Voorlegger vergadering Raad van Bestuur UWV

	Vergadering Raad van bestuur		
Datum	4 april 2023		
Agendapunt	Agendapunt 6	Nummer	23 – 116
Onderwerp	Decharge project 'Sonar IB&P'		
Directeur	Directeur Werkbedrijf		
Opsteller	5.1 lid 2 sub e		
Portefeuillehouder RvB	Guus van Weelden		

	Onderwerp heeft instemming van
Directeur	Toelichting
Advies Portfolio Bureau 22-3-2023	PB adviseert het eerder onder voorwaarde gegeven akkoord op het Dechargerapport te bekrachtigen. Stuurgroep Portfoliobureau is op 18 januari 2023 akkoord gegaan met de decharge, onder voorbehoud van het akkoord van de FG. De FG heeft op 26 januari 2023 akkoord gegeven onder voorwaarde van een vijftal verzoeken. Deze verzoeken zijn beantwoord. Voorstel tekst voor het Rijks ICT Dashboard: *De tekortkomingen, gebleken uit een externe privacy audit, van Sonar op het gebied van informatiebeveiliging en privacy (IB&P) zijn sterk gereduceerd. Dit omvat ook het accepteren van eventuele restrisico's op het juiste niveau van de organisatie*.
Advies PortfolioBureau 18-1-2023	PB adviseert akkoord te gaan met de decharge van het project Sonar IB&P. PB adviseert de leerpunten te bespreken in het IB&P-overleg. Gezien het belang van dit onderwerp en gezien de periode dat Sonar nog actief blijft langer is dan eerder is aangenomen, adviseert PB in juni een evaluatie te plannen met onder andere de BSO en CISO. PB adviseert daar te adresseren: - De restpunten dienen goed gevolgd te moeten worden en mede ook in lijn met het AcICT; - Dat er periodiek actief wordt gekeken naar nieuwe IB&P-risico's en de mogelijk dan te nemen aanvullende maatregelen; - Toetsing op de werking van de 77 maatregelen.
Reactie indienende directeur op PB-advies 22-03-2023	Tekst voor het Rijks ICT enigszins aanpassen naar: *Alle 77 bevindingen uit een externe privacy audit van Sonar op het gebied van informatiebeveiliging en privacy (IB&P) zijn binnen de gestelde termijn en budget opgelost. Dit omvat ook het accepteren en beleggen van eventuele restrisico's op het juiste niveau binnen de organisatie.*
Portfoliobureau WB	Het project is op 18 januari voorwaardelijk gedechargeerd. Het projectteam heeft inmiddels voldaan aan de gestelde voorwaarde. Portfoliobureau WB adviseert daarom om decharge te verlenen. • 18 januari 2023 heeft Portfolio Bureau Stuurgroep voorwaardelijk decharge verleend voor het project Sonar IB&P. De voorwaarde was dat de FG het dechargerapport zou doornemen en het projectteam gevolg zou geven aan eventuele adviezen. De inhoudelijke meerwaarde van dit project en reden voor decharge zijn destijds al toegelicht en worden om die reden niet nogmaals in deze voorlegger benoemd.

	• Op 27 januari heeft de FG inhoudelijk gereageerd op het dechargerapport en heeft enkele aanbevelingen gegeven. • Op 27 februari heeft het projectteam gereageerd op de aanbevelingen van de FG waarin zijn gevolg geven aan de aanbevelingen. De reactie is als bijlage opgenomen in het dechargerapport. • Op 28 februari is het DT Werkbedrijf akkoord met het dechargerapport. • Op 14 maart verzoekt Portfolio Bureau Werk Bedrijf Portfolio om de decharge te verlenen.

Door Raad van bestuur te nemen besluiten

1 Decharge op project Sonar IB&P (zie bijgevoegd Sonar IB&P dechargerapport v1.0)

Samenvatting onderwerp en reden bespreking

Deze voorlegger geeft een samenvatting van het resultaat van project Sonar IB&P. De volledige uitwerking is opgenomen in bijgevoegd eindrapport. Het onderliggende projectplan (v1.20) is goedgekeurd door de RvB op 31 januari 2022.

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 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 nieuw gecreëerde rol van 'IB&P Risicomanager' is een belangrijke factor in het toezicht op de restrisico's en restpunten, ondersteund middels het geïmplementeerde GRC-systeem.[1]

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 de paragraaf Financiële consequenties, hieronder.

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 waarin 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 resultaten van dit onderzoek zijn beschreven in de rapportage van de Accountantsdienst.

Gevolgen voor mensen

[1] Voor de rol van 'IB&P-risicomanager' is geen aparte functie gecreëerd. Het verdient aanbeveling deze rol UWV-breed te standaardiseren en formaliseren. Zie verder ook punt 2 onder het kopje 'Duurzaamheid' (p. 5).

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
Klant	De privacy van de klant wordt beter gewaarborgd. De klant moet erop kunnen vertrouwen dat zorgvuldig met zijn of haar persoonsgegevens wordt omgegaan, de persoonsgegevens adequaat worden beveiligd en alleen worden verwerkt indien noodzakelijk.
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.
Gebruikers Sonar	Het bewustzijnsniveau van Sonargebruikers over privacy en informatiebeveiliging is verhoogd en wordt periodiek meegenomen in awarenessactiviteiten.

Tabel 1 Bijdragen aan organisatiedoelstelling

Kansen en risico's voor (de opdracht van) UWV

Vanuit het project zijn de 77 KPMG-bevindingen opgelost. De hiermee gemoeide informatiebeveiliging & privacy-risico's zijn significant gereduceerd. In sommige gevallen zijn restrisico's geïdentificeerd. Deze zijn allen formeel geaccepteerd, op het juiste besluitvormingsniveau (gegeven de risicoclassificatie en rijkweidte van de impact; zoals ook beschreven is in het projectplan). Bijgevoegd eindrapport beschrijft de projectresultaten en restrisico's in detail (respectievelijk bijlagen A en C). Daarnaast zijn in bijlage E in detail de overkoepelende (project-) kansen en risico's beschreven.

Strategische aspecten van het besluit

Zie eindrapport (bijgevoegd), hoofdstuk 2 "Bijdrage aan organisatiedoelstelling". In het kort heeft dit project 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.

Bedrijfsvoering (personeel/financieel)

Financiële consequenties

De eenmalige en structurele projectkosten zijn hieronder weergegeven:

	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 Overig	€ 1.177 € 140	€ 492 € 149	-€ 685 € 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 het 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 jan. '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 een stukje administratieve uitloop in 2023, niet nodig geweest. Op kostensoortniveau is het aantal benodigde uren intern en extern hoger uitgevallen. Dit is met name het gevolg van het langer doorlopen dan oorspronkelijk begroot. De uitbestede 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 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.

Duurzaamheid

Diverse verbeteracties hebben een duurzaam karakter. De bestendigheid hiervan is expