van de klant wordt beter gewaarborgd. De klant moet erop kunnen vertrouwen dat zorgvuldig met zijn of haar persoonsgegevens wordt omgegaan, adequaat wordt beveiligd en alleen wordt verwerkt indien noodzakelijk.	WERKbedrijf
Medewerkers, andere divisies, gemeenten en andere externe gebruikers	In totaal heeft Sonar 16.000 gebruikers, waarvan een derde WERKbedrijf collega's zijn. De 'rest' van de Sonar gebruikers is verdeeld over de andere divisies, gemeenten en andere externe gebruikers. Dit project heeft de autorisaties van deze gebruikers verbeterd en aangescherpt, waardoor deze rollen voldoen aan de eisen van doelbinding en proportionaliteit.	WERKbedrijf
Gebruikers Sonar	Het bewustzijnsniveau van Sonargebruikers over privacy en informatiebeveiliging is verhoogd en wordt periodiek meegenomen in awarenessactiviteiten.	WERKbedrijf

Tabel 1 Bijdragen aan organisatiedoelstelling

Projectresultaat en scope

De hoofddoelstelling van het project is behaald, namelijk: het sterk reduceren van het IB&P-risiconiveau voor Sonar, door het oplossen van de 77 bevindingen uit het integrale KPMG-onderzoek op de IB&P-maatregelen rondom Sonar van 12 augustus 2020. Nota bene: het 'oplossen' van bevindingen omvat hierbij ook het accepteren van eventuele restrisico's op het juiste niveau van de organisatie. Er kunnen immers onderdelen van bevindingen zijn die – ondanks de mitigerende maatregelen die genomen zijn – niet volledig zijn weggenomen. Belangrijk is dat het risicobeeld van de bevindingen wel behoorlijk is gereduceerd. Afhankelijk van de risicoscore van het restrisico dient het restrisico te worden geaccepteerd op het niveau van de Stuurgroep, DT of Regiegroep/RvB (zie hieronder de paragraaf 'Dossier opbouw en wijzigingen' voor details).

De scope van dit project bestond uit het oplossen van de 77 KPMG-bevindingen, middels het uitvoeren van de in dit projectplan gedefinieerde deelprojecten en onderliggende verbeteracties. Voor elke bevinding zijn één of meer verbeteracties gedefinieerd. Bij het ontwerpen van deze verbeteracties is rekening gehouden met de mogelijkheden en beperkingen van de huidige Sonar-inrichting en de bedrijfsvoering. De tabel hieronder geeft de verdeling van de bevindingen over de deelonderzoeken en per opgegeven risicoclassificatie (hoog, midden, laag, conform criteria KPMG) weer.

	Aantal bevindingen per risiconiveau			
Deelonderzoek	**Hoog**	**Midden**	**Laag**	**Totaal**
Privacy	25	7	1	**33**
Identity & Access Management	9	7	1	**17**
Informatiebeveiliging: organisatorisch	7	8	1	**16**
Informatiebeveiliging: technisch	9	2	-	**11**
Totaal	**50**	**24**	**3**	**77**

Tabel - Aantallen KPMG-bevindingen per risiconiveau vanuit de vier deelonderzoeken

Het resultaat van het project is dat – door het oplossen van de 77 bevindingen – de staat van IB&P van en rondom Sonar aanzienlijk is verbeterd. Zowel technisch als procesmatig zijn er immers veel verbeteringen doorgevoerd (zie Bijlage A: Projectresultaten in detail). Sommige verbeteringen zijn ook

breder dan Sonar, zoals het opzetten van een UWV-brede awarenessactiviteiten en een proces voor kwetsbaarhedenscanning. Zie meer onder het kopje 'Gerealiseerde resultaten'.

Dossier opbouw en wijzigingen

Gedurende het project zijn op verschillende momenten herijkingen en aanscherpingen aangebracht in de aanpak van het project. Ten aanzien van het projectplan gaat het om de volgende herijkingen:

- December 2020-januari 2021: Herijking op het projectplan, na afronding van de "korte termijn"-fase (v1.10).
- December 2021-januari 2022: Het tweede herijkingsmoment betrof het projectmanagementplan (v1.20).

Herijking dechargeformulieren acties en bevindingen

Dit betreft de formulieren om individuele verbeteracties en bevindingen te dechargeren. De formulieren zijn in eerste instantie automatisch gevuld op basis van de gegevens in het projectplan (zie bijlage A van het projectplan, in Excel). Dit omvat ook verwijzingen van één dechargeformulier naar gerelateerde verbeteracties en bevindingen. Echter, sommige koppelingen zijn na herijkingen gewijzigd (i.e. nieuwe koppelingen en/of ontkoppelingen), waardoor er in sommige dechargeformulieren van met name acties kan worden verwezen naar andere verbeteracties en bevindingen, waartussen in de uiteindelijke versie van het projectplan geen koppeling meer bestaat. Het projectteam heeft zorggedragen dat de verwijzingen naar onderliggende acties in de bevindingen-formulieren correct zijn, maar de daaronder liggende documentatie is niet ook retrospectief aangepast.

De opzet van de dechargeformulieren zijn t.a.v. herijkingen ook enkele malen gewijzigd. Bij het aanscherpen van de taakinvulling, is ook het stramien van de dechargeformulieren aangescherpt. Toegevoegd zijn:

- Getekende kwaliteitscheck van de PMO en BSO.
- Kopje voor specifieke vragen aan de QAC leden.
- Kopje voor specifieke opmerkingen vanuit de QAC leden.

Behandeling van restrisico's

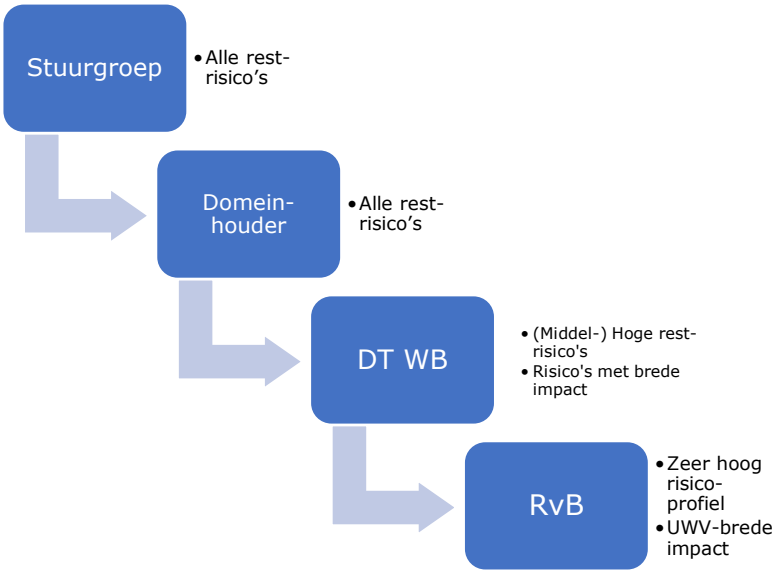
Zoals aangegeven onder 'Projectresultaat en scope' omvat het oplossen van bevindingen tevens het accepteren van eventuele restrisico's, na het nemen van mitigerende maatregelen waardoor het risiconiveau van de bevinding al (sterk) is gereduceerd. Bij de behandeling van restrisico's is de kans en impact berekend met een 5x5-schaal van het UWV. Dit leidt tot een risicoscore (zie Bijlage C: Restrisico's voor een overzicht van alle restrisico's met bijbehorende score).

Legenda Risico matrix						
	Kans	1	2	3	4	5
Impact		zeer klein	klein	redelijk	groot	zeer groot
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

	Risicoclassificatie	Risicoacceptatie door
	Zeer klein	Directie bedrijfsonderdeel, gedelegeerd aan domeinhouder/verantwoordelijk management
	Klein	Directie bedrijfsonderdeel, gedelegeerd aan domeinhouder/verantwoordelijk management
	Gemiddeld	Directie bedrijfsonderdeel
	Hoog	Directie bedrijfsonderdeel **en mogelijk** Raad van Bestuur

De hoogte van de risicoscore en de aard van het restrisico bepaalde op welk niveau van de organisatie het restrisico dient te worden voorgelegd. Alle restrisico's zijn ter accordering voorgelegd aan de Stuurgroep. Daarnaast zijn de verschillende domeinhouders actief geïnformeerd hierover. Twee restrisico's hebben een hogere score dan "(Zeer) Klein", namelijk beiden "Gemiddeld"; deze zijn ook voorgelegd aan het DT WB. Verder zijn in het projectplan vier op voorhand voorziene restrisico's

beschreven. Deze vier zijn gedurende het project nader met de Regiegroep afgestemd. Zie voor details over de restrisico's Bijlage C: Restrisico's.



Risico-acceptatieformulier (RAF)
Een RAF is gebruikt bij acties en bevindingen waarbij een restrisico resteert. Dit restrisico wordt omschreven in het RAF, bijgevoegd aan de actie of bevinding, en voorgelegd aan de QAC en de Stuurgroep. De opbouw van het RAF is gewijzigd in de loop van het project, waardoor er twee verschillende versies gebruikt werden. Het verschil is dat in de nieuwe versie een risicoberekening is opgenomen (kans * impact = risicoscore) aan de hand van het zojuist genoemde 5x5 diagram van het UWV.

Vernieuwde opzet QAC en samenvoeging T-QAC en O-QAC (per mei 2022)

De inzet en toetsing door de QAC is vanaf mei 2022 aangescherpt. De nadruk lag vanaf dat moment enkel op het geven van inhoudelijke opmerkingen vanuit de expertisegebieden van de QAC-leden, en geen opmerkingen meer over de vorm, begrijpelijkheid en bewijs bij de decharges. De QAC gaat daarbij uit van de juistheid van de gegevens in de decharge. BG en SBK nemen niet meer standaard deel aan de overleggen, tenzij specifiek is verzocht om opmerkingen door het PMO. Parallel werd er meer nadruk gelegd op de rol van PMO en de BSO. Beide partijen dienen vanaf dit moment een expliciete goedkeuring aan een actie of bevinding te geven.

Tevens geeft de QAC geen positief of negatief advies meer vanaf mei 2022. In plaats daarvan geeft de QAC-opmerkingen of aanvullende adviezen op acties en bevindingen. De bij de QAC ingediende stukken worden ook slechts eenmalig behandeld (uitzonderingen daargelaten). Dat wil zeggen dat acties en bevindingen – na behandeling in de QAC – altijd doorgaan naar de Stuurgroep.

Zoals eerder aangegeven waren er twee varianten van de QAC: de O-QAC (decharges van acties) en de T-QAC (decharge van bevindingen). In de loop van de tweede helft van 2022 is the T-QAC variant samengevoegd met de wekelijkse O-QAC. Dat wil zeggen dat decharge van bevindingen vanaf dat moment wekelijks werden behandeld in de QAC. De reden hiervan was dat – nadat steeds meer acties waren gedechargeerd – de focus begon te verschuiven naar het dechargeren van bevindingen en daarom meer bijeenkomsten nodig waren. Dit staat los van de zojuist besproken aangescherpte invulling van de QAC.

Gerealiseerde resultaten

Het project Sonar IB&P is succesvol afgerond; de 77 KPMG-bevindingen zijn allen opgelost, binnen de geplande tijdslijnen en ook (ruim) binnen budget. Oplossen betekent hier dat het risico volledig is gemitigeerd of dat er sprake is geweest van een formele (gedeeltelijke) risicoacceptatie. Om dit te bereiken zijn 142 verbeteracties uitgevoerd, waarmee een zeer omvangrijke risicoreductie is gerealiseerd. De restrisico's zijn helder in kaart gebracht, behandeld door onafhankelijke experts (in de

Quality Assurance Commissie) en formeel geaccepteerd op het juiste niveau. Ook zijn er twee acties (overdrachtspunten) voorbereid of in gang gezet, waarvan de uitvoering of afronding is overgedragen aan de lijnorganisatie, omdat het moment van uitvoering in de tijd afhankelijk is van externe invloeden. Het project heeft het Portfoliobureau WERKbedrijf verzocht toe te zien op de uitvoering hiervan. De vanuit dit project nieuw gecreëerde rol 'IB&P Risicomanager' is een belangrijke factor in het toezicht op de restrisico's en restpunten, ondersteund middels het geïmplementeerde GRC-systeem.[2] De tijdelijke risico's, die tot het moment van afronding van deze overdrachtspunten blijven bestaan tot en met uiterlijk de RW1 2023 release (juni 2023), zijn allen formeel geaccepteerd.

Met het oplossen van de 77 bevindingen zijn enorm veel IB&P-risico's gereduceerd en weggenomen. De belangrijkste verbeteringen aan het IB&P-risiconiveau zijn:

1. Begeleiden, opleiden en volwassen maken van het IB&P ambassadeursnetwerk. Het op strategisch en tactisch (landelijk) niveau bestaande privacy netwerk van de afdelingen IV Office en Bedrijfsmiddelen is uitgebreid met dit operationele netwerk van deskundige IB&P ambassadeurs op rayon- of regioniveau. Dit vormt een landelijk dekkend en uitvoerend actief privacy netwerk waarbij IM Office de kaders vaststelt en de IB&P specialisten instrueert.
2. Door de vele awarenessactiviteiten zijn medewerkers meer bewust van de risico's van gevoelige (persoons)gegevens. Veel van deze awarenessactiviteiten hebben een duurzaam karakter. Dat wil zeggen dat ze periodiek worden uitgevoerd (ook na het Sonar IB&P project), zoals de IB&P Game. Er is een awarenesskalender met activiteiten die ieder jaar opnieuw wordt opgezet.
3. Er heeft een eerste schoning plaatsgevonden vanuit het project in Sonar, waardoor veel overbodige (persoons)gegevens zijn verwijderd. Tevens is een verbeterd schoningsmechanisme (aangepaste schoningsscripts) ontwikkeld, getest en geïmplementeerd, waardoor het UWV periodiek schoning kan uitvoeren in Sonar.
4. De exportfunctionaliteit is uitgeschakeld, waardoor de kans op onzorgvuldige omgang van Excel-bestanden met persoonsgegevens behoorlijk is afgenomen.
5. Fijnmazige autorisaties zijn ingevoerd en duurzaam belegd, waardoor oneigenlijke toegang tot persoonsgegevens is verminderd. Fijnmazige autorisaties wil zeggen dat per functie is beoordeeld welke (persoons)gegevens noodzakelijk zijn. Voor gemeenten zijn de autorisaties ook aangescherpt, resulterende in dat gemeentemedewerkers alleen nog klanten kunnen raadplegen binnen hun eigen gemeente.
6. De C1 t/m C8 controles van het autorisatiecontrolemodel borgen het autorisatiebeheerproces. Het autorisatiecontrolemodel heeft tot doel periodiek autorisaties te beoordelen, zoals de juistheid van gekoppelde functierollen en een controle op de deltalijst.
7. Risicomanagement (lees: IB&P beheersingsraamwerk) geïmplementeerd en duurzaam belegd middels GRC Control. D.w.z. dat IB&P beheersingsmaatregelen – uit de BIO (Baseline Informatiebeveiliging Overheid) en de AVG (Algemene Verordening Gegevensbescherming) – zijn opgenomen in de tool, toegewezen aan eigenaren en worden periodiek getest.
8. Voor wat betreft wachtwoorden is aangesloten op de generieke OAM waarbij Sonar wachtwoorden conform UWV-richtlijnen zijn. Hierdoor worden sterke wachtwoorden gebruikt.
9. Functionele logging en monitoring is ingericht op raadplegen en muteeracties met betrekking tot Sonar.
10. Er is een proces ingericht voor kwetsbaarhedenscanning op Sonar. Bevindingen uit deze scans worden geprioriteerd en opgevolgd.

De projectresultaten worden in onderstaande tabellen nader uiteengezet. Van belang om op te merken is dat het risicobeeld van iedere bevinding met een restrisico doorgaans significant is afgenomen, omdat naast het restrisico andere onderdelen van de bevinding wel zijn opgelost. Restrisico's geven dus aan dat slechts een onderdeel van de bevinding niet is opgelost, waarvan het risico is geaccepteerd. De resterende bevinding is wel opgelost.

[2] Voor de rol van "IB&P risicomanager" is geen aparte functie gecreëerd. Het verdient aanbeveling deze functie – UWV-breed – te standaardiseren en formaliseren.

Deelonderzoek	Volledig gemitigeerd	Deels gemitigeerd en restrisico geaccepteerd	Totaal
Privacy	15	18	**33**
Identity & Access Management	4	13	**17**
Informatiebeveiliging: organisatorisch	12	4	**16**
Informatiebeveiliging: technisch	7	4	**11**
Totaal	**38**	**39**	**77**

Tabel Afrondingsstatus van bevindingen, per deelonderzoek KPMG

Deelproject	Totaal
Mens	**42**
Proces	**61**
Techniek	**39**
Totaal	**142**

Tabel 2 Afgeronde verbeteracties per deelproject

In Bijlage A: Projectresultaten in detail wordt per bevinding de resultaten en restrisico's weergegeven.

Niet of gedeeltelijk gerealiseerde resultaten

Niet van toepassing (alle beoogde projectresultaten zijn behaald).

Nog uit te voeren acties om resultaat alsnog te behalen

Een aantal acties (overdrachtspunten) zijn voorbereid of in gang gezet, waarvan de uitvoering of afronding is overgedragen aan de lijnorganisatie, omdat het moment van uitvoering in de tijd afhankelijk is van externe invloeden (zie Bijlage B: Overdrachtspunten).[3] De vanuit dit project nieuw gecreëerde rol van IB&P Risicomanager speelt een belangrijke rol in het toezicht op de restrisico's en restpunten, ondersteund middels het in dit project geïmplementeerde GRC-systeem. De tijdelijke risico's, die tot het moment van afronding van deze acties blijven bestaan, zijn allen formeel geaccepteerd door de Stuurgroep. Het Portfoliobureau WERKbedrijf dient na afronding van deze acties te worden geïnformeerd door de actiehouder.

ID	Onderwerp	Actiehouder	Acceptatie
OP1	De uitzondering die is gecreëerd waarbij 5 VRIM-medewerkers kunnen blijven exporteren (zie RR12) moet worden ingetrokken nadat de alternatieve gegevenslevering is gerealiseerd; momenteel gepland in de RW1 2023 release (juni 2023).	VRIM lijnmanager(s) van betreffende 5 medewerkers	Deelproject Proces
OP2	Ondanks onderzoek door WERKbedrijf FB zijn 70 schermen waar de autorisatiematrix naar refereert niet in kaart gebracht, omdat de schermen niet kunnen worden gevonden. Van deze schermen is nog onduidelijk of ze worden gebruikt. Volgens logging en monitoring (LOMO) is dat niet het geval. De nadere analyse hiernaar is overgedragen aan de lijn (beheer Sonar) (02.01.01c). Het gerelateerde restrisico is in detail beschreven in RR15.	Functioneel Beheer Sonar (IT WB)	Deelproject Proces

Adviezen en leerpunten

De belangrijkste en overkoepelende adviezen zijn hieronder beschreven. De gedetailleerde leerpunten, vanuit de onderliggende deelprojecten, zijn opgenomen in **Bijlage D: Leerpunten**. Het verschil is dat onderstaande punten meer adviezen zijn richting de staande organisatie en leerpunten zaken zijn die

[3] Daarnaast zijn er overige restpunten (RP), die niet direct bijdragen aan het behalen van het projectresultaat, maar wel de kwaliteit en het duurzame effect van enkele verbeteracties bestendigen. Zie daarvoor bijlage B.

door de organisatie kunnen worden gebruikt om te verbeteren of om te overwegen bij lopende en nieuwe trajecten.

- Het ontbreken van volwassen GRC-tooling bemoeilijkt het duurzaam inregelen van (IB&P-) verbetermaatregelen. Er bestaat dan immers geen centrale plek om beheersingsmaatregelen in te registreren en te monitoren. Het belangrijkste advies is om, zodra GRC-tooling beschikbaar is, alle verbetermaatregelen vanuit dit project met terugwerkende kracht op te nemen in het beheersingssysteem. Zodat er centraal, structureel en gestandaardiseerd toezicht kan worden gehouden op de effectieve werking hiervan. Wat overigens ook een aanzwengelende werking heeft.
- Voor een robuuste opvolging van (IB&P-) risico's is het verstandig een (gestandaardiseerde) functie/rol voor Risicomanager UWV-breed in te richten. Deze rol is vanuit dit project nieuw gecreëerd bij het WERKbedrijf, maar de wens bestaat deze vorm te geven in een vaste en organisatie-breed gestandaardiseerde functie. De Risicomanager kan, met behulp van de hierboven benoemde GRC-tooling, zorgdragen dat (IB&P-) risico's gestructureerd worden geïdentificeerd, geregistreerd, opgevolgd en gemonitord.
- Het ontbreken van gestandaardiseerde document-stramienen (zoals een risico-acceptatieformulier) heeft voor extra administratieve belasting gezorgd. Het advies is om veelgebruikte documentvormen te inventariseren, te standaardiseren en zorg te dragen dat de stramienen hiervoor eenvoudig toegankelijk zijn.
- De Quality Assurance Commissie is een onmisbaar onderdeel van de kwaliteitsborging van dit project geweest. De opzet en de benodigde tijdsinspanning hiervoor zijn gedurende het project meermaals ter discussie gesteld. Het advies is om, op basis van de inzichten vanuit dit traject, goede procesafspraken te maken aan het begin van een soortgelijk toekomstig project, waarbij dergelijke input van tweedelijnsfuncties nodig is.
- Het inrichten en beleggen van data-eigenaarschap en risico-eigenaarschap. Als immers niet bekend is van wie welke data is is het lastiger om risico's met betrekking tot deze data te koppelen aan eigenaren. Het advies is om data-eigenaarschap en risico-eigenaar te implementeren in de organisatie, als onderdeel van de verdere inrichting van risicomanagement.

Planning en financiën

Start- en einddatum	Startdatum	Augustus 2020
	Oorspronkelijke einddatum	31-7-2022
	Werkelijke einddatum	12-1-2023

Financiële consequenties

	Kostensoort	Totaal initieel begroot**	Totaal werkelijk	Verschil
Eenmalige projectkosten*	Intern	€ 914	€ 1.088	€ 174
	Extern	€ 2.522	€ 3.056	€ 534
	Automatisering:			
	• Hardware	€ 0	-	-
	• Standaard Software	€ 0	-	-
	• Spraak & Dataverbindingen	€ 0	-	-
	Uitbesteed ICT Leveranciers	€ 1.177	€ 492	-€ 685
	Overig	€ 140	€ 149	€ 9
	Totaal	**€ 4.753**	**€ 4.785**	**€ 32**

* *De eenheid van alle bedragen is € 1.000 en bedragen zijn in voorkomende gevallen inclusief BTW.*
** *Initieel begroot is het eerst vastgestelde projectplan.*

Structurele kosten	Divisie/Directoraat	Initieel per jaar	Werkelijk per jaar	Verschil
	WERKbedrijf	€ 495	€ 939	€ 444
	Totaal	**€ 495**	**€ 939**	**€ 444**
Structurele baten	**Divisie/Directoraat**			
	WERKbedrijf	€ 0	€	€
	Totaal	€ 0	€	€

De totale werkelijke kosten zijn gebaseerd op de realisatie van de kosten tot en met november 2022 en een prognose voor december en afronding in januari 2023.

In december 2020 is het eerste projectplan van het project SONAR IB&P goedgekeurd. De ingeschatte begroting voor het gehele project bedroeg toen € 4.753 met een looptijd tot en met juli 2022. In mei 2021 volgde een herijkt projectplan (v1.10), waarbij de inschatting van de totale projectkosten zijn toegenomen van € 4.753 tot € 8.933K. Toename van de risicobuffer, kosten voor verbeterinitiatief risicomanagement, verbeteren autorisatiebeheer, fine tuning planning en doorlopende kosten projectmanagement zorgden voor deze stijging. De risicobuffer was gesteld op € 3 miljoen. Daarmee werd de risico-opslag verhoudingsgewijs gekoppeld aan de uitloopreserve in termen van tijd (1 miljoen per kwartaal). Het volgende herijkte projectplan (v1.20) dateert van maart 2022. In de projectplan is de verdeling van de begroting meer verdeeld over 2021 en 2022. In dit herijkte projectplan is de begroting naar beneden bijgesteld naar € 6.633K. Hierin is meegenomen een stijging van de kosten in verband de doorloop tot en met eind 2022 en een (administratieve) uitloop tot Q1 2023. De risicobuffer is echter weer naar beneden bijgesteld. Deze was gebaseerd op de uitloop die eventueel zou ontstaan door vertraging bij DXC en op eventuele technische werkzaamheden die uitgevoerd zouden moeten worden. Van beide is geen sprake geweest.

	Initieel	Herijking mei '21	Herijking feb. '22	Totaal werkelijk
Basisbudget	€ 4.253k	€ 5.933k	€ 4.785K	€ 4.727k
Risico-opslag	€ 500k	€ 3.000k	€ 1.848k	€ 58K
Totaal	**€ 4.753k**	**€ 8.933k**	**€ 6.633k**	**€ 4.785K**

Zoals in de bovenstaande tabel is te zien is de uiteindelijke realisatie echter nagenoeg gelijk aan de inschatting vanuit het eerste projectplan. Ondanks dat de verwachte einddatum een half jaar later is dan hierin werd ingeschat. Daarnaast zijn de risicobuffers, behalve voor het stukje administratieve uitloop in 2023, niet nodig geweest. Op kostensoortniveau zijn het aantal benodigde uren intern en extern hoger uitgevallen. Dit is met name het gevolg van het langer doorlopen dan oorspronkelijk begroot. De uitbesteedde leverancierskosten zijn echter lager. De overige kosten zijn nagenoeg gelijk gebleven.

Structurele kosten
De structurele meerkosten zijn in kaart gebracht en afgestemd binnen WERKbedrijf. Op dit moment lopen er echter nog enkele inventarisaties bij IV Office met betrekking tot de inzet van capaciteit als gevolg van het project. Dit wordt komende 2 weken eventueel nog toegevoegd. Voor nu zijn de structurele kosten in geschat op € 939K per jaar, hiervan is € 104K al is opgenomen/geabsorbeerd in de begroting van 2023. De structurele kosten door het project zijn daarmee € 835K.

De structurele kosten zoals nu bekend zijn als volgt opgebouwd:
- € 100.000 vanwege het uitvoeren van een jaarlijkse pentest en het opvolgen van de resultaten
- 2,0 FTE voor de rol van Risicomanager en het uitvoeren van het autorisatiebeheer. Financieel is 1 FTE opgenomen in de begroting 2023 en 1 FTE via de structurele kosten van het project. (€ 104K opgevangen binnen bestaande begroting / € 104K nog meenemen in de structurele kosten).
- 2,0 FTE Centrale coördinatie ambassadeursnetwerk, IB&P coördinatie en opvolging opschoning Sonar (€ 203K)
- 3,25 additionele fte voor het IB&P Champion-netwerk. Dit is reeds belegd in de lijnorganisatie.
- 1,0 FTE Academie (€103K).
- 3,2 FTE Domeinconsultants met betrekking tot werkzaamheden rondom de BIO. (€ 325k).

Personele consequenties

Er zijn als gevolg van dit project 7,2 fte's gerelateerd aan – bestaande – IB&P-rollen toegevoegd aan het WERKbedrijf. Hiervoor zijn geen functiewijzigingen benodigd geweest. De paragraaf over structurele meerkosten hierboven geeft een overzicht van uitbreidingen/toevoegingen van personele bezetting. Specifiek over de 7,2 FTE gaat het over de volgende FTE's (Academy betreft geen specifieke IB&P rol):

- 2,0 FTE voor de rol van Risicomanager en het uitvoeren van het autorisatiebeheer.
- 2,0 FTE Centrale coördinatie ambassadeursnetwerk, IB&P coördinatie en opvolging opschoning Sonar
- 3,2 FTE Domeinconsultants met betrekking tot werkzaamheden rondom de BIO.

Tabel versiebeheer

Versie	Datum	Voorgelegd aan	Beslissing
0.80	9-12-2022	PB WB	Feedback verwerkt
0.81	12-12-2022	Projectcontroller	Feedback verwerkt
0.82	13-12-2022	PB WB, PB C, project-controller, Stuurgroep	Feedback verwerkt
0.9	20-12-2022	PB WB, PB C	Feedback verwerkt
0.91	12-01-2023	Stuurgroep	

Bijlagen

De bijlagen hieronder benoemd bevatten aanvullend materiaal t.b.v. dit dossier. De documenten zijn nuttig om een meer omvattend begrip van het project en de projectresultaten te krijgen, naast de bovenstaande beschreven hoofdlijnen.

1. Bijlage A: Projectresultaten in detail
2. Bijlage B: Overdrachtspunten
3. Bijlage C: Restrisico's
4. Bijlage D: Leerpunten
5. Bijlage E: Kansen en risico's

Bijlage A: Projectresultaten in detail

De onderstaande tabel geeft een samenvatting en overzicht van alle 77 bevindingen. Deze zijn allemaal volledig opgelost; het risico is volledig gemitigeerd, of er is een (beperkt) restrisico vastgesteld, wat vervolgens formeel is geaccepteerd. Daarnaast zijn er voor enkele bevindingen nog overige restpunten vastgesteld, die niet direct bijdragen aan het projectresultaat (de bevinding is al opgelost) maar in plaats daarvan bijdragen aan de duurzaamheid van de oplossing in de toekomst.

Zie Bijlage C: Restrisico's voor een gedetailleerd overzicht van de restrisico's (RR) en Bijlage B: Overdrachtspunten en overige restpunten voor een overzicht van de overige restpunten (RP).

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
Priv1.1 (Hoog) Onvoldoende privacyrollen en -verantwoordelijkheden in de eerste lijn belegd om privacyrisico's effectief te kunnen beheersen	Deze bevinding is opgelost omdat allerlei privacy-gerelateerde awareness activiteiten zijn uitgevoerd en periodiek worden herhaald. Tevens is een ambassadeursnetwerk opgezet waarbij de IB&P-ambassadeur per regiokantoor als centraal privacy contactpunt fungeren. Het BSO-team is versterkt met IB&P-coördinatoren om het WERKbedrijf te ondersteunen bij privacy- en informatiebeveiligingsvraagstukken.	— RR12 (klein): De afdeling VRIM maakt nog gebruik van exports voor bestelkantoren (tijdelijk restrisico: t/m release RW1 2023, gepland in juni 2023).
Priv1.2 (Hoog) Er wordt geen of onvoldoende eigenaarschap van privacyrisico's in Sonar genomen	Deze bevinding is opgelost omdat door de integrale IB&P audit op Sonar door KPMG de privacy risico's in kaart zijn gebracht en – door middel van acties en bevindingen – maatregelen zijn gekoppeld aan deze risico's om de risico's op te lossen. De term oplossen kan volgens het project ook een risico-acceptatie inhouden.	Niet van toepassing
Priv2.1 (Hoog) Het register is te grofmazig om te kunnen bepalen of	Deze bevinding is opgelost omdat het verwerkingsregister van WERKbedrijf is geüpdatet en gedetailleerder is, ditmaal ingevuld conform de eisen van de AVG. Tevens is t.a.v. een duurzame belegging een PDCA-cyclus ingericht om het	Niet van toepassing

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
persoonsgegevens onrechtmatig worden verwerkt	verwerkingsregister periodiek te updaten. De nieuwe versie en bijbehorende procedure wordt vervolgens intern gepubliceerd.	
Priv2.2 (Midden) Dataclassificatie is niet vastgesteld op adequaat niveau	Deze bevinding is opgelost omdat de dataclassificatielijst is aangevuld en geactualiseerd met de RAL (Risico Applicatielijst) en de FUGEM (Functioneel Gegevensmodel). Hierna zijn de maatregelen geijkt op het geclassificeerde dataclassificatieniveau van Sonar (BIV 2+). Tenslotte zijn door het afdwingen van niveau 2+ alle schermen op Sonar geclassificeerd en in lijn gebracht met deze nieuwe dataclassificatie.	— RR12 (klein): De afdeling VRIM maakt nog gebruik van exports voor bestelkantoren (tijdelijk restrisico: t/m release RW1 2023, gepland in juni 2023). — RR13 (klein): Er zijn gemeentegebruikers die via BI dashboards privacygevoelige gegevens kunnen downloaden.
Priv3.1 (Hoog) WERKbedrijf (WB) is niet in controle over privacyrisico's in Sonar	De bevinding is opgelost, omdat privacy risico's in Sonar zijn opgepakt in het Sonar IB&P project, waardoor WB in controle is over deze risico's. Tevens is er een privacy visie over toegang tot Sonar en een UWB breed privacy beleidskader opgesteld. Ook is het jaarplan van de BSO is vastgesteld door het DT. Tenslotte privacy een vast onderdeel van de DT-agenda gemaakt.	Niet van toepassing
Priv3.2 (Hoog) WERKbedrijf heeft geen gap-analyse ten opzichte van het privacy beleidskade**r** uitgevoerd	Deze bevinding is opgelost omdat het WERKbedrijf een gap-analyse heeft uitgevoerd m.b.t. Sonar in de vorm van het KPMG-onderzoek. Dit onderzoek is breder dan alleen privacy, dus het opzetten een integrale PDCA-cyclus is tevens een structurele oplossing waardoor ook andere applicaties kunnen worden meegenomen en geborgd.	— RR19 (klein): Er zijn (privacy)risico's voor betrokkenen, omdat de GEB's die relevant zijn voor Sonar niet volledig in beeld zijn gebracht.
Priv3.3 (Hoog) Reeds gerapporteerde privacyrisico's in Sonar worden niet, niet tijdig of niet effectief gemitigeerd	Deze bevinding is opgelost omdat als onderdeel van het Sonar project een robuust systeem is opgezet voor het opvolgen van gerapporteerde risico's m.b.v. een restriscoregister. Ook zijn deze risico's in de ISMS-tool (Information Security Management System) ingevoerd. Op deze manier worden reeds gerapporteerde privacy risico's in Sonar tijdig gemitigeerd in de verschillende stages.	Niet van toepassing
Priv4.1 (Hoog) De transparante arbeidsmarkt van de Wet SUWI is geen grondslag op basis waarvan toegang en inzage niet of nauwelijks	Deze bevinding is opgelost omdat in het verbeterinitiatief autorisatiemanagement in detail is uitwerkt dat Sonar-autorisaties (opnieuw) ingericht moeten worden, waarbij de toegang tot persoonsgegevens wordt geminimaliseerd, huidige processen en procedures worden herzien vanuit IB&P perspectief, en doelbinding van huidige autorisaties in de autorisatiematrix zijn vastgelegd.	— RR2 (klein): Sonargebruikers kunnen in specifieke onderdelen van Sonar doordrillen naar alle (landelijke) Sonarklanten in de Sonardatabase.

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
beperkt hoeven te worden in Sonar (zie ook onder 5)		— RR4 (klein): Regionaal autoriseren gebruikersgroepen gemeenten niet meer in Sonar aanpassen. — RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er (tijdelijk restrisico: na afronding onderzoek door FB).
Priv4.2 (Hoog) Medische gegevens worden in Sonar verwerkt zonder wettelijke grondslag	Deze bevinding is opgelost omdat werkinstructies zijn opgesteld voor medewerkers over het gebruik van bijzondere persoonsgegevens en – als onderdeel van die actie – controlewerkzaamheden zijn ingericht naar medische gegevens in de vrije tekstvelden van Sonar om te voorkomen dat dergelijke gegevens daar worden opgeslagen. Ook zijn verbeteracties uiteengezet m.b.t. de MOK controles. Deze worden in de PDCA-cyclus van BC&K tweejaarlijks uitgevoerd (steekproeven binnen elk rayon van 25 dossiers per rayon). Tenslotte zijn in de IB&P awareness-campagnes uitgebreid aandacht besteed aan vrijetekstvelden en medische gegevens.	Niet van toepassing
Priv4.3 (Midden) Toestemming wordt onnodig als grondslag gebruikt voor sommige verwerkingen in Sonar	Deze bevinding is met de onderliggende acties opgelost omdat er geen gebruik wordt gemaakt van de AVG-grondslag 'toestemming' aangezien de verwerking op basis de 'wettelijke taak van algemeen belang' geschied. Om medewerkers duidelijk te maken dat er geen gebruik gemaakt mag/hoeft te worden van de AVG-grondslag toestemming, zijn en worden er awareness activiteiten georganiseerd.	Niet van toepassing
Priv5.1 (Hoog) Nagenoeg alle gebruikers van Sonar hebben dezelfde leesrechten: Landelijk/regionaal	Deze bevinding is opgelost omdat via autorisatiebeheer de toegangsprofielen zijn geëvalueerd en herijkt op basis van het 'need-to-know' principe voor de betreffende functie en/of rol. Tevens is landelijke toegang voor diverse gebruikersgroepen ingeperkt, waaronder met name gemeentegebruikers. De toegangsrechten op Sonar zijn dusdanig voor gebruikers ingeperkt.	— RR4 (klein): Regionaal autoriseren gebruikersgroepen gemeenten niet meer in Sonar aanpassen. — RR13 (klein): Er zijn gemeentegebruikers die via BI dashboards privacygevoelige gegevens kunnen downloaden.

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
		— RR12 (klein): De afdeling VRIM maakt nog gebruik van exports voor de bestelkantoren (tijdelijk restrisico: t/m release RW1 2023, gepland in juni 2023). — RR2 (klein): Sonargebruikers kunnen in specifieke onderdelen van Sonar doordrillen naar alle (landelijke) Sonarklanten in de Sonardatabase.
Priv5.2 (Hoog) Nagenoeg alle gebruikers van Sonar hebben dezelfde leesrechten: Gemeentes, derde partijen en overige gebruikers	Deze bevinding is opgelost omdat via autorisatiebeheer toegangsprofielen zijn geëvalueerd en herijkt op basis van het need-to-know principe voor de betreffende functie/rol. Voor alle gemeentemedewerkers is ingeregeld dat ze alleen klanten binnen hun UWV-vestiging kunnen zien.	— RR2 (klein): Sonargebruikers kunnen in specifieke onderdelen van Sonar doordrillen naar alle (landelijke) Sonarklanten in de Sonardatabase. — RR4 (klein): Regionaal autoriseren gebruikersgroepen gemeenten niet meer in Sonar aanpassen. — RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er (tijdelijk restrisico: na afronding onderzoek door FB).
Priv5.3 (Hoog) Nagenoeg alle gebruikers van Sonar hebben dezelfde leesrechten: Gegevensvelden en gebruik ervan	Deze bevinding is opgelost, omdat via autorisatiebeheer de toegangsprofielen zijn geëvalueerd en herijkt op basis van het 'need-to-know' principe voor de betreffende functie/rol. Ook is de landelijke toegang voor diverse gebruikersgroepen ingeperkt.	— RR2 (klein): Sonargebruikers kunnen in specifieke onderdelen van Sonar doordrillen naar alle (landelijke) Sonarklanten in de Sonardatabase. — RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er (tijdelijk restrisico: na afronding onderzoek door FB).

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
Priv5.4 (Hoog) Nagenoeg alle gebruikers van Sonar hebben dezelfde leesrechten: Tabbladen	Deze bevinding is opgelost, omdat via autorisatiebeheer de toegangsprofielen zijn geëvalueerd en herijkt op basis van het 'need-to-know' principe voor de betreffende functie/rol. Ook is de landelijke toegang voor diverse gebruikersgroepen ingeperkt. Hierbij is ook het tabbladniveau meegenomen.	— RR2 (klein): Sonargebruikers kunnen in specifieke onderdelen van Sonar doordrillen naar alle (landelijke) Sonarklanten in de Sonardatabase. — RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er (tijdelijk restrisico: na afronding onderzoek door FB).
Priv5.5 (Hoog) Maatregel BI-dashboards naar aanleiding van datalek dekt maar een gedeelte van het risico af	Deze bevinding is opgelost omdat de exportmogelijkheid van Sonar technisch is gesloten. Hiermee kunnen medewerkers geen datasets vanuit de dashboards meer exporteren. In de uitgebreide BI-dashboard zijn BSN en NAW-gegevens nog wel zichtbaar, maar deze groep is significant beperkt en voor deze resterende groep is het risico geaccepteerd.	— RR9 (klein): BSN blijft tijdelijk nog gebruikt worden in MIP/GIP. — RR12 (klein): De afdeling VRIM maakt nog gebruik van exports voor de bestelkantoren (tijdelijk restrisico: t/m release RW1 2023, gepland in juni 2023). — RR13 (klein): Er zijn gemeentegebruikers die via BI dashboards privacygevoelige gegevens kunnen downloaden. — RR14 (klein): 24 gebruikers hebben rechten behouden om exportlijsten te genereren.
Priv5.6 (Hoog) Er zijn geen effectieve maatregelen om de risico's van vrije invoervelden te beperken	Deze bevinding is opgelost door met name de controlewerkzaamheden naar de vrije invoervelden door kwaliteitsmedewerkers. Deze controles zullen op den duur onderdeel uitmaken van hun werkproces en worden geborgd in de MOK controles. Dit is opgenomen in de verbetermatrix die jaarlijks door de directie van WERKbedrijf wordt vastgesteld.	— RR10 (klein): Plaatsen van gevoelige informatie in vrije tekstvelden. — RP2: De in het project gedefinieerde IB&P KPI's moeten SMART gemaakt worden. Tevens moeten deze voorzien worden van meetbare brongegevens en/of resultaatoverzichten. Deze data moeten, voor zover mogelijk, worden

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
		opgenomen in het reguliere dashboard van het MIP.
Priv5.7 (Hoog) Sonar-gegevens worden niet of nauwelijks meer geschoond	Deze bevinding is opgelost, omdat schoning inmiddels in begin Q1 2021 is uitgevoerd. Tevens zijn er schoningsscripts ontwikkeld om dit in de toekomst structureel uit te voeren door de lijnorganisatie (per Q1 2023).	— Vooraf voorzien risico #1 (hoog): Niet maskeren uitgeschreven klanten (tijdelijk restrisico tot aan realisatie schoningscripts).
Priv5.8 (Hoog) Lokale opslag van Sonar-data	Deze bevinding is opgelost omdat de exportmogelijkheid van Sonar voor de meeste gebruikers technisch is gesloten en er een beperkt BI-dashboard is ontwikkeld die minder persoonsgegevens toont. Tevens zijn er periodieke controles op de G-schijven ingevoerd om folders en bestanden met privacygevoelige informatie te signaleren en waar nodig te verwijderen. Ten slotte komen de risico's rondom exports aan bod in diverse IB&P awareness materialen en -trainingen.	— RR13 (klein): Er zijn gemeentegebruikers die via BI dashboards privacygevoelige gegevens kunnen downloaden. — RR12 (klein): De afdeling VRIM maakt nog gebruik van exports voor bestelkantoren (tijdelijk restrisico: t/m release RW1 2023, gepland in juni 2023).
Priv5.9 (Hoog) Geen (extra) maatregelen getroffen ten behoeve van BN'ers en kwetsbare personen	Deze bevinding is opgelost omdat er is besloten dat BN'ers geen uitzonderingssituatie ontvangen conform UWV-beleid. Bijzondere GevalsBehandeling (BGB) en VIP's (personen in de lijst van Binnenlandse Zaken) en Eigen Personeel (EP) hebben wel een bijzondere status. Hier is een use case voor functionele LOMO (logging en monitoring) voor ontwikkeld voor het monitoren van de activiteiten van eigen gebruikers.	— RR16 (klein): Er is geen real-time monitoring. — RR20 (klein): Geen (extra) maatregelen getroffen ten behoeve van BN'ers (Bekende Nederlanders) en kwetsbare personen.
Priv6.1 (Hoog) Privacy statement WERK.nl reflecteert niet accuraat de verwerkingen in Sonar	Bureau gegevensbescherming heeft een nieuw privacy statement opgesteld met input van alle divisies om de verwerkingen in Sonar accuraat vast te leggen. Het privacy statement van WERK.nl verwijst nu naar het privacy statement zoals op uwv.nl is vastgelegd. Tevens is dit duurzaam in de PDCA-cyclus belegd. Het proces m.b.t. het updaten van de privacy-verklaringen gaat in de toekomst gelijk op met het updaten van het Register van verwerkingen.	Niet van toepassing
Priv7.1 (Midden) De risico's met betrekking tot Sonar zijn niet	Deze bevinding is opgelost omdat vanuit een privacy gap-analyse op Sonar de privacy risico's in kaart zijn gebracht en hierop maatregelen worden en zijn geïmplementeerd (die anders uit de GEB op Sonar zouden blijken). Baserend op	— RR19 (klein): Er zijn (privacy)risico's voor betrokkenen, omdat de GEB's die relevant zijn voor Sonar niet volledig in beeld zijn gebracht.

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
vastgelegd/geïdentificeerd in een GEB	de acties en bevindingen van het project is een privacy audit-cyclus opgezet met een ingerichte PDCA-cyclus vanuit GRCcontrol.	
Priv7.2 (Laag) Er is geen overzicht en eenduidige procedure voor het afhandelen van verzoeken van rechten van betrokkenen	Deze bevinding is opgelost omdat een centrale ingang is gekomen voor het indienen van verzoeken waarbij BG (Bureau Gegevensbescherming) in de lead is. Het afhandelen van deze verzoeken vindt vervolgens decentraal plaats. Ook zijn op centraal niveau voor 'Inzage', 'Correctie', en 'Verwijderen' processen vastgesteld om te bepalen in hoeverre UWV kan voldoen aan een verzoek tot vergetelheid en over moet tot gaan tot het wissen van gegevens en wanneer een verzoek moet worden afgewezen.	Niet van toepassing
Priv8.1 (Hoog) Toegangsrechten zijn niet beperkt op basis van 'need-to-know'-principe	Deze bevinding is opgelost omdat een analyse is uitgevoerd ten behoeve van het opstellen van de autorisatiematrices (op scherm- en veldniveau, met een classificatie op schermniveau). Hieruit is een actuele en volledige autorisatiematrix opgesteld waardoor toegangsrechten kunnen worden beperkt op basis van het need-to-know principe. Ook is landelijke toegang voor diverse gebruikersgroepen ingeperkt.	— RR2 (klein): Sonargebruikers kunnen in specifieke onderdelen van Sonar doordrillen naar alle (landelijke) Sonarklanten in de Sonardatabase. — RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er klantgegevens op deze schermen te raadplegen of te muteren zijn.
Priv8.2 (Hoog) Sonar heeft geen tweefactorauthenticatie, ook niet voor externen	Deze bevinding is voldoende opgelost omdat uit diverse analyses is gebleken dat 2FA niet nodig is voor Sonar. De CISO benadrukt deze richting. Kort gezegd zijn de argumenten dat (a) Sonar een intern systeem is, dat enkel bereikbaar is via het interne netwerk (VPN, Citrix), (b) het wachtwoord dat wél nodig is om in te loggen is gereset en "sterk" gemaakt en (c) LOgging en MOnitoring (LOMO) op de Sonar PROD-omgeving is geïmplementeerd.	— RR4 (klein): Regionaal autoriseren gebruikersgroepen gemeenten niet meer in Sonar aanpassen. — RR6 (zeer klein): Ontbreken van multi-factor authenticatie leidt tot risico op delen van accounts. — RR7 (klein): Ontbreken van multi-factor authenticatie leidt tot risico op ongeautoriseerde toegang.

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
		— RR8 (klein): Geen koppeling Sonar accounts en AD-accounts, waardoor er geen SSO is.
Priv8.3 (Hoog) Logging & monitoring is beperkt ingericht	Deze bevinding is opgelost omdat functionele Logging en Monitoring (LOMO) op inzage voldoende is ingericht. Door de gerealiseerde technische koppeling tussen Qradar en RUEI is het mogelijk te monitoren welke medewerkers (UWV en Gemeente) welke burgers raadplegen in Sonar tabblad Personalia en welke medewerkers (UWV en gemeente) data uit Sonar exporteren).	— RR16 (klein): Er is geen real-time monitoring. — RR17 (klein): Er is geen logging en monitoring op backend applicaties, zoals databases. Ook niet bij DXC.
Priv8.4 (Midden) Niet voor alle categorieën betrokkenen is veilig berichtenverkeer binnen Sonar mogelijk	Deze bevinding is opgelost, omdat Zivver is ingevoerd en daarmee veilig berichtenverkeer mogelijk is gemaakt sinds december 2020.	RP2: De in het project gedefinieerde IB&P KPI's moeten SMART gemaakt worden. Tevens moeten deze voorzien worden van meetbare brongegevens en/of resultaatoverzichten. Deze data moeten, voor zover mogelijk, worden opgenomen in het reguliere dashboard van het MIP.
Priv9.1 (Midden) Er is onvoldoende ontwikkelcapaciteit bij de softwareontwikkelaar om te voldoen aan de eisen die UWV aan Sonar stelt met betrekking tot privacy	Deze bevinding is opgelost omdat deze bevinding via OrgMF#3, Priv5.1, en Priv8.3 al is opgelost. Deze individuele bevinding voegt daardoor weinig toe om te voldoen aan de eisen die UWV aan Sonar stelt met betrekking tot privacy.	— RR16 (klein): Er is geen real-time monitoring. — RR18 (middel): Er zijn heel weinig Siebel ontwikkelaars beschikbaar.
Priv10.1 (Hoog) Sommige medewerkers gebruiken 'workarounds' omdat ze het privacyrisico niet begrijpen	Deze bevinding is tweeledig opgelost. Ten eerste omdat er allerlei acties zijn uitgevoerd op het gebied van IB&P awareness die eraan bijdragen dat medewerkers meer inzicht krijgen in privacy risico's, zoals het gebruik van workarounds, en daardoor zorgvuldiger omgaan met persoonsgegevens. Ten tweede is de exportmogelijkheid grotendeels dichtgezet om het risico van de in de bevinding genoemde workaround te beperken.	— RR9 (klein): BSN blijft tijdelijk nog gebruikt worden in MIP/GIP. — RR12 (klein): 5 VRIM gebruikers hebben tijdelijk nog rechten om exportbestanden te maken. — RR13 (klein): Er zijn gemeentegebruikers die via BI dashboards privacygevoelige gegevens kunnen downloaden.

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
		— RR14 (klein): 24 gebruikers hebben rechten behouden om exportlijsten te genereren.
Priv10.2 (Midden) De effectiviteit van trainingen wordt niet getoetst	Deze bevinding is opgelost omdat de effectiviteit van trainingen wordt gemeten en gemonitord. De uitkomsten worden gerapporteerd a.d.h.v. een infographic met 10 awareness items die de effectiviteit van trainingen, awarenesscampagnes en toets momenten weergeeft.	Niet van toepassing
Priv11.1 (Hoog) Er is geen actieve monitoring om te controleren of voorgenomen privacy verhogende development changes daadwerkelijk doorgevoerd zijn	Deze bevinding is opgelost omdat via het Sonar IB&P project veel achterstallig onderhoud is weggewerkt (zoals de schoning van Sonar-data) en meer prioriteit is gegeven aan IB&P eisen en verandersignalen in het vraagsturing- en voortbrengingsproces, zoals door deelname van de IB&P coördinator aan de intaketafels. De rol van IB&P in de acceptatiefase is verstevigd. Er zijn ten aanzien van SSD voor de voorfase, ontwikkelfase en controlefase aangescherpte afspraken gemaakt met de releasemanager, product owner en TSC test coördinator (Test Service Center). Hierdoor zit het IB&P-team dichter op het SSD-proces.	— RP1: Na een jaar evalueren of privacymaatregelen hoog op de prioriteitenlijst blijven staan door het beleggen van de IB&P-rol in het acceptatieproces. — RR11 (klein): 23 Sonargebruikers hebben toegang tot de Sonar acceptatieomgeving en daarmee toegang tot (verouderde) productiedata.
Priv11.2 (Midden) Privacymaatregelen worden niet structureel getoetst op effectiviteit	Deze bevinding is opgelost, omdat door de implementatie van GRCcontrol (een ISMS-systeem) een intern beheersingssysteem voor IB&P risico's is ingeregeld. Voor deze bevinding is ervoor gekozen om de oplossing met name generiek te behandelen (privacymaatregelen die niet structureel getoetst worden) in plaats van in te gaan op het voorbeeld genoemd in de bevinding, omdat het voorbeeld een onderdeel is van het geheel aan privacymaatregelen). De tool bevat een integrale set aan beheersingsmaatregelen uit de BIO en de AVG.	Niet van toepassing
Priv12.1 (Hoog) Medewerkers hebben onvoldoende kennis over datalekken	Deze bevinding is opgelost omdat awarenesstrainingen, campagnes, en materiaal zijn uitgezet om de kennis m.b.t. privacy te vergroten. Zo is er bijvoorbeeld de verplichte training 'veilig omgaan met informatie'. De effectiviteit van deze activiteiten zijn getoetst door middel van een phishing test en een IPSOS 'houding en gedrag' onderzoek. Beiden tonen een positieve trend in bewustzijn van het belang van het beschermen van persoonsgegevens.	Niet van toepassing

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
Priv12.2 (Hoog) Datalekken worden onvoldoende geëvalueerd om in de toekomst te worden voorkomen	Deze bevinding is opgelost omdat de bestaande processen m.b.t. IB&P zijn verbeterd en de opgebouwde achterstand qua kennis en de implementatie van technische maatregelen zijn weggewerkt.	— RR12 (klein): 5 VRIM gebruikers hebben tijdelijk nog rechten om exportbestanden te maken. — RR13 (klein): Er zijn gemeentegebruikers die via BI dashboards privacygevoelige gegevens kunnen downloaden.
IAM1.1 (Hoog) Onvoldoende inzicht in privacygevoeligheid van Sonar-autorisaties	Deze bevinding is opgelost omdat soll-matrices zijn opgesteld binnen het initiatief autorisatiebeheer. Daarbij zijn analyses uitgevoerd op scherm- en veldniveau, waardoor voldoende inzicht is verkregen in de privacy-gevoeligheid van Sonar-autorisaties.	— RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er (tijdelijk restrisico: na afronding onderzoek door FB).
IAM1.2 (Midden) Diffuse verantwoordelijkheid voor toegangsbeheer Sonar	Deze bevinding is opgelost omdat de verantwoordelijkheid voor toegangsbeheerbeleid van Sonar centraal en eenduidig is belegd. De manager IV WERKbedrijf is systeemverantwoordelijke en de coördinator Realisatie & Beheer is eindverantwoordelijk voor de implementatie van autorisaties. Per divisie (AD, FEZ, ICT, SMZ, B&B, Handhaving, K&S, Uitkeren en WERKbedrijf) is er een proceseigenaar die verantwoordelijk is voor de autorisaties die vallen onder het bijbehorende proces.	— RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er (tijdelijk restrisico: na afronding onderzoek door FB).
IAM1.3 (Midden) Toegangsbeheerbeleid Sonar onvoldoende uitgewerkt in processen of bekend in de organisatie	Deze bevinding is opgelost omdat het bestaan van uitgewerkte processen voor toegangsbeheer binnen Sonar zijn geanalyseerd en aangevuld waar nodig. De vernieuwde en verbeterde processen en procedures zijn besproken met de betrokken stakeholders.	Niet van toepassing
IAM2.1 (Midden) Uitdiensttreders niet tijdig verwijderd uit Sonar	Deze bevinding is opgelost omdat het ABS aanvragen-proces is verbeterd. Deze verbetering is uniform voor alle gebruikers, inclusief ketenpartners. Alle provisioning wordt binnen 5 dagen verwerkt door de Servicedesk. Enig overblijvende capaciteitsissues zijn reeds opgelost. Tevens is de deactiveringsperiode van accounts van ketenpartners verkort van 6 maanden naar 3 maanden sinds de start van het KPMG-onderzoek.	Niet van toepassing

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
IAM2.2 (Laag) Functiewisselproces niet vastgelegd	De bevinding is opgelost omdat het functieveranderproces is teruggebracht van 1 maand naar 1 werkweek en er een kwaliteitsslag is gemaakt op ABS-aanvragen. Tevens is het beleid en processen onder de aandacht gebracht worden bij andere divisies (m.n. HRM), en het niet meer mogelijk is om een functieprofiel van een andere divisie te hebben zonder einddatum.	— RR5 (klein): Medewerkers binnen heel UWV kunnen langer overgeautoriseerd blijven dan strikt noodzakelijk, door beperkte controles op toegekende autorisaties door de eindverantwoordelijken.
IAM3.1 (Hoog) Sonar kent geen multi-factorauthenticatie	Deze bevinding is voldoende opgelost omdat uit diverse analyses is gebleken dat 2FA (tweefactorauthenticatie) niet nodig is voor Sonar. De CISO benadrukt deze richting. Kort gezegd zijn de argumenten dat (a) Sonar een intern systeem is, dat enkel bereikbaar is via het interne netwerk (VPN, Citrix), (b) het wachtwoord dat wél nodig is om in te loggen is gereset en "sterk" gemaakt en (c) logging en monitoring op de Sonar productie-omgeving is geïmplementeerd.	— RR6 (zeer klein): Ontbreken van multi-factor authenticatie leidt tot risico op delen van accounts. — RR7 (klein): Ontbreken van multi-factor authenticatie leidt tot risico op ongeautoriseerde toegang. — RR8 (klein): Geen koppeling Sonar accounts en AD-accounts, waardoor er geen SSO is.
IAM3.2 (Hoog) Wachtwoordbeleid sterk onvoldoende	Er heeft in zowel de WERKbedrijf Acceptatie Test Omgeving (WATO) als in de productieomgeving een wachtwoord reset plaatsgevonden middels een script voor alle gebruikers van Sonar (UWV en Gemeenten) conform de BIO normering. Dit is duurzaam belegd middels de aansluiting op Oracle Access Manager die het beleid afdwingt d.m.v. automatische procedures.	Niet van toepassing
IAM4.1 (Hoog) Onvoldoende ondersteuning aan rolbeheerders om functie uit te voeren	Deze bevinding is opgelost omdat er een analyse is uitgevoerd ten behoeve van het opstellen van de autorisatiematrices (op scherm- en veldniveau, met een classificatie op schermniveau). Hieruit is een actuele en volledige autorisatiematrix opgesteld vanuit het soll- en ist-principe. Hierdoor hebben rolbeheerders nu een actueel overzicht beschikbaar van schermen en bijbehorende datavelden die gekoppeld zijn aan Sonar.	— RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er (tijdelijk restrisico: na afronding onderzoek door FB).
IAM4.2 (Hoog) Validatieproces van goedgekeurde toegang onvoldoende	Deze bevinding is opgelost omdat de autorisatieprofielen zijn herijkt op basis van het 'need-to-know' principe. Ook worden via C1, C2, C5, C6, en C8 controles de toegekende rechten periodiek gecontroleerd waarmee de validatie op toegang thans wel voldoende is ingeregeld.	— RR1 (klein): HRM-profielen te generiek en niet frequent beoordeeld. — RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er klantgegevens op

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
		deze schermen te raadplegen of te muteren zijn. — RP2: De in het project gedefinieerde IB&P KPI's moeten SMART gemaakt worden. Tevens moeten deze voorzien worden van meetbare brongegevens en/of resultaatoverzichten. Deze data moeten, voor zover mogelijk, worden opgenomen in het reguliere dashboard van het MIP.
IAM4.3 (Hoog) Autorisatieconcept onvoldoende fijnmazig voor toegang tot privacygevoelige informatie	Deze bevinding is opgelost omdat middels het detailplan autorisatiebeheer alle Sonar autorisatieprofielen fijnmaziger kunnen worden ingericht en daarmee beter voldoen aan doelbinding en proportionaliteit. Voor alle gemeentemedewerkers is ingeregeld dat ze alleen klanten binnen hun UWV-vestiging kunnen zien.	— RR2 (klein): Sonargebruikers kunnen in specifieke onderdelen van Sonar doordrillen naar alle (landelijke) Sonarklanten in de Sonardatabase. — RR15 (klein): 70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er klantgegevens op deze schermen te raadplegen of te muteren zijn.
IAM4.4 (Hoog) Geen daadwerkelijke archivering uitgeschreven klanten	Deze bevinding is opgelost (lees: het restrisico is geaccepteerd), omdat weliswaar de toegang tot uitgeschreven klanten niet wordt beperkt tot een beperkte groep gebruikers, maar de Regiegroep dit risico (het niet-maskeren van uitgeschreven klanten) heeft geaccepteerd.	— Vooraf voorzien risico #1 (hoog): Niet maskeren uitgeschreven klanten (tijdelijk restrisico tot aan realisatie schoningscripts).
IAM4.5 (Midden) Exporteren van privacygevoelige informatie onvoldoende beschermd	Deze bevinding is opgelost omdat de exportmogelijkheid technisch is gesloten. Hierdoor is het voor medewerkers niet meer mogelijk om klantgegevens te exporteren en is het risico op het uitlekken van deze informatie (binnen of buiten de organisatie) gemitigeerd.	— RR12 (klein): De afdeling VRIM maakt nog gebruik van exports voor bestelkantoren (tijdelijk restrisico: t/m release RW1 2023, gepland in juni 2023). — RR9 (klein): BSN blijft tijdelijk nog gebruikt worden in MIP/GIP. (tijdelijk restrisico tot alternatieve

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
		gegevenslevering beschikbaar is vanuit Gegevensdiensten). — RR13 (klein): Er zijn gemeentegebruikers die via BI dashboards privacygevoelige gegevens kunnen downloaden. — RR14 (klein): 24 gebruikers hebben rechten behouden om exportlijsten te genereren.
IAM5.1 (Hoog) Forse discrepantie tussen goedgekeurde (SOLL) en toegekende (IST) autorisaties	Deze bevinding is opgelost, omdat er een kwaliteitsslag is gemaakt op autorisatiebeheer m.b.t. ABS aanvragen waarbij toegekende rechten die afwijken op de Deltalijst terecht komen en d.m.v. de herijkte maandelijkse C1 controle worden opgelost door de IB&P coördinator.	— RR3 (midden): Proces voor invoeren gebruikersautorisaties vanuit ABS naar Sonar is gevoelig voor menselijke fouten.
IAM5.2 (Midden) AutorisatieBeheerSysteem (ABS) foutgevoelig en niet rigide	Deze bevinding is opgelost omdat de C-controles zijn vernieuwd vanuit de processen m.b.t. autorisatie, authenticatie en monitoring en het restrisico van niet-automatisch provisionen is geaccepteerd. Vanuit het Helios programma zal in de toekomst automatische provisioning worden gestandaardiseerd, waarmee de problemen omtrent handmatige provisioning in ABS zijn opgelost.	— RR3 (midden): Proces voor invoeren gebruikersautorisaties vanuit ABS naar Sonar is gevoelig voor menselijke fouten.
IAM6.1 (Midden) Geen beleid voor gebruik van accounts met hoge rechten	Deze bevinding is opgelost omdat de functieprofielen op basis van doelbinding en proportionaliteit m.b.t. hun rechten zijn aangepast. Dit hoeft niet formeel vastgesteld te worden in beleid aangezien er nu enkel sprake is van doelbinding of niet; "hoog recht" is irrelevant. Dit is vastgesteld in de uitgebreide autorisatiematrix en het updaten en beleggen nieuwe (gemiste) controles in het ABS-controlemodel (C1 t/m C8). Hiermee is het risico dat hoge rechten accounts onterecht toegekend of foutief gebruikt worden gemitigeerd.	Niet van toepassing
IAM6.2 (Midden) Geen specifieke logging of monitoring op accounts met hoge rechten	Deze bevinding is opgelost (lees: door middel van een risico-acceptatie), omdat weliswaar Logging en Monitoring (LoMo) is ingeregeld op het toekennen van rechten, maar er geen specifieke LoMo is ingericht met use cases op hoge rechten. De reden hiervan is dat het UWV geen onderscheid maakt tussen reguliere en hoge rechten. Dit restrisico is reeds geaccepteerd.	— RR16 (klein): Er is geen real-time monitoring. — RR17 (klein): Er is geen technische logging en monitoring op backend

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
		applicaties, zoals databases. Ook niet bij DXC.
IAM7.1 (Hoog) Momenteel geen logging of monitoring op raadplegingen in Sonar	Deze bevinding is opgelost, omdat LoMo (Logging en Monitoring) op Sonar-raadplegingen is ingeregeld waardoor wordt opgemerkt als gebruikers informatie raadplegen waartoe ze geen doelbinding hebben.	— RR16 (klein): Er is geen real-time monitoring.
OrgL&G#1 (Midden) Gelimiteerde rapportage inzake informatiebeveiliging en privacy	Deze bevinding is opgelost omdat via de implementatie van het risicomanagementsysteem GRCcontrol er dashboards en rapportages worden opgesteld over de status van interne beheersingsmaatregelen. Tevens is er een awareness dashboard opgezet die de resultaten van verscheidene IB&P activiteiten weergeeft, en hiermee inzicht geeft in de effectiviteit van interne beheersingsmaatregelen.	Niet van toepassing
OrgL&G#2 (Midden) Gelimiteerd onafhankelijk toezicht op de IB&P-functie binnen het WERKbedrijf	Deze bevinding is opgelost omdat door de implementatie van GRCcontrol een intern beheersingssysteem is ingeregeld om (ook) integraal onafhankelijk toezicht te houden op de effectiviteit van interne IB&P beheersingsmaatregelen.	Niet van toepassing
OrgMF#1 (Midden) Gestructureerde aandacht voor informatiebeveiligingsbewustzijn is beperkt	Deze bevinding is opgelost, omdat er verplichte IB&P trainingen zijn en een online IB&P toets is die jaarlijks wordt uitgevoerd. IB&P onderwerpen waarop minder goed is gescoord in deze toets zullen extra aandacht krijgen in andere IB&P trainingen en awarenessacitiviteiten, zoals VOMI (Veilig omgaan met informatie) en BUVI (Bewust Uitwisselen van Informatie). Dat wordt opgenomen in de jaarlijks herijkte awarenesskalender.	
OrgMF#2 (Midden) Kritieke afhankelijkheden van individuen rondom het beheer en de ontwikkeling van Sonar worden niet periodiek geëvalueerd	Door het introduceren van procedures ter beheersing en evaluatie van kennis en capaciteitsrisico's voor Sonar, worden bijbehorende risico's voldoende gemitigeerd. Het ontwikkelen van een kennis- en capaciteitsmatrix op verschillende Sonar applicatie onderdelen geeft een basis waarop operationele en tactische personeelsplanning mogelijk wordt. Tevens heeft de matrix een duurzaam karakter aangezien gepersonifieerde en performancegerichte leer- en ontwikkelplannen gemaakt kunnen worden die zich richten op het borgen van de benodigde kennis. Tenslotte zijn beheerprocessen en procedures geactualiseerd.	Niet van toepassing

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
OrgMF#3 (Laag) De beschikbaarheid van juiste kennis en expertise rondom het beheer en de ontwikkeling van Sonar wordt niet periodiek geëvalueerd	Er zijn verschillende maatregelen geïntroduceerd waarmee elke mogelijke single point of failure wordt opgeheven en capaciteit voor het onderhouden en beheren van Sonar wordt gewaarborgd. De geüpdatete Sonar kennis en capaciteitsmatrix geeft een overzicht van de huidige bezetting (kwalitatief en kwantitatief). Gaps in de bezetting kunnen worden opgevangen door verschillende third-party contracten met Capgemini, Oracle, en IBM. Daarnaast zijn de beheerprocessen (zoals het evaluatieproces) aangescherpt op basis van de nieuw ontwikkelde kennis en capaciteitsmatrix. Zowel natuurlijk verloop als incidenteel verloop van kennishouders wordt geborgd door actueel inzicht (periodiek) in beschikbare capaciteit (fte's) en inzicht in kennisniveau middels kennis/capaciteits-matrix.	Niet van toepassing
OrgIRM#1 (Hoog) Geen gestructureerde toetsing van interne beheersingsmaatregelen op het gebied van informatiebeveiliging en privacy	Deze bevinding is opgelost omdat door de implementatie van GRCcontrol (een ISMS-systeem) een intern beheersingssysteem voor IB&P risico's is ingeregeld. De tool bevat immers een integrale set aan beheersingsmaatregelen uit o.a. de BIO en de AVG. Ook zijn de beheersingsmaatregelen uit SSD (Secure Software Development) toegevoegd aan GRCcontrol.	Niet van toepassing
OrgIRM#2 (Hoog) Ongestructureerd proces voor informatierisicomanagement (identificatie, registratie, opvolging en monitoring)	Deze bevinding is opgelost omdat het proces voor informatierisicomanagement wordt ondersteund door en geregistreerd in GRCcontrol (ISMS-tool). Het proces voor integrale dreigingen- en risicoanalyses is ingericht in GRCcontrol en er worden penetratietesten uitgevoerd in aanvulling op reguliere testen.	Niet van toepassing
OrgIRM#3 (Midden) Integriteits- en beschikbaarheidsaspecten onderbelicht ten opzichte van vertrouwelijkheid (en privacy)	Deze bevinding is opgelost omdat ten aanzien van de beschikbaarheid de RTO en RPO per applicatie is verzameld en vastgelegd in Confipedia en in GRC Control. Ook het inregelen van backup-/restoretesten en het inregelen van een uitwijktest bij de DXC-migratie dragen bij aan het borgen van de beschikbaarheid van Sonar.	— RR18 (middel): Er zijn heel weinig Siebel ontwikkelaars beschikbaar.
OrgIRM#4 (Midden) De BIV-classificatie voor vertrouwelijkheid (2) past niet bij de gegevens die binnen Sonar worden verwerkt	Deze bevinding is opgelost omdat de dataclassificatielijst (Risico Applicatielijst/RAL en het Functioneel Gegevensmodel/FUGEM) is aangevuld en geactualiseerd. Op basis van deze herijking van de RAL en FUGEM zijn (als onderdeel van de autorisatiematrix o.b.v. BIO) alle schermen van Sonar	Niet van toepassing

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
	geclassificeerd op niveau 2+, waarna vervolgens het maatregelniveau tot deze BIV-classificatie wordt afgedwongen.	
OrgBC#1 (Hoog) Er worden geen back-up-restoretesten uitgevoerd voor Sonar	Deze bevinding is opgelost omdat de back-up en restoretest gaat plaatsvinden tijdens de migratie naar DXC (Q4 2022). Het tussentijdig niet inregelen van een uitwijktest binnen IBM is geaccepteerd als restrisico (zie RAF 02.06.11a / 02.06.12).	Niet van toepassing
OrgBC#2 (Midden) Er worden geen uitwijktesten uitgevoerd voor Sonar	Deze bevinding is opgelost omdat er als onderdeel van de DXC-migratie een uitwijktest is uitgevoerd, er procedures en draaiboeken zijn opgezet, en uitwijktesten periodiek zullen worden uitgevoerd. De `failover/failback-testen zijn succesvol getest voor Sonar op 4/8 en 5/8/2022`. Er is met DXC afgestemd om jaarlijks 2 data-uitwijktesten en maximaal 5 steekproefsgewijze BUR testen te laten plaatsvinden.	Niet van toepassing
OrgO&T#1 (Hoog) Er vinden geen penetratietesten plaats op gehele Sonar-applicatie en onderliggende infrastructuur	Deze bevinding is opgelost omdat er een nieuw proces voor periodieke pentesten is ingericht. Ook is er budget voor dit nieuwe proces gereserveerd en worden bevindingen uit de pentesten opgevolgd.	Niet van toepassing
OrgO&T#2 (Hoog) Er is geen adequaat kwetsbaarhedenscanning- en -managementproces	Deze bevinding is opgelost omdat er een proces voor periodieke vulnerability scanning is ingericht en waar nodig wordt aangesloten op bestaande processen. Hiervoor is extra capaciteit bij het USOC gereserveerd om de scans uit te voeren. Doordat de bevindingen uit de scans worden gedeeld met de juiste teams wordt hieraan daadwerkelijk opvolging gegeven. Er is een eenmalige vulnerability scan uitgevoerd en de uitkomsten van deze scan zijn opgevolgd	Niet van toepassing
OrgO&T#3 (Hoog) Er vindt beperkte technische logging of monitoring plaats rondom Sonar	Deze bevinding is opgelost omdat er door een technische koppeling tussen Sonar en QRadar functionele logging op mutaties op tabbladniveau gelogd worden. Tevens wordt er door de koppeling tussen QRadar en RUEI-raadplegingen personalia en raadplegingen data export gemonitord. Het LoMo proces van het WERKbedrijf op de applicatie Sonar is hiermee naar een hoger AVG-volwassenheidsniveau getild.	— RR16 (klein): Er is geen real-time monitoring. — RR17 (klein): Er is geen logging en monitoring op backend applicaties, zoals databases. Ook niet bij DXC.
OrgW&R#1 (Hoog) De compliance aan intern beleid en wet- en	Deze bevinding is opgelost omdat door de implementatie van GRCcontrol (een ISMS-systeem) een intern beheersingssysteem voor IB&P risico's is ingeregeld.	Niet van toepassing

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
regelgeving wordt niet periodiek getoetst	De tool bevat een integrale set aan beheersingsmaatregelen uit de BIO en de AVG. Al het – voor het Sonar IB&P project relevante – beleid en wet- en regelgeving met betrekking tot Sonar is hiermee samengebracht in eenduidige beheersingsmaatregelen.	
OrgW&R#2 (Midden) Gelimiteerd onafhankelijk toezicht op de IB&P-functie binnen het WERKbedrijf	Deze bevinding is opgelost omdat door de implementatie van GRCcontrol een intern beheersingssysteem is ingeregeld om (ook) integraal onafhankelijk toezicht te houden op de effectiviteit van interne IB&P beheersingsmaatregelen. Vanuit de CIO (eindverantwoordelijk voor implementatie BIO) is geborgd dat de Accountantsdienst jaarlijks de BIO compliance controleert. Verder beoordeelt de CISO de testresultaten van uitgevoerde controles.	Niet van toepassing
TechB1.1 (Hoog) Gebruik van zwakke en raadbare wachtwoorden	Deze bevinding is opgelost omdat via scripts naar alle gebruikers van Sonar (zowel UWV- als Gemeenten-gebruikers) de opdracht is verstrekt om hun wachtwoord te wijzigen naar een sterk wachtwoord conform de BIO-beleidslijn (Baseline Informatiebeveiliging Overheid). Dit proces is duurzaam geborgd d.m.v. de aansluiting op de generieke OAM. Hiermee kun je technisch afdwingen dat een wachtwoord BIO-conform is, dat eens in de 3 maanden vernieuwd moet worden, en dat het account geblokkeerd wordt bij meer dan 5 foutieve inlogpogingen. Dit is van toepassing op alle Sonar gebruikers (ook voor Beheerders).	Niet van toepassing
TechB1.2 (Hoog) Gevoelige bestanden bereikbaar binnen gedeelde mappen	Deze bevinding is opgelost omdat het SMB-protocol in mei 2021 is uitgeschakeld waardoor de gedeelde mappen niet meer bereikbaar zijn behalve voor een geselecteerde groep beheerders. Tevens zijn alle overbodige mappen en bestanden tijdens het Groot Onderhoud-traject geschoond. De logbestanden voor monitoring zijn verplaatst naar een andere omgeving waardoor de leverancier geen toegang meer heeft tot de Sonar omgeving	Niet van toepassing
TechB1.3 (Hoog) Gebruik van niet-ondersteunde en kwetsbare software	Deze bevinding is opgelost omdat met het Groot Onderhoud Traject in juli 2020 een majeure Siebel upgrade is uitgevoerd waarbij alle componenten van Sonar en Siebel zijn geüpgraded. Dit maakt de periodieke (jaarlijkse) Siebel upgrades makkelijk doorvoerbaar in het Sonar domein. Tevens heeft WERKbedrijf de directe Sonar servers en aanverwante servers gehardened, met extra aandacht voor de WATO. WERKbedrijf heeft het software Lifecyclemanagement proces duurzaam belegd door minimaal 1x per jaar de Siebel te upgraden en pakt hiermee dit proces strikter op.	Niet van toepassing

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
TechB1.4 (Hoog) Authenticatie ontbreekt op werk.nl API	Deze bevinding is opgelost, omdat de authenticatie van de SOAP API is verbeterd via middleware. Per januari 2022 kunnen niet-geautoriseerde gebruikers de SOAP API van Werk.nl niet meer gebruiken (deze wordt niet-benaderbaar vanuit de UWV KA-omgeving) als gevolg van het nieuwe inrichtingsplan van Werk.nl/middleware bij DXC.	Niet van toepassing
TechB1.5 (Hoog) Productiedata in acceptatieomgeving	Deze bevinding is opgelost omdat wordt voldaan aan het UWV-beleid voor wat betreft logging en monitoringseisen bij het gebruik van productiedata in de acceptatie-omgeving. Dit betekent dat er geen extra maatregelen geïmplementeerd hoeven te worden. Bij de DXC-migratie is logging en monitoring (LOMO) op de acceptatie-omgeving geïmplementeerd. Het resterende risico – toegang blijft mogelijk voor een select aantal werknemers tot de Sonar WATO omgeving die oude gegevens bevat – is formeel geaccepteerd.	— RR11 (klein): 23 Sonargebruikers hebben toegang tot de Sonar acceptatieomgeving en daarmee toegang tot (verouderde) productiedata.
TechB1.6 (Hoog) Domain Controller-mappen bevatten plain-tekst wachtwoorden	Deze bevinding is opgelost omdat alle scripts en configuratiebestanden op de Domain Controllers zijn gecontroleerd op wachtwoorden. Bestanden die niet actueel of noodzakelijk zijn voor het correct werken van de omgeving zijn verwijderd. Door een juiste inrichting van Group Policies en training van beheerders wordt het gebruik van plain-tekst wachtwoorden in bestanden zoveel mogelijk voorkomen.	Niet van toepassing
TechB1.7 (Midden) Beperkte hardening Citrix-omgeving	Deze bevinding betreft "Beperkte hardening Citrix-omgeving". Deze bevinding is opgelost omdat onderzoek heeft uitgewezen dat de maatregelen die zijn getroffen, toereikend zijn om kwaadwillende gebruikers geen kans te geven om het systeem te hacken. Daarmee is het SUWI-portaal robuust. Het risico dat KPMG in de bevinding aanduidt is daarom niet aanwezig en er zijn geen aanvullende acties nodig.	Niet van toepassing
TechB1.8 (Midden) Gebruik van onbeveiligde beheerinterfaces en protocollen	Deze bevinding is opgelost omdat onbeveiligde interfaces zijn uitgeschakeld en vervangen door beveiligde beheerinterfaces, waardoor het risico op het hacken van onversleuteld netwerkverkeer gemitigeerd is.	— RP3 (klein): https-protocol op de Sonar PDF servers is pas afgerond na de nazorgperiode.
TechB1.9 (Hoog) Onveilige SMB-instellingen	Deze bevinding is opgelost omdat er bij IBM een wijziging is aangevraagd om op alle AIX-machines binnen de Sonar omgeving het SMB v1 protocol uit te zetten. Op de resterende machines waar SMB niet kan worden uitgeschakeld is deze geüpgraded naar versie 2 en is 'SMB signing' geactiveerd. Hiermee is dit risico	Niet van toepassing

Bevinding	Mitigerende acties	Restrisico's (RR) en overige restpunten (RP)
	gemitigeerd omdat de risicovolle actie niet meer wordt uitgevoerd, of is gemitigeerd door de SBM-instellingen te upgraden tot een veilig niveau.	
TechB2.1 (Hoog) Hardening Windows-systemen	Deze bevinding is opgelost omdat de Windows systemen eenmalig zijn gehardened. Als onderdeel van 'Groot Onderhoud' worden deze systemen vervolgens elke 3 jaar opnieuw gehardened. Tenslotte worden er periodiek vulnerability scans uitgevoerd om de status van de systemen te blijven monitoren.	Niet van toepassing
TechB2.2 (Hoog) Hardening AIX-systemen	Deze bevinding is opgelost omdat de AIX-systemen zijn gehardened. Als onderdeel van 'Groot Onderhoud' worden deze systemen vervolgens elke 3 jaar opnieuw gehardened. Tenslotte worden er periodiek vulnerability scans door het USOC uitgevoerd om de status van de systemen te monitoren.	Niet van toepassing

Bijlage B: Overdrachtspunten en overige restpunten

Overdrachtspunten zijn acties die nog moeten worden uitgevoerd buiten het project, die direct bijdragen aan het projectresultaat. Dit in tegenstelling tot overige restpunten (later in deze bijlage), welke niet direct bijdragen aan het projectresultaat (maar desalniettemin overgedragen acties zijn).

De onderstaande tabel geeft een overzicht van geaccepteerde overdrachtspunten (OP) aan de lijn. Dit is een herhaling van de tabel in paragraaf: 'Nog uit te voeren acties om resultaat alsnog te behalen'.

ID	Onderwerp	Actiehouder	Acceptatie
OP1	De uitzondering die is gecreëerd waarbij 5 VRIM-medewerkers kunnen blijven exporteren (zie RR12) moet worden ingetrokken nadat de alternatieve gegevenslevering is gerealiseerd; momenteel gepland in de RW1 2023 release (juni 2023).	VRIM lijnmanager(s) van betreffende 5 medewerkers	Deelproject Proces
OP2	Ondanks onderzoek door WERKbedrijf FB zijn 70 schermen waar de autorisatiematrix naar refereert niet in kaart gebracht, omdat de schermen niet kunnen worden gevonden. Van deze schermen is nog onduidelijk of ze worden gebruikt. Volgens logging en monitoring (LOMO) is dat niet het geval. De nadere analyse hiernaar is overgedragen aan de lijn (beheer Sonar) (02.01.01c). Het gerelateerde restrisico is in detail beschreven in RR15.	Functioneel Beheer Sonar (IT WB)	Deelproject Proces

Onderstaande tabel geeft een overzicht van overige restpunten (welke niet direct bijdragen aan het behalen van het projectresultaat, maar wel de kwaliteit en het duurzame effect van enkele verbeteracties bestendigen). De restpunten zijn geaccepteerd bij de Stuurgroep, omdat de restpunten onderdeel uitmaken van acties die zijn gedechargeerd.

ID	Onderwerp	Actiehouder
RP1	Na een jaar zal geëvalueerd worden of het beleggen van de IB&P-rol in het acceptatieproces inderdaad heeft geleid tot verbetering (PDCA). Dit wordt gedaan om zorg te dragen dat privacymaatregelen hoog op de prioriteitenlijst blijven staan. Daarom is het belangrijk dat IB&P betrokken blijft bij het acceptatieproces en de development changes van Sonar (02.06.04).	BSO
RP2	De in het project gedefinieerde IB&P KPI's (zoals schonen van G-schijven en controle van de vrije tekstvelden in Sonar) moeten SMART gemaakt worden. Tevens moeten deze voorzien worden van meetbare brongegevens en/of resultaatoverzichten. Deze data moeten, voor zover mogelijk, worden opgenomen in het reguliere dashboard van het MIP. Gezien het speciale karakter en de specifieke benodigde kennis, is voorgesteld de voortzetting buiten het project Sonar IB&P te organiseren en op basis van een PDCA cyclus methodiek wordt doorgepakt (01.02.02).	WERKbedrijf IB&P
RP3	Het HTTP protocol op de PDF-servers wordt vervangen door het HTTPS protocol. De technische aanpassing naar HTTPS gaat mee met de RW4 2022 release (17 december) en is afgerond na een succesvolle afronding van de nazorgfase (medio januari 2023).	WERKbedrijf IB&P

Bijlage C: Restrisico's

De onderstaande tabel geeft een overzicht van de in kaart gebrachte en formeel geaccepteerde restrisico's. Merk op dat op deze restrisico's inhoudelijk is geadviseerd door de Quality Assurance Commissie en dat zij later formeel zijn geaccepteerd door de Stuurgroep (en in sommige gevallen ook het DT/de Regiegroep).

De risicoclassificaties zijn gegeven a.d.h.v. het UWV risicoclassificatiemodel. Na het oplossen van bevindingen worden eventuele restrisico's geclassificeerd en geaccepteerd. Dit volgt na het nemen van mitigerende maatregelen die het risiconiveau van de bevinding al (sterk) reduceren. Bij de behandeling van restrisico's wordt de kans en impact berekend met een 5x5-schaal van het UWV. Dit leidt tot een risicoscore van kans maal impact, welke conform de matrix hiernaast wordt omgezet naar een classificatie (zeer klein, klein, gemiddeld, hoog).

Legenda Risico matrix						
	Kans	1	2	3	4	5
Impact		zeer klein	klein	redelijk	groot	zeer groot
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

	Risicoclassificatie	Risicoacceptatie door
	Zeer klein	Directie bedrijfsonderdeel, gedelegeerd aan domeinhouder/verantwoordelijk management
	Klein	Directie bedrijfsonderdeel, gedelegeerd aan domeinhouder/verantwoordelijk management
	Gemiddeld	Directie bedrijfsonderdeel
	Hoog	Directie bedrijfsonderdeel **en mogelijk** Raad van Bestuur

Merk verder op dat het merendeel van de restrisico's gerelateerd is aan meerdere bevindingen. En ook dat zij onderling gerelateerd zijn. Ten behoeve van de effectieve opvolging (middels GRC-tooling) heeft het project gekozen om restrisico's met meerdere aspecten/consequenties zoveel mogelijk op te splitsen in individuele restrisico's.

Vooraf voorziene risico's die niet volledig opgelost kunnen worden

Naast de restrisico's gekoppeld aan het oplossen van bevindingen, zijn er ook – reeds in het projectplan – vier restrisico's op voorhand gedefinieerd. Deze restrisico's zijn niet opgenomen in de projectscope. Volledigheidshalve worden zij onderaan deze bijlage benoemd.

De tabel hieronder geeft de restrisico's weer, welke resulteren vanuit het oplossen van gerelateerde bevindingen in dit project.

Deze tabel is opgesteld aan het einde van het project (**peildatum: medio december 2022**); de restrisico's zullen actief gemanaged worden en zijn derhalve aan verandering onderhevig.

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
RR1	HRM-profielen te generiek en niet frequent beoordeeld.	2	3	K	De HRM-profielen, op basis waarvan het autorisatiemodel wordt ingericht, zijn niet volledig bruikbaar om goede autorisatieprofielen op te baseren. Dit omdat de HRM-profielen soms te generiek zijn en ook niet structureel periodiek opnieuw worden beoordeeld. Ze kunnen daarmee in sommige gevallen niet toereikend zijn om de doelbinding exact en juist vast te stellen en vast te leggen in het autorisatieprofiel. De kans bestaat dat	Risico geaccepteerd in actie 02.06.20 (RAF)	IAM4.2

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
					gebruikers autorisaties beschikbaar hebben, welke zij niet strikt nodig hebben voor hun functie/rol. Logging en monitoring werkt mitigerend op dit restrisico. Dit restrisico betreft de blijvende kans dat gebruikers autorisaties beschikbaar hebben welke zij niet nodig hebben voor de werkzaamheden die zij uitvoeren aanwezig blijft, omdat de HRM-profielen niet periodiek worden herbeoordeeld. Echter, deze kans is beperkt door verscheidene mitigerende maatregelen. Zo vormt het functieprofiel slechts één van de onderdelen op basis waarvan autorisatie aanvragen worden beoordeeld. Tevens gaat rolbeheer en IB&P in gesprek met de aanvrager. Ten slotte wordt het herbeoordelen van toegekende autorisaties geborgd via de C4 controle (4. Controle rolinhoud functierollen) uit het controlemodel.		
RR2	Sonargebruikers kunnen in specifieke onderdelen van Sonar doordrillen naar alle (landelijke) Sonarklanten in de Sonardatabase.	2	4	K	Bij autoriseren van Sonargebruikers middels de gebruikersautorisaties (per vestiging) van ABS naar Sonar blijft de mogelijkheid bestaan dat Sonargebruikers in specifieke onderdelen van Sonar kunnen doordrillen naar alle Sonarklanten in de Sonar database. Het doordrillen naar alle Sonarklanten in de database is een standaard Siebel feature (tooling) en werkt op de Siebel database (dus buiten de ABS vestigingskoppeling om). Dit was altijd al mogelijk sinds de introductie van Sonar. Hierdoor kunnen gegevens worden geraadpleegd van klanten die niet behoren tot iemands takenpakket. Een kwaadwillende medewerker kan deze gegevens gebruiken voor malafide doeleinden, zoals phishing of het chanteren van de betrokkene en/of het UWV. De kans dat dit gebeurd is klein, omdat de informatie alleen is op te vragen indien het BSN bekend is. ‘Wildcards’ en andere zoektechnieken werken niet. Mitigerende maatregelen zijn logging en monitoring op oneigenlijke raadplegingen in Sonar, de C1 t/m C8 controles van het autorisatiecontrolemodel (dit verminderd het risico dat gebruikers verkeerde autorisaties hebben), en IB&P awarenesstrainingen die bijdragen aan het beperken van het risico dat gebruikers klanten benaderen die zij niet nodig hebben voor hun dienstverlening.	Risico geaccepteerd actie 03.05.09 (RAF)	Priv5.1 ; Priv5.2;Priv 5.3;Priv 5.4 ; Priv8.1 ; IAM4.3;Priv 4.1;

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
RR3	Proces voor invoeren gebruikersautorisaties vanuit ABS naar Sonar is gevoelig voor menselijke fouten.	2	5	M	Het proces voor het invoeren van gebruikersautorisaties vanuit ABS naar Sonar is gevoelig voor menselijke fouten. Dit proces is niet gewijzigd gedurende het project; het risico bestond voorheen al. Dit restrisico wordt niet meer opgelost aangezien de uitfasering van Sonar het niet opportuun maakt om bijvoorbeeld automatische provisioning in te regelen. Het restrisico wordt wel deels gemitigeerd procesverbeteringen rondom ABS aanvragen. Daarnaast zijn de autorisatiecontroles (C1-C8-controles) aangescherpt en verbeterd en is LoMo ingericht, waardoor eventueel gemaakte fouten beter gedetecteerd en gecorrigeerd kunnen worden. Vanuit WorkIT kan worden overwogen om middels automatische federatie (en single sign-on) deze processen te automatiseren, wat de kans op menselijke fouten wegneemt. Tevens zal vanuit het Helios programma in de toekomst automatische provisioning worden gestandaardiseerd.	Risico geaccepteerd 03.05.04 (RAF) (tijdelijk restrisico tot het programma Helios is afgerond)	IAM5.1 ; IAM5.2
RR4	Regionaal autoriseren gebruikersgroepen gemeenten niet meer in Sonar aanpassen.	2	3	K	Dit restrisico betreft de mogelijkheid van gebruikersgroep 2 (Werkgeversdienstverlening) om landelijk te kunnen zoeken. Deze autorisatie is nodig, omdat deze gebruikersgroep landelijke toegang nodig hebben voor het vinden van personen met bepaalde competenties (om hen aan werk te helpen). Er zijn verschillende mitigerende maatregelen (reeds) genomen om het risico te beperken. Zo is het BSN uit de BI dashboard exportlijst gehaald, vinden er elke maand controles plaats naar inactieve accounts, en is er periodiek overleg met gemeenten om gezamenlijk de autorisaties te actualiseren. In het reeds afgeronde project ASG (Autorisatiesegmentering Gemeenten) zijn verschillende segmentaties toegevoegd in rollen en daaraan verbonden autorisaties voor gemeentelijke gebruikers.	Risico geaccepteerd (02.01.01f)	Priv4.1 ; Priv5.1 ; Priv5.2 ; Priv8.1
RR5	Medewerkers binnen heel UWV kunnen langer overgeautoriseerd blijven dan strikt noodzakelijk, door beperkte	2	4	K	Dit restrisico betreft de situatie dat Sonargebruikers overgeautoriseerd kunnen blijven doordat eindverantwoordelijken (met name bij andere divisies) de voor hen relevante autorisaties niet tijdig aanpassen wanneer medewerkers veranderen van functie. Overgeautoriseerde UWV-medewerkers kunnen daardoor gegevens van burgers raadplegen die zij niet nodig hebben voor hun werkzaamheden. De impact hiervan is groot, omdat veel persoonsgegevens in Sonar zijn opgenomen. De kans bij het WERKbedrijf is klein, omdat rolbeheerders een einddatum invoeren bij	Risico geaccepteerd actie 02.06.07b (RAF)	IAM2.2

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
	controles op toegekende autorisaties door de eindverantwoordelijken.				rollen en erop toezien dat eindverantwoordelijken periodiek worden geïnformeerd over het belang van goed autorisatiebeheer. Tevens zijn er halfjaarlijkse controles van autorisaties onder verantwoordelijkheid van IB&P Werkbedrijf. Dergelijke maatregelen zijn echter beperkt mogelijk bij andere divisies, omdat WERKbedrijf dit beleid slechts kan uitdragen bij andere divisies (wat gedaan is in het rolbeheeroverleg en het kernteamoverleg bij project Helios) en niet kan afdwingen. WERKbedrijf kan dit niet afdwingen, omdat zij daar geen mandaat voor heeft. Mitigerende maatregelen op dit vlak zijn dat (1) rolbeheerders van andere divisies hun leidinggevenden faciliteren door een einddatum in te voeren bij rollen, en (2) er is met de directeur van WB HRM afgestemd dat HRM zich gaat inzetten om awareness over sluitende autorisatiebeheer UWV breed te verhogen.		
RR6	Ontbreken van multi-factor authenticatie leidt tot risico op delen van accounts.	1	3	ZK	Sonar accounts zijn niet beveiligd met multi-factor authenticatie. Hierdoor is het relatief eenvoudig om inloggegevens te delen, wat de mate van zekerheid over de authenticiteit van gebruikers vermindert. Dit heeft meerdere effecten tot gevolg, waaronder het risico dat malafide, frauduleuze of foutieve acties (vanuit accounts) niet meer herleid kunnen worden naar natuurlijke personen. Conform de BIO wordt voor interne applicaties met het risicoprofiel van Sonar geen multi-factor authenticatie vereist. Het delen van inloggegevens is niet toegestaan. Awarenesstrainingen en logging & monitoring werken met name mitigerend tegen dit risico.	Risico geaccepteerd actie 03.04.05	Priv8.2 ; IAM3.1
RR7	Ontbreken van multi-factor authenticatie leidt tot risico op ongeautoriseerde toegang.	2	4	K	Sonar accounts zijn niet beveiligd met multi-factor authenticatie. Hierdoor neemt het risico op oneigenlijke toegang tot accounts toe wanneer wachtwoorden worden gecompromitteerd. Wel heeft de aanvaller ook toegang tot de UWV-omgeving nodig. Voor UWV en gemeente gebruikers is hier, van buitenaf, multi-factor authenticatie nodig op het UWV-account. Omdat er geen beheeraccount aan gemeentegebruikers wordt uitgegeven, is ongeautoriseerde toegang tot Sonar beheeraccounts vanuit het gemeentenetwerk geen aanvullend risico. Tevens loggen	Risico geaccepteerd actie 03.04.05	Priv8.2 ; IAM3.1

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
					gemeentemedewerkers alleen via een vertrouwd netwerk in op Sonar (Suwinet en SUWI-KA). Conform de BIO wordt voor interne applicaties met het risicoprofiel van Sonar geen multi-factor authenticatie vereist. Awarenesstrainingen, het verzwaarde wachtwoordbeleid (voor Sonar), het gebruik van een vertrouwd netwerk, en logging & monitoring werken met name mitigerend tegen dit risico.		
RR8	Geen koppeling Sonar accounts en AD-accounts, waardoor er geen SSO is.	3	2	K	Dit risico betreft de blijvende kans op menselijke fouten in het bijhouden van twee administraties m.b.t. leavers en movers (omdat Sonar accounts en AD accounts niet zijn gekoppeld). Dit risico geldt voor gemeentemedewerkers in het bijzonder, aangezien hun administraties zich buiten het zichtveld van UWV bevinden. Het risico hiervan is dat er meerdere wachtwoorden moeten worden bijgehouden, wat de kans vergroot van onzorgvuldige omgang met deze wachtwoorden	Risico geaccepteerd decharge bevinding IAM3.1	IAM3.1 ; Priv8.2
RR9	BSN blijft tijdelijk nog gebruikt worden in MIP/GIP.	2	3	K	Gedurende de tijd dat er een alternatieve oplossing wordt uitgewerkt (i.e. alternatieve gegevenslevering zonder BSN) blijft het BSN gebruikt worden in MIP/GIP. BSN-gegevens zijn in de basis niet nodig om beschikbaar te stellen in MIP/GIP. Als BSN's al eerder verwijderd zouden worden, dan zouden gemeentelijke processen verstoord worden. De alternatieve gegevenslevering worden momenteel ontwikkeld door Gegevensdiensten en wordt naar verwachting opgeleverd in 2023. Na release verwijdert LTS de BSN's vanuit MIP/GIP.	Risico geaccepteerd actie 03.06.02a (RAF) (tijdelijk restrisico tot alternatieve gegevenslevering beschikbaar is vanuit Gegevensdiensten)	Priv5.5 ; Priv10.1 ; IAM4.5
RR10	Plaatsen van gevoelige informatie in vrije tekstvelden	2	4	K	Het restrisico is dat gevoelige informatie, zoals gezondheidsgegevens of medische persoonsgegevens, in vrije tekstvelden kan worden geplaatst zonder dat dit direct wordt opgemerkt. Logging en monitoring kan niet op vrijetekstvelden ingeregeld worden. Het verminderen of maskeren van de vrije tekstvelden is eveneens (technisch) niet geschikt bevonden. Als gevoelige informatie in de vrije tekstvelden wordt opgeslagen dan kan dit vertrekkende gevolgen hebben voor de betrokkene. Zo kan een kwaadwillende hacker die bij de gegevens terecht kan komen deze gebruiken voor malafide doeleinden, zoals phishing of het chanteren van	Risico geaccepteerd decharge bevinding Priv5.6 (RAF)	Priv5.6

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
					de betrokkene en/of het UWV. De kans dat dit gebeurd is klein; uit een eerdere steekproef is gebleken dat in 0.4% van de gevallen gevoelige informatie is achtergelaten in de vrije tekstvelden. Mitigerende maatregelen op dit vlak zijn de steekproefsgewijze controles op de inhoud van de vrijetekstvelden, een instructiekaart voor medewerkers over bijzondere persoonsgegevens en wanneer bijzondere persoonsgegevens verwerkt mogen worden en de uitgebreide aandacht die wordt besteedt aan de vrije tekstvelden in IB&P awarenesstrainingen.		
RR11	23 Sonargebruikers hebben toegang tot de Sonar acceptatieomgeving en daarmee toegang tot (verouderde) productiedata.	2	4	K	Dit restrisico betreft 23 Sonargebruikers die toegang hebben tot de acceptatieomgeving en daardoor inzage hebben in de (verouderde) productiedata in de acceptatieomgeving. Het risico hiervan is dat zij (bewust of onbewust) onzorgvuldig omgaan met deze persoonsgegevens, of dat derden toegang weten te verkrijgen tot hun accounts en daarmee tot die productiedata. Om deze risico's te mitigeren zijn er maatregelen genomen: (1) het aantal gebruikers op de acceptatieomgeving is verminderd van 12.000 naar 23, (2) deze gebruikers hebben geen verhoogde rechten, (3) er is logging en monitoring is op de acceptatieomgeving op muteeracties, en (4) er zijn periodieke IB&P bewustzijnstrainingen die bijdragen aan het beperken van het risico dat gebruikers klanten benaderen die zij niet nodig hebben voor hun dienstverlening. Logging en monitoring op de acceptatieomgeving op raadplegen is niet nodig, omdat het IB&P risico al behoorlijk is verlaagd door bovenstaande acties en andere (standaard) beveiligingsmaatregelen ook van toepassing zijn op de acceptatieomgeving (complexe wachtwoorden, periodiek evalueren van accounts).	Risico geaccepteerd 03.08.02 (RAF)	Priv11.1 ; TechB1.5
RR12	5 VRIM gebruikers hebben tijdelijk nog rechten om exportbestanden te maken	2	4	K	5 VRIM gebruikers hebben tijdelijk nog rechten om exportbestanden te maken (voor overige VRIM-gebruikers zijn deze rechten al ingetrokken). Deze uitzonderingssituatie is nodig om de primaire processen van Bestelkantoren niet te verstoren. De exportbestanden worden enkel voor dit doel gebruikt en worden niet verder verspreid. Desalniettemin bestaat het risico dat gemaakte exports, met daarin gevoelige (klant-) gegevens, uitlekken. Bijvoorbeeld door onzorgvuldig gebruik van de medewerker. De	Risico geaccepteerd 02.04.06c/e (RAF)	Priv2.2 ; Priv5.1 ; Priv5.5 ; Priv5.8 ; Priv10.1 ; Priv12.2 ; IAM 4.5;Priv 1.1

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
					5 medewerkers zijn expliciet geïnstrueerd zorgvuldig om te gaan met de exportrechten en exportbestanden. Er is een alternatieve oplossing ontwikkeld, welke in de RW1 2023-release wordt uitgerold (momenteel gepland: juni 2023). Vanaf dat moment wordt de uitzondering ingetrokken, door de leidinggevende(n) van de 5 medewerkers vanuit VRIM.		
RR13	Er zijn gemeentegebruikers die via BI dashboards privacygevoelige gegevens kunnen downloaden	2	4	K	Er zijn gemeentelijke gebruikers die via de BI-dashboards persoonsgegevens van klanten kunnen inzien en downloaden. Op de peildatum betreft dit 36 van de oorspronkelijk 815 gemeentegebruikers (578 accounts zijn ontkoppeld en 201 accounts hebben alleen toegang tot het beperkte dashboard). Het risico bestaat dat gebruikers onzorgvuldig omgaan met de persoonsgegevens, zoals het onnodig uitprinten van gegevens of het per abuis sturen van het gedownloade bestand naar verkeerde ontvangers. Er zijn verschillende mitigerende maatregelen genomen om het risico te beperken. Bij het aanvraag-/wijzigingsformulier voor een BI-dashboard account wordt de benodigde doelbinding uitgevraagd en vervolgens getoetst door het Landelijke team samenwerking (LTS). Hiermee worden onnodige accounts zoveel mogelijk voorkomen. Tevens wordt periodiek gemonitord op het gebruik van de BI-dashboard autorisaties. Gebruikers verliezen hun autorisatie, indien ze langer dan 6 maanden geen gebruik hebben gemaakt van de BI-dashboards. Onzorgvuldige omgang met de persoonsgegevens op de uitgebreide dashboards kan ertoe leiden dat de persoonsgegevens worden ingezien door onbevoegden. Dit kan een potentieel datalek opleveren en leiden tot (zeer) nadelige gevolgen voor klanten wiens persoonsgegevens zijn gelekt en/of imagoschade voor en een eventuele boete van de toezichthouder voor het UWV.	Risico geaccepteerd actie 02.04.02d (RAF)	Priv2.2 ; Priv5.1 ; Priv5.5 ; Priv5.8 ; Priv10.1 ; Priv12.2 ; IAM4.5

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
RR14	24 gebruikers hebben rechten behouden om exportlijsten te genereren	2	4	K	24 gebruikers hebben rechten behouden om exportlijsten te generen. Voor alle andere gebruikers is de exportfunctie technisch afgesloten. Het restrisico betreft de kans op datalekken die via deze exportlijsten kunnen voortvloeien. De uitzondering is in stand gehouden om de mogelijkheid te behouden te voorzien in uitzonderlijke situaties, waar exportbestanden noodzakelijk zijn. De 24 gebruikers zijn zorgvuldig geselecteerd en hebben duidelijke instructies ontvangen. Een mitigerende maatregel is dat deze 24 gebruikers expliciete autorisaties moeten aanvragen om te exporteren. Tevens vindt logging en monitoring plaats op het gebruik van exports door de overgebleven 24 personen om eventueel oneigenlijk gebruik vast te stellen.	Risico geaccepteerd decharge actie 03.06.01	Priv5.5 ; Priv10.1 ; IAM4.5
RR15	70 schermen in Sonar zijn niet terug te vinden, waardoor er geen inzicht is of er klantgegevens op deze schermen te raadplegen of te muteren zijn.	2	4	K	Via (het toekennen van) verantwoordelijkheden krijgt een Sonargebruiker toegang tot bepaalde schermen in Sonar. Van de toegekende schermen aan de verantwoordelijkheden zijn 70 schermen niet terug te vinden, ondanks dat ze toegekend zijn aan verantwoordelijkheden. Dat wil zeggen dat voor deze 70 schermen onduidelijk is of de schermen überhaupt bestaan en, zo ja, of de schermen persoonsgegevens bevatten. Dit betekent dat voor de 70 schermen (eigenlijk: 39, zie hierna) onbekend is wat kwaadwillenden eventueel zouden kunnen doen als ze toegang weten te verkrijgen tot deze schermen, zoals het muteren van gegevens. Een analyse van de 70 schermen bleek dat 9 schermen niet toegekend kunnen worden via ABS aan gebruikers, 22 schermen alleen toegekend zijn aan landelijke beheerders (zij verwerken geen persoonsgegevens van klanten. Voor de resterende 39 schermen is onduidelijk of ze nog bestaan en waarom ze aanvankelijk aangemaakt zijn. Het is dus onbekend of er persoonsgegevens via deze schermen te raadplegen zijn, en zo ja, welke persoonsgegevens. De kans dat de informatie kan worden ingezien door onbevoegden is klein. Uit een eerste analyse bleek dat het voor functioneel beheer niet mogelijk is om de schermen te benaderen. De kans dat dat wel mogelijk is voor een eindgebruiker is daarmee klein. Ook uit de loggingsgegevens van de schermen bleek dat de missende schermen niet (recent) zijn geraadpleegd.	Risico geaccepteerd actie 02.01.01c (RAF) (mogelijk tijdelijk restrisico tot het onderzoek van de lijnorganisatie is voltooid)	IAM1.1 ; IAM 1.2;IAM4.1;IAM 4.2; IAM 4.3; Priv 5.2; Priv 4.1; Priv 5.3; Priv 5.4;Priv 8.1

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
					Er kan pas meer duidelijkheid over dit restrisico worden verschaft als het nader onderzoek over de missende schermen heeft plaatsgevonden. Dit issue is al deels onderzocht in het Sonar IB&P project en wordt nader onderzocht door de lijnorganisatie (functioneel beheer).		
RR16	Er is geen real-time monitoring.	2	3	K	Er is logging en monitoring ingeregeld. De opvolging van verdachte gebeurtenissen (monitoring) vindt echter niet direct plaats op basis van real-time signalen (maar dagelijks; eenmaal per werkdag). Hiermee loopt men het risico dat oneigenlijk gebruik niet op tijd wordt opgevolgd. Een hacker of kwaadwillende medewerker kan dan ook voor beperkte tijd ongestoord 'zijn of haar gang gaan', waardoor er risico's ontstaan voor Sonargebruikers en het UWV (zoals het inzien van gegevens waartoe een medewerker geen bevoegdheid heeft en het gebruiken ervan voor malafide doeleinden, zoals phishing). Voor het UWV kan dit leiden tot bijvoorbeeld imagoschade of een boete van de toezichthouder. De monitoring van mogelijk oneigenlijk gebruikt wordt altijd opgevolgd door het incident te valideren. Hiervoor vindt afstemming plaats met de manager van de betreffende medewerker middels hoor en wederhoor. Het opvolgen van hoor en wederhoor vindt alleen plaats gedurende reguliere werktijden, zodat automatische logging en monitoring niet altijd direct wordt opgevolgd. Wel worden alerts binnen een werkdag opgepakt. Indien oneigenlijk gebruik wordt vastgesteld, wordt het incident belegd bij Bureau Integriteit. De kans is klein dat oneigenlijke mutaties en raadplegingen niet worden ontdekt, omdat er geen real-time monitoring is. Er vindt namelijk al reguliere logging en monitoring plaats op basis van bestaande use cases en medewerkers zijn op de hoogte van de integriteitscontroles op het inzien en gebruik van gegevens. Tevens wordt uitgebreid aandacht besteedt aan het belang van zorgvuldig omgaan met persoonsgegevens tijdens awarenesstrainingen.	Risico geaccepteerd actie 02.06.08b (RAF)	Priv5.9 ; Priv8.3 ; Priv9.1 ; IAM6.2 ; IAM7.1 ; OrgO&T#3
RR17	Er is geen technische logging en monitoring op	2	4	K	Technische logging en monitoring is niet ingericht op backend applicaties, zoals databases. Hierdoor is men niet op de hoogte van raadplegingen en onbevoegde mutaties in databases door een hacker. Een hacker kan deze	Risico geaccepteerd actie 03.11.01a (RAF)	Priv8.3; IAM 6.2; OrgO&T#3

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
	backend applicaties, zoals databases. Ook niet bij DXC.				gegevens gebruiken voor bijvoorbeeld het afpersen van de organisatie, wat weer kan leiden tot imagoschade of een boete van de toezichthouder. Technische logging en monitoring wordt alleen generiek ingericht bij USOC. De ontbrekende logging en monitoring is dus breder dan enkel het Sonar domein; het ontbreekt op alle backend applicaties van het UWV. De kans dat misbruik wordt gemaakt van gegevens in backend applicaties is klein. De gegevens bevinden zich immers 'onder water', waardoor reguliere gebruikers hier geen (functionele) toegang tot hebben. De backend applicaties zijn ook beveiligd zodat niet zomaar toegang kan worden verkregen tot deze gegevens. Aangezien aanvullende technische logging en monitoring UWV-generiek dient te worden ingericht overstijgt dit restrisico de scope van het Sonar IB&P project. Het CISO Office gaat nadere richtlijnen uitbrengen over technische logging en monitoring.		
RR18	Er zijn heel weinig Siebel ontwikkelaars beschikbaar.	2	5	M	Dit risico betreft de schaarste aan Siebel ontwikkelaars, die nodig zijn voor ontwikkelwerkzaamheden aan Sonar. Dit risico is inherent aan het gebruik van legacy software. Het risico wordt deels gedekt door de gecontracteerde leveringsverplichting met Capgemini en Oracle, maar er blijft een restrisico over als deze bedrijven de leveringsverplichting niet na kunnen komen (door de beperkte beschikbare Siebel expertise op de arbeidsmarkt). Sonar wordt op termijn uitgefaseerd door deelsystemen vanuit het programma WorkIT, waarmee het wordt vervangen door modernere technologie waar geen of veel minder schaarste voor beheerders en ontwikkelaren voor bestaat. Het restrisico wordt daarmee op termijn opgeheven.	Restrisico geaccepteerd in DT (tijdelijk restrisico tot vervanging door deelsystemen vanuit WorkIT)	OrgMF3; Priv9.1
RR19	Er zijn (privacy)risico's voor betrokkenen, omdat de GEB's die relevant zijn voor Sonar niet volledig in beeld zijn gebracht.	2	4	K	Dit restrisico gaat over het inzichtelijk maken welke GEB's die relevant zijn voor Sonar nog niet zijn uitgevoerd. Er wordt oftewel een gap-analyse verricht naar de aanwezigheid van deze GEB's. De gap-analyse is momenteel onvolledig, omdat niet alle domein GEB's in kaart zijn gebracht. Dit betekent dat onderdelen van Sonar niet zijn beoordeeld op mogelijke privacyrisico's. De kans dat misbruik wordt gemaakt van persoonsgegevens in Sonar door kwaadwillende derden of medewerkers en de kans op onbedoelde datalekken en onrechtmatige verwerkingen, doordat niet alle GEB's in	Risico geaccepteerd actie 02.03.01 (RAF)	Priv7.1;Priv 3.2

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
					kaart zijn gebracht is klein, omdat veel GEB's wel zijn uitgevoerd. Daarnaast is per functie bekeken welke gegevens nodig zijn, waardoor de kans op misbruik van persoonsgegevens, onbedoelde datalekken en onrechtmatige verwerkingen verder wordt geminimaliseerd. Ten slotte zijn (de meest belangrijke) mitigerende maatregelen uitgevoerd in het kader van het project Sonar IB&P: er is schoning uitgevoerd en er zijn (aangepaste) schoningscripts, er is logging en monitoring ingesteld, er zijn tal van awareness activiteitein ondernomen, en de autorisaties zijn aangepast en (worden) geïmplementeerd. De impact van misbruik van persoonsgegevens, onbedoelde datalekken of onrechtmatige verwerkingen in Sonar doordat niet alle GEB's in kaart zijn gebracht is groot, omdat deze omstandigheden kunnen leiden tot (zeer) nadelige gevolgen voor betrokkenen wiens gegevens zijn gelekt en/of voor het UWV. De actie om GEB's uit te voeren binnen UWV is een actie die reeds in de lijn is belegd binnen het team van Werkbedrijf IB&P. De restrisico's voortkomend uit de GEB's worden nu nog separaat gemonitord op het oppakken van mitigerende maatregelen. Zodra de implementatie van het ISMS gereed is zullen ook de risico's zoals benoemd in alle GEB's opgenomen worden in het risicoregister van GRC-control.		
RR20	Geen (extra) maatregelen getroffen ten behoeve van BN'ers (Bekende Nederlanders) en kwetsbare personen.	2	4	K	Met betrekking tot kwetsbare personen (BGB, VIP's en EP) is onderzocht in hoeverre extra afscherming van deze categorie gewenst is. Het advies vanuit het project - dat is overgenomen door de stuurgroep – is om additionele LOMO (logging en monitoring) in te richten voor deze groep klanten. Hiervoor zal een technische uitwerking gerealiseerd gaan worden, en procedureel moet vastgesteld worden hoe de opvolging van mogelijk oneigenlijk gebruik plaatsvindt naar de leidinggevende en het Bureau Integriteit. De monitoring wordt belegd bij SMZ Bijzondere Zaken, die verantwoordelijk is voor de afhandeling en het toezicht op EP Klanten. Er is al wel enige logging en monitoring ingericht. Eén van de punten waarop wordt gemonitord, is hoe vaak (x per dag) een BSN wordt geraadpleegd door hoeveel medewerkers. Dit ondervangt de situatie dat	Risico geaccepteerd actie 02.05.03b (RAF)	Priv5.9

ID	Naam	K	I	R	Toelichting	Acceptatie	Gekoppelde bevindingen
					een BN'er in het nieuws komt, waarna UWV-medewerkers direct het BSN en bijbehorende dossiers raadplegen. Dit is niet op basis van een speciale indicatie, zoals VIP of EP, maar dit geldt voor alle BSN's. Er is geen aparte LOMO voor BN'ers, omdat het begrip BN'er niet (nationaal) is gedefinieerd en ingekaderd. De reden daarvan is dat er geen normen bestaan die aangeven wanneer iemand BN'er is, wanneer niet (meer) en wie dat bepaalt. Een burger kan binnen een kort tijdsbestek van 'zero naar hero' gaan en vice versa. Doordat er geen officiële lijst met BN'ers is is het ook niet mogelijk om hier rekening mee te houden in de dienstverlening van het UWV. Zo kan er geen signaal worden afgegeven als een BN'er een uitkeringsaanvraag indient.		

Vooraf voorziene risico's die niet volledig opgelost kunnen worden

Door de functionele en technische beperkingen van het verouderde systeem, kunnen niet alle in kaart gebrachte tekortkomingen op het gebied van IB&P worden verholpen in Sonar. Er zijn hierdoor reeds op voorhand risico's bekend die niet volledig opgelost kunnen worden. Dit kan pas gerealiseerd worden wanneer het systeem is uitgefaseerd (vervangen door WorkIT). In het kader van dit project zullen, voor zover mogelijk, mitigerende maatregelen worden geïmplementeerd en zullen de restrisico's worden beoordeeld na implementatie van alle gerelateerde verbeteracties (conform het risicoacceptatieproces zoals hierboven beschreven). De restrisico's zijn als volgt:

1. Beperking: **Gegevens van inactieve klanten kunnen in Sonar niet gemaskeerd of verborgen worden.** Het gaat hier om gegevens van inactieve klanten die nog niet verwijderd mogen worden in verband met de wettelijke bewaartermijn van 5 jaar. De implementatie van het meer fijnmazige autorisatiemodel lost dit probleem niet geheel op.
   Risico: Dit leidt tot risico op het gebied van dataminimalisatie, omdat de gegevens nog toegankelijk zijn voor (geautoriseerde) gebruikers van Sonar, terwijl deze gegevens niet noodzakelijk zijn voor de uitvoering van wettelijke taken.
   Mitigerende maatregelen: Via de verbeterde logging en monitoring is het mogelijk om onrechtmatig gebruik van Sonar te signaleren, te monitoren en indien nodig te sanctioneren.

2. Beperking: Door technische beperkingen aan logging en monitoring met Q-radar is het **niet mogelijk om afwijkend gedrag op individueel gebruikersniveau automatisch te herkennen.** Er worden alleen signalen afgegeven als vooraf gedefinieerde drempelwaarden worden overschreden. Daarmee blijft het noodzakelijk om hier handmatig toezicht op te houden. Daarnaast wordt alleen het tabblad 'personalia' gemonitord op raadplegingen, i.v.m. de netwerkbelasting. Verder wordt er alleen op tabbladniveau gelogd en gemonitord, niet op individueel gegevensniveau.
   Risico: Niet vooraf gedefinieerde ongewenste/verdachte gedragingen worden niet gedetecteerd. Dit geldt ook voor ongewenste/verdachte raadplegingen op specifieke (gevoelige) gegevens op het tabblad 'personalia', alsook op andere tabbladen. Dit kan leiden tot het niet detecteren van (doelbewuste) schending van confidentialiteit en integriteit van gegevens.
   Mitigerende maatregelen: De verbeterde logging en monitoring geeft wel geautomatiseerde signalen op vooraf gedefinieerde drempelwaarden op het tabblad 'personalia', waarmee diverse onbewuste en ook bewuste gedragingen zullen worden gedetecteerd. Verder zullen middels het verfijnen van de autorisaties de toegangsrechten worden beperkt.

3. Beperking: In het ontwerp van Sonar zitten inherente **beperkingen in hoeverre autorisatierechten van gebruikers fijnmazig kunnen worden uitgesplitst**. Bij het ontwerp van Sonar zijn keuzes gemaakt die gebaseerd waren op het effectief en efficiënt delen van gegevens ten behoeve van de arbeidsbemiddeling op landelijk niveau. Die keuzes zijn gebaseerd op transparantie en openheid. Dit betekent dat fijnmazige toegangsrechten in het huidige Sonar alleen kunnen worden toegekend op scherm-/tabbladniveau; het inrichten op het niveau van individuele gegevens is buitenproportioneel complex en kostbaar.
   Risico: Dit leidt tot risico op het gebied van dataminimalisatie, confidentialiteit en integriteit van gegevens, doordat specifieke gegevens niet afgeschermd kunnen worden voor specifieke functionarissen die toegang nodig hebben in het belang van hun dienstverlening.
   Mitigerende maatregelen: Via de aanscherping van het autorisatiebeheer zal onnodige toegang tot gevoelige schermen/tabbladen zo veel mogelijk worden ingeperkt. Daarnaast zal met logging en monitoring oneigenlijk gebruik (op scherm-/tabbladniveau) kunnen worden gedetecteerd.

Nota bene: in het oorspronkelijke projectplan werden vier risico's op voorhand voorzien, die niet volledig opgelost kunnen worden. Eén van deze risico's, namelijk de onmogelijkheid om de exportfunctionaliteit af te sluiten, is toch gerealiseerd gedurende het project.

Bijlage D: Leerpunten

Deelproject Mens

Projectnaam:	Sonar IB&P
Projectcode:	UN0929
Datum:	12-1-2023
Versie:	1.0

- Ervoor zorgen dat ingezette verbeteracties na afronding/dechargering op gedegen wijze van Project Sonar IB&P overgaan naar de reguliere organisatie en dat ze daarin geborgd worden en blijven. Met name dit laatste – blijven – is een leerpunt; we zien na 1 à 1½ jaar dat met moeite doorgevoerde activiteiten/verbeteringen/innovaties alweer door o.a. gebrek aan daadkracht en urgentiebesef bij (hoger) management 'ins blaue hinein' verdwijnen. Het is dus belangrijk om de opvolging van resultaten te borgen, monitoren, en continue verbetering te stimuleren zodat dezelfde fout niet nogmaals gemaakt wordt.
- Leerpunt is dat al de awareness acties niet eenmalig zijn. Awareness vergt continue aandacht, ook na het project. Leerpunt is dat er tijdig in de begrotingen geld wordt gereserveerd voor continue acties op het gebied van IB&P en acties welke zijn/worden opgenomen in nieuwe awareness kalenders.
- Een belangrijk leerpunt is om het hoofd communicatie goed en tijdig te informeren over de acties die op stapel stonden, waardoor tijdslijnen beter gecommuniceerd kunnen worden. Communicatie wordt vaak onderschat bij dergelijke projecten, maar een goede en tijdige communicatie is cruciaal voor het slagen van een project. Communicatie dient te allen tijde vroegtijdig te worden betrokken (bijvoorbeeld d.m.v. een communicatie collega als counterpart bij de afdeling communicatie hebben en houden). Een leerpunt is om dit blijvend goed te borgen, te monitoren en continu te verbeteren.
- Leerpunt is een projectteam of projectleider tijdig informeren over bestuurlijke wijzigingen.
- Leerpunt is dat er tijdig in de begrotingen geld wordt gereserveerd voor continue acties op het gebied van IB&P en acties welke zijn en/of worden opgenomen in de nieuwe awareness kalenders.
- Een leerpunt is het organiseren van een onderzoekstructuur om de bestaande kennis en materialen vanuit het UWV te gebruiken in lopende onderzoeken.
- Beheer van informatie dient goed te worden belegd en dient tevens elk jaar in het jaarplan te worden opgenomen. Hierbij hoort de betreffende informatie ten minste 1 keer te worden gecontroleerd en goedgekeurd.
- Als leerpunt kan worden aangegeven dat het maken van een kalender voor 2 à 3 jaar niet realistisch is. De kalender is een organisch en dynamisch document en kan jaarlijks inspelen op actuele ontwikkelingen. Een nieuwe kalender voor het komende kalenderjaar wordt aan het eind van elk jaar opgesteld. Hierover vindt jaarlijks aan het einde van het jaar door IV Office/IB&P communicatie plaats. Als aanbeveling kan worden meegenomen dat de directie jaarlijks aan het einde van het jaar de Awarenesskalender bespreekt met de security officer.
- Kortere lijnen met een QAC lid is essentieel. Dit kan door ze nauwer te betrekken bij het ontwikkelproces, zonder dat dit ook een objectieve beoordeling (een slager die zijn eigen vlees keurt), in de weg staat.
- Aanbevolen wordt om te toetsen in hoeverre gedetacheerde medewerkers op de hoogte zijn van de UWV IB&P richtlijnen en medewerkers te informeren en te wijzen op de awarenesscampagne bij UWV WERKbedrijf.
- Een leerpunt is om het IPSOS-gedragsonderzoek jaarlijks te herhalen en te kijken waar verbeteringen kunnen worden doorgevoerd.
- Er zal nadrukkelijker moeten worden toegezien op de resultaten van de kennistoets en hieraan consequenties verbinden bij het niet verplicht volgen van trainingen. Leerpunt hierin is ook dat er goed op dient te worden toegezien dat medewerkers en management deze trainingen gevolgd hebben. Een aanbeveling is dat hierover in de managementrapportages of monitorgesprekken aandacht aan wordt besteed.
- Leerpunt is dat de gesprekken tussen de coördinator bedrijfsmiddelen en de rayonmanagers rondom het afhandelen van beveiligingsincidenten en impactvolle datalekken en het evaluatieproces bij een voorkomende calamiteit ook online hadden kunnen plaatsvinden. Dit is onder de aandacht gebracht bij de coördinator Bedrijfsmiddelen en wordt opgepakt.
- Samenwerking in een multidisciplinair team heeft meerwaarde en werkt steeds beter naarmate je elkaar beter kent. Starten i.p.v. afsluiten met een teamactiviteit of borrel kan nog meer bijdragen aan een vliegende start.
- Stilstaan bij hoe sneller opvolging aan resultaten gegeven kan worden. De game "Het slimste IB&P team" werd eigenlijk pas een jaar na het IPSOS-onderzoek ontwikkeld. Dit zorgde er ook voor dat de nameting al uitgevoerd was voordat alle verbeterrichtingen goed waren uitgevoerd

en geland (Het slimste IB&P team is een duidelijk voorbeeld, maar ook de ambassadeurs hadden nog geen volledige rolvolwassenheid etc.).
- Er is weinig gevoel/raakvlakken met de dagelijkse uitvoering van het onderwerp IB&P.

Deelproject Proces

- Het belangrijkste leerpunt is dat ervoor gezorgd moet worden dat elke afdeling een overzicht heeft van de functies binnen zijn team en de daarbij behorende autorisaties om de processen uit te kunnen voeren waarvoor de afdeling verantwoordelijk is. Voor Rolbeheer is het namelijk essentieel dat er een onafhankelijk document is dat dient als bron van waaruit benodigde autorisaties kunnen worden herleid. Het is dus noodzakelijk dat er per functie ook een Functierol beschikbaar moet zijn.
- Een ander belangrijk leerpunt is het strak regelen dat de ingezette verbeteracties na afronding/dechargering op gedegen wijze van Project Sonar IB&P overgaan naar de reguliere organisatie en dat ze daarin geborgd worden en blijven.
- Zorg dat elke afdeling een overzicht heeft van de functies binnen zijn team en de daarbij behorende autorisaties om de processen uit te kunnen voeren waarvoor de afdeling verantwoordelijk is. Dit afdelingsoverzicht van de rechten per functie geeft de manager/gedelegeerde de juiste informatie om hun taak uit te kunnen voeren namens de eindverantwoordelijke. Hiermee wordt tevens ingeregeld dat bij Instroom de rechten automatisch goed worden aangevraagd en nieuwe collega’s direct kunnen starten als het account wordt aangemaakt en de rollen zijn aangevraagd door de leidinggevende en/of gedelegeerde.
- Er waren veel overautorisaties als gevolg van gekozen invulling van Rolbeheer in ABS. De toekennen van taakrollen moet worden gedaan aan de functionele rol i.p.v. de applicatie rol. Met het omzetten van taakrollen naar applicatierollen en validatie op gebruik (laatste login) is het aantal gebruikers met rechten voor Sonar met 25% teruggebracht. Dit is zeker een optie die verder kan worden benut. Voor bepaalde functies is het mogelijk en het zal dus nader moeten worden onderzocht wat dit zou betekenen voor het aanvraagproces én het onderhouden van deze keuze.
- In ABS kan de manager niet kiezen uit alleen de benodigde autorisaties voor de medewerkers van het team op basis van een beperkte set rollen (Functieprofielen). Dit is meegenomen als uitgangspunt voor het nieuwe IAM. Die mogelijkheden zijn er wel en dat zal voor bepaalde functies een oplossing kunnen bieden. Hier zal met name bij de inrichting van het nieuwe ABS IIQ rekening mee moeten worden gehouden. Verzoeken om het op een genoemde manier in te regelen hebben Rolbeheer tot nu toe nooit bereikt. Managers weten Rolbeheer niet te vinden.
- Het uitgangspunt bij het definiëren van functierollen is een actueel functieprofiel. Aanvullend kan een extra functierol nodig zijn op basis van een specifieke taak of opdracht. Dit kan structureel zijn maar ook tijdelijk bijvoorbeeld voor projecten en pilots. De reden is dat een Functierol ergens op gebaseerd moet zijn. Voor Rolbeheer is het essentieel dat er een onafhankelijk document is die dient als bron van waaruit benodigde autorisaties kunnen worden herleid. In het nieuwe systeem ABS IIQ worden Functierollen (later Businessrol) bestemd voor een medewerker in een bepaalde HRM functie automatisch gekoppeld aan de medewerker op basis van kostenplaats en functiecode. Het is dus noodzakelijk dat er per functie ook een Functierol beschikbaar moet zijn. Voor het WERKbedrijf is dit naar schatting voor ongeveer 95% zo ingeregeld. Het inregelen van functierollen op basis van een rol i.p.v. een HRM functie maakt het aanvraagproces nodeloos ingewikkeld. Iedere aanvraag zal dan moeten worden gemotiveerd. Degenen van het aanvraagproces zijn hier (nog) niet aan toe. De genoemde functierollen onder dit leerpunt kunnen meer worden voorzien van applicatierollen dan taakrollen. Rolbeheer heeft voor zijn werkzaamheden al een eigen rol gedefinieerd.
- De signalen vanuit Rolbeheer op het niet uitvoeren van de taken door leidinggevende moeten worden opgevolgd. Op basis van deze signalen moeten de training en begeleiding van leidinggevende worden aangepast vanuit WB-HRM.
- Voor de inrichting van de nieuwe systemen meenemen dat archivering en toegang tot niet actieve klanten beperkt wordt via autorisaties, omdat Legacy systemen niet eenvoudig aan te passen zijn aan verbeterde IB&P richtlijnen.

- Een leerpunt is dat door definiëring van KPI's voor het management het belang van IB&P duidelijker wordt en het onderdeel van de sturing wordt.
- In ABS kan de manager niet kiezen uit alleen de benodigde autorisaties voor de medewerkers van het team op basis van een beperkte set rollen (Functieprofielen). Dit is meegenomen als uitgangspunt voor het nieuwe IAM. Die mogelijkheden zijn er wel en dat zal voor bepaalde functies een oplossing kunnen bieden. Hier zal met name bij de inrichting van het nieuwe ABS IIQ rekening mee moeten worden gehouden. Verzoeken om het op een genoemde manier in te regelen hebben Rolbeheer tot nu toe nooit bereikt. Managers weten Rolbeheer niet te vinden.
- Met het gebruik van de juiste logging en monitoring worden risico's verlaagd. Het is een goed alternatief voor grote investeringen en het verlagen van risico's op continuïteit van legacy systemen zoals Sonar.
- Beperkte of geen controle op toegekende rechten door managers met de KPI op de C2 en C4 controle moeten worden opgevolgd.
- Betrek eindverantwoordelijke van een applicatie bij het opstellen van de RAL-Lijst en vraag om sturing op deze lijst. Nu staan er veel kolommen op oranje en/of rood en zijn niet alle applicaties op deze lijst opgenomen. Als een aspect niet voldoet zorg dat systeemeigenaar een risico acceptatieformulier hiervoor invult. De BIO maatregelen kunnen hierin voorzien.
- BCM krijgt weinig tot geen aandacht. RPO (herstelpunt: maximaal toegestane dataverlies) en RTO (Hersteltijd: Maximaal toegestane onbeschikbaarheid) waren niet vastgesteld. Met invulling van BIO wordt dit nu opgehaald.
- De dreigingen - zoals gedefinieerd met de MAPGood methodiek - kunnen risicogebaseerd worden behandeld. Het behandelen van alle dreigingen is overbodig als het risico laag is. Een Quickscan van te hanteren dreigingen voor een bepaald systeem of proces verhoogd de effectiviteit van het bepalen van de benodigde implementatiemaatregelen.
- ISO 27001/27002 maatregelen zijn over het algemeen geïmplementeerd op een bepaald niveau. Het aantonen van de werking is een leertraject voor zowel IB&P als de verantwoordelijke die de maatregelen hebben geïmplementeerd.
- Bij het ontwikkelen uitgaan van 'Privacy by design' en dat gebruiken bij WorkIT en andere aanbestedingen. Het kader voor Privacy by Design is nog niet UWV breed gedefinieerd.
- Er moet logging en monitoring op veld-, raadpleeg-, of mutatieniveau worden ingeregeld.
- Een leerpunt is dat lijsten niet mogen geëxporteerd om de risico's op datalekken te verlagen.
- Overzichten met persoonsgegevens (incl. BSN, geboortedatum en NAW) zouden niet in een systeem moeten staan als dat niet nodig is. Zo kan mogelijk worden volstaan met alleen NAW-gegevens.

Deelproject Techniek

- Overbodige en oude infra structuur en programmatuur moet in de volgende release worden verwijderd.
- De impact op schoning en archivering moet bij wijzigingen in de WERKbedrijf dienstverlening (i.e. nieuwe wet(ten) en regels die invloed hebben op de UWV dienstverlening) worden meegenomen.
- Bij de opzet van nieuwe WB dienstverlening of nieuwe Sonar aanpassingen moet rekening worden gehouden met de diverse soorten klanten (actief, niet actief, VIP, EP, 16-, 65+ etc.). Hierop moet de autorisatie en doelbinding worden bepaald en ingericht.
- Monitoring moet jaarlijks worden getoetst en waar nodig nauwkeuriger worden ingericht. Bij voorkeur worden de meest actuele versies van monitoring tools ('state of the art') gebruikt op alle (OSI) lagen van de UWV bedrijfsapplicaties (BA's) in HRC (Hoofd Rekencentrum) (ook bij hosting partij). Op dit moment worden monitoring tools niet op alle (OSI) lagen ingezet.
- Ieder jaar zouden de nieuwste technologische ontwikkelingen m.b.t. autorisaties en hardening moeten worden meegenomen bij het IB&P team, inclusief trends over de grootste IB&P issues op deze vlakken voor de komende 2 à 3 jaar.
- Samen met KPN jaarlijks (3 maanden voor nieuwe jaar/contractperiode) moet de checklijst worden doorlopen met onderwerpen over robuustheid (hoe blijft UWV en KPN in control m.b.t. SUWI-portaal).
- Vulnerability bevindingen vanuit JIRA moeten naar een voortbrengingsproces van WERKbedrijf, of het TOH-proces worden gestuurd (al dan niet samen met ICT UWV).

- Sonar moet worden aangesloten op generieke componenten waarvan de IB&P (monitoring en rapportage) UWV-breed is geregeld.
- Bij wijzigingen in Sonar (of opvolgers) zou vigerende schoning werkbaar en rechtmatig moeten blijven.
- Standaard controles in IAT moeten worden opgenomen m.b.t. robuustheid van koppelvlakken tussen alle WERKbedrijf dienstverlening (DV) business analyse en UWV businessanalyses.
- Bij gegevenslevering vanuit WERKbedrijf dienstverlening business analyses moet vooraf de informatieanalyse worden gemaakt en geaccordeerd. Daarin moet worden aangegeven welke WERKbedrijf dienstverlening gegevens wel geleverd mogen worden. Tevens moet aangegeven worden op welke wijze deze zichtbaar zijn (GUI), wie die mogen zien, en of er kopieën mogen worden gemaakt (inclusief het proces).
- UWV moet jaarlijks blijven toetsen op de noodzaak van PROD-gegevens in de Accept omgeving. Indien noodzakelijk moet hierbij een RAF worden getekend (risicoaccepatieformulier).
- Om de borging van de KPMG bevindingen in te regelen kan een jaarlijkse 'self assessment' vanuit iedere Beheerorganisatie worden ingericht.

Bijlage E: Kansen en risico's

Nr.	Risico	K	I	P	Maatregel	Eigenaar
	Risico's met externe impact					
1.	Tot uiting komen van één van de vier "vooraf voorziene restrisico's" na acceptatie, waarna blijkt dat er meer gedaan had kunnen worden.	M	H	H	Grondige impactanalyse vooraf met QAC en Regiegroep.	Stuurgroep
2.	Niet halen tijdslijnen gecommuniceerd aan 2e kamer (m.n. eind 2022).	M	H	H	Twee wekelijkse voortgangsbewaking, maandelijkse voortgangsrapportages en kwartaalevaluaties. Toezicht op voortgang vanuit QAC en Regiegroep. *Nota bene: kans omhoog bijgesteld na niet halen tijdslijnen voor kortetermijnmaatregel rondom schoning.*	Stuurgroep
3.	Datalek op Sonar na ineffectieve projectuitvoering (vertraging of onvolledige afronding).	K	H	M	Invoering Quality Assurance Commissie en onafhankelijke audits op projectplan (Q1 2021) en na afronding op projectresultaten (Q1 2022).	Stuurgroep
4.	AP vindt dat er onvoldoende maatregelen worden genomen om onrechtmatigheid van verwerkingen op te heffen.	L	H	M	Validatie en documentatie van het risiconiveau door (externe) Quality Review (zie ook paragraaf 6.2).	Deelproject-verantwoordelijken.
5.	Externe (onterechte) verwachting dat project alle IB&P-risico's tot 0 zal reduceren. Terwijl streven is om risiconiveau naar acceptabel niveau terug te brengen.	M	M	M	Duidelijke en eenduidige communicatie over de projectdoelstelling, de risico accceptatieprocedure, en de definitie van een acceptabel risiconiveau.	Stuurgroep
6.	Niet invoeren van maatregelen vanwege negatieve impact op de (technische) werking zorgt voor non-compliance met AVG.	L	M	M	Afwijkingen gedegen documenteren en waar nodig gewijzigde aanpak (extern) laten toetsen door kennishouders.	Verantwoordelijke Deelproject Techniek
7.	Tot uiting komen van overige geaccepteerd restrisico, waarna blijkt dat er meer gedaan had kunnen worden.	K	M	K	Grondige impactanalyse en advies QAC en risicoaacceptatie op juiste niveau van de organisatie.	-Stuurgroep
	Risico's met interne/project- impact					

8.	Vertraging door onvoldoende draagvlak bij andere gremia, o.a.: CISO, SBK, JZ en FG.	H	H	H	Instellen Quality Assurance Commissie, waarmee afstemming wordt gezocht met CISO, SBK, JZ en FG, zowel op plannen, implementatie en decharge.	Coördinator QAC -BSO
9.	Beschikbaarheid van resources voor overleg, onderzoek en afstemming.	M	H	H	Op basis van prioritering beschikbaarheid resources borgen. Escaleren in hiërarchische lijn bij issues.	Deelproject-verantwoordelijken
10.	Voorgenomen verbeteracties zijn (in de praktijk) onrealistisch c.q. niet realiseerbaar.	M	H	H	Kwartaal sprints, inclusief evaluaties en bijsturing.	Deelproject-verantwoordelijken
11.	Vertraging door ineffectieve samenstelling en/of positionering van de QAC.	M	H	H	Nader afstemmen samenstelling en positionering QAC met leden en eventueel ook Regiegroep. Periodieke evaluatie van besluitvormingsproces en resulterende doorlooptijden.	Coördinator QAC -BSO
12.	Vertraging in besluitvorming door gevoeligheid dossier.	M	H	H	Tijdige en voldoende afstemming met belanghebbenden via projectgremia, in het bijzonder de Regiegroep en QAC.	Opdrachtgever
13.	Uitloop als gevolg van technische beperkingen en/of organisatorische weerstand rondom aanscherping autorisatiebeheer (mede op basis van ervaringen project ASG).	M	H	H	Dit project heeft meer prioriteit, welke ook is verankerd op directieniveau. Daarnaast risico-opslag van 3.000k getroffen voor eventuele uitloop, welke tussentijds geëvalueerd wordt. Op inhoud zijn lessons learned ASG meegenomen in planning verbeterinitiatief "Autorisatiebeheer".	Projectmanager Verantwoordelijke Deelproject Proces
14.	Uitloop als gevolg van beperkingen in het aantal Sonar releasemomenten, in verband met prioritering en beschikbaarheid van IT-capaciteit ten opzichte van DXC-migratie.	H	H	H	Dit project heeft veel prioriteit, welke ook is verankerd op directieniveau. Daarnaast risico-opslag van 3.000k getroffen voor eventuele uitloop, welke tussentijds geëvalueerd wordt. In kwartaalevaluaties wordt planning periodiek en gaandeweg herijkt.	Projectmanager Verantwoordelijke Deelproject Techniek
15.	ISMS tooling (“CompLions”) kan niet (tijdig) beschikbaar worden voor WERKbedrijf.	M	H	H	C-ICT te kennen geven waarom het essentieel is dat WERKbedrijf spoedig beschikking krijgt over de tooling.	Verantwoordelijke Deelproject Proces
16.	Beschikbaarheid van adequaat budget voor beoogde verbeteringen in de deelprojecten Mens, Proces en Techniek.	L	H	M	Op basis van prioritering budget borgen. Escaleren in hiërarchische lijn bij issues.	Deelproject-verantwoordelijken
17.	Onvoldoende aansluiting op initiatieven en gevolgen vanuit WorkIT en andere projecten.	M	M	M	Tijdens het identificeren, en uitvoeren, van de te nemen acties een afweging maken betreffende gelieerde projecten (o.a. WorkIT).	Deelproject-verantwoordelijken
18.	Onvoldoende (IB&P-) kennis en bewustzijn van externe gebruikers van Sonar, alsook de beperkte zicht en invloed op het gedrag van deze gebruikers.	M	M	M	Maatregelen opnemen in contracten met externen. Inzetten op opleiden van gebruikers. (Informele) Aandacht voor cultuur en gedrag in periodieke overleggen.	Contactpunt Gemeenten Communicatie-verantwoordelijke
19.	Afhankelijkheid van VNG; zelf onvoldoende invloed op het gedrag van eindgebruikers in de gemeentes.	M	M	M	Maatregelen opnemen in contracten met externen. Inzetten op opleiden van gebruikers. (Informele) Aandacht voor cultuur en gedrag in periodieke overleggen.	Contactpunt Gemeenten Communicatie-verantwoordelijke
20.	Gebruikers zijn onvoldoende over mitigerende maatregelen doordrongen.	H	L	M	Toetsing van effect training/instructies.	Verantwoordelijken Deelproject Mens

21.	Risico dat invoering van technische maatregelen een niet-acceptabele negatieve impact heeft op de (technische) werking van Sonar.	M	M	M	Voldoende aandacht/tijd besteden aan potentiële impact van wijzigingen op de performance van Sonar.	Verantwoordelijken Deelproject Techniek
22.	Vertraging door budget- en prioriteringsdiscussies ten opzichte van andere projecten en initiatieven.	M	M	M	Duidelijke signalering van conflicten vanuit Stuurgroep naar Directieteam WERKbedrijf; prioriteitstelling op het juiste niveau beslechten. Stuurgroep is link naar Domein WW.	Stuurgroep
23.	Inefficiënte of ineffectieve samenwerking tussen de verschillende Deelprojecten, door ontoereikende coördinatie en afstemming.	M	M	M	(Operationele) Projectgroep-overleg voor deelproject-overstijgend overleg en afstemming.	Projectmanager
24.	Onderschatting van inspanning/doorlooptijd door deelprojecten.	H	H	H	Risico-opslag van 3.000k in 2022, voor eventuele uitloop (in de "afsluit- en uitloopfase")	Stuurgroep

Legenda: K = Kans I = Impact G(root), M(iddel) of K(lein) - P = Prioriteit: H(oog), M(iddel) of L(aag)

PortfolioBureau heeft het projectplan getoetst op onderstaande criteria.

Onderwerp	Oordeel
Beleid	
1. Getoetst of Project een 'Groot ICT Project' betreft	Groen
2. Conform UWV InformatiePlan (UIP), Projectportfolio en U-toets	Groen
3. Compliancy met beleid UWV	Groen
Doelstelling	
4. Doelstelling van het project SMART geformuleerd	Groen
5. Nut en noodzaak voldoende aangetoond	Groen
6. Projectresultaten duidelijk	Groen
7. Businesscase voldoende onderbouwd en aannemelijk	Groen
Aanpak	
8. Gekozen ontwikkelaanpak voor het project	Groen
9. Oplossingsrichting voldoende onderbouwd middels goedgekeurde PSA	Groen
10. Aansluiting met eventueel vorig plan duidelijk	Groen
11. Realisatiepad met producten (productbreakdown)	Groen
12. Benodigde (release) capaciteit geregeld	Groen
Organisatie	
13. Projectorganisatie en organisatorische ophanging passend	Groen
14. Is rekening gehouden met een OR-traject?	Groen
15. Verhouding externen en invulling sleutelposities	Groen
Communicatie	
16. Kwaliteit voorlegger	Groen
17. Aanpak interne en externe communicatie bepaald	Groen
Financiën	
18. Wijze van financiering afgestemd en fasegewijze financiering mogelijk	Groen
19. Baten afgestemd, voldoende onderbouwd en aannemelijk	Groen
20. Financieel goede onderbouwing	Groen
21. Structurele meerkosten aangegeven	Oranje
Beheersing	
22. Relatie met andere projecten/trajecten afgestemd	Groen
23. Risico's en fallback voldoende afgedekt	Groen
24. Beheersingsmechanismen voldoende	Groen

Toelichting: (indien oranje of rood)

21	PB constateert dat de inzet reeds in de begroting WB, daarmee is het niet te claimen in decharge:

	• 3,25 additionele fte voor het IB&P Champion-netwerk. Dit is reeds belegd in de lijnorganisatie. • 1 fte rolbeheer, 1 fte IB&P coördinator en 1 fte Risicomanager (business consultant) zijn al onderdeel van de begroting PB constateert dat in de besluitvorming rondom BIO 2023 de domein consultants reeds zijn meengenomen, niet claimen via decharge: • 3,2 FTE Domeinconsultants met betrekking tot werkzaamheden rondom de BIO. (€ 325k).

PB stelt tbv de centrale administratie van FEZ de volgende meer-minderkosten vast.

	Divisie/Directoraat	Kosten type	€ *1.000	notitie
Structurele kosten	WERKbedijf	Personeel	939	Er zijn als gevolg van dit project 7 fte's gerelateerd aan – bestaande – IB&P-rollen toegevoegd aan het WERKbedrijf.
Structurele Baten				

BIJLAGE 1

De FG heeft n.a.v. het dechargerapport onderstaande bevindingen geconstateerd. De reactie van het projectteam op deze bevindingen zijn hierin opgenomen.

#	Verzoeken	Reactie Projectteam
1	Bij het lezen van de stukken valt op dat een aantal zaken enigszins rooskleurig is neergezet. Er wordt bijvoorbeeld aangegeven dat alle 77 bevindingen zijn opgelost, terwijl er twintig restrisico's zijn geaccepteerd (dit betekent dat UWV juist accepteert dat een bevinding gedeeltelijk blijft bestaan en niet geheel wordt opgelost) en er ook nog overdrachtspunten zijn. Dit spreekt elkaar tegen. Ook bij de stelling dat alle projectresultaten binnen de gestelde termijn zijn afgerond heb ik mijn vraagtekens, omdat de planning op bepaalde punten gedurende het project is herzien. Ik verzoek de formulering hierop aan te passen, ook met het oog op het delen van deze stukken met SZW of de pers (zie kopje Communicatie van de voorlegger).	De term "oplossen" wordt consistent gehanteerd sinds het initiële projectplan (december 2020). In het dechargerapport (in de tweede zin in de managementsamenvatting) wordt de door ons gehanteerde definitie duidelijk aangegeven, namelijk: "Oplossen betekent hier dat het risico volledig is gemitigeerd of dat er sprake is geweest van een formele (gedeeltelijke) risicoacceptatie.". Aangezien 100% veilig, c.q. 0% risico niet bestaat, staan wij achter deze formulering en benadrukken wij de consistente toepassing hiervan. Aanpassing in dit stadium is niet wenselijk. Ten aanzien van de tweede opmerking: de externe planning is altijd geweest dat de middellange termijn-acties zouden zijn afgerond voor 31 december 2022. Deze planning is behaald en op basis van deze planning is de voortgang ook altijd extern gecommuniceerd. Daarnaast was er spraken van een interne planning die ambitieuzer was en waarin reserve-ruimte was opgenomen ten behoeve van eventuele tegenvallers gedurende het project. Geen actie nodig.

2	Het project onderkent twee overdrachtspunten. Deze punten zijn niet gerealiseerd, omdat die afhankelijk zijn van externe invloeden. OP1 is afhankelijk van een release, maar van welke externe invloeden OP2 precies afhangt, is o.b.v. het rapport niet duidelijk. Ook is de planning voor OP2 niet vermeld. Ik verzoek deze punten in het dechargerapport te verhelderen en een concrete opleverdatum op te nemen waar Werkbedrijf zich aan committeert.	Voor OP2 is reeds een verandersignaal ingediend. Deze actie is geborgd in Jira-ticket WBEDV65199 en zal uiterlijk 1 mei 2023 opgelost zijn.
3	Tevens vraag ik mij af of er geen andere overdrachtspunten zijn. Op basis van een scan van de restrisico's in de bijlage valt bijvoorbeeld op dat de structurele schoning (Priv 5.7) en het in kaart brengen van relevante GEB's (Priv 7.1) niet als overdrachtspunten worden meegeven, terwijl dit wel twee punten zijn die buiten het project dienen te worden opgepakt. Ik verzoek deze en eventueel andere niet benoemde punten ook op te nemen en te voorzien van een concrete opleverdatum.	Het project is zeer zorgvuldig geweest met het registreren van restpunten (inclusief overdrachtspunten, maar ook restrisico's en leerpunten). De QAC heeft bij elke decharge van acties en bevindingen geadviseerd, inclusief over overdrachtspunten en restrisico's. Alle overdrachtspunten en restrisico's zijn opgenomen in de rapportage. Ten aanzien van de genoemde voorbeelden: 1. Structurele schoning is middels de oplevering van het vernieuwde schoningsmechanisme (vanuit het project) beschikbaar gesteld aan de lijnorganisatie. Er is geen aanvullende actie nodig. De lijnorganisatie heeft schoning reeds opgenomen in haar reguliere werkzaamheden. De status wordt via de maandrapportages gereapporteerd, ten behoeve van de monitorgesprekken. Op termijn wordt deze controle en rapportage ook gefaciliteerd vanuit de GRC-tool. 2. GEB's: opgenomen via restrisico #19 (RR19); geaccepteerd. Het uitvoeren van de GEB's is reeds belegd in de lijn, als reguliere lijnactiviteit. Waarbij via het nieuwe risicomanagementproces dat is ingericht risico's vanuit bestaande en toekomstige GEB's zullen worden geregistreerd in en monitord via het GRC-systeem. Deze actie is niet nodig om het projectresultaat (alsnog, later) te behalen en betreft derhalve geen overdrachtspunt.
4	Gezien het aantal restrisico's en de vooraf voorziene risico's is het wenselijk dat het programma WORKit niet te lang op zich laat wachten, zodat deze risico's verder kunnen worden gereduceerd. Mocht de realisatietermijn van WORKit in de toekomst verplaatsen, dan is het wenselijk om deze risico's nogmaals tegen het licht te houden en te beoordelen of verdere acceptatie van deze risico's nog steeds acceptabel is. Ik verzoek daarom in het dechargerapport op te nemen tot welke datum de restrisico's worden geaccepteerd en wanneer er	De restrisico's zijn alle opgenomen in de GRC-tool en worden nu bewaakt middels het risicomanagementproces (geleid door de IB&P-risicomanager). De risicoacceptaties zijn soms "oneindig", maar alle geaccepteerd risico's worden minimaal jaarlijks geëvalueerd. Dit ook zo extra geduid in de managementsamenvatting.

	opnieuw een afweging van de risico's moet plaatsvinden.	
	Overige aandachtspunten:	
5	Ik verwacht dat Werkbedrijf er zorg voor draagt dat de restrisico's en de vooraf voorziene risico's in de relevante, bestaande en nog op te stellen domein GEB's van Werkbedrijf worden opgenomen.	Dit is geen projectverantwoordelijkheid. Het IV-office heeft het opstellen van de GEB's opgenomen in het jaarplan 2023. Daarbij wordt opgemerkt: • • Grote gedeelten van de domeinen zijn/worden met behulp van losse GEB's wel al in kaart gebracht. WERKbedrijf is binnen UWV koploper GEB-checks en GEB's. Het uitvoeren van een Domein GEB is arbeidsintensief voor IB&P en uitvoering/domeinen. • • Vertrekpunt GEB is privacy-by-design op alle nieuwe werkprocessen en producten. • • Achteraf "ver-GEB-ben" is niet effectief in verband met de uitfasering van WERKbedrijf legacy (via WORKit) en privacy-by-design (doel van een GEB) is achteraf niet meer mogelijk.
6	Op basis van de scan van de restrisico's in de bijlage valt op dat bij Priv 4.2 geen restrisico is benoemd. Dit betreft het verwerken van gezondheids- en/of medische gegevens in Sonar zonder wettelijke grondslag, doordat er vrije tekstvelden zijn genomen. Er zijn verbeteracties uitgevoerd, zoals een werkinstructie en de inrichting van controlewerkzaamheden, maar er blijft een risico bestaan dat medewerkers gezondheids- en/of medische gegevens in de vrije tekstvelden opnemen.	Priv4.2 is gekoppeld aan restrisico #10 (RR10); we hebben abusievelijk deze koppeling niet opgenomen in de tabel. Dit is nu verbeterd.
7	Het project heeft een aantal waardevolle adviezen en leerpunten in het dechargerapport genoemd. Een suggestie is om deze punten breder te delen binnen UWV, zodat ook andere projecten/organisatieonderdelen hier hun voordeel mee kunnen doen.	Dit wordt inderdaad zo opgevolgd (door de BSO, in het bijzonder).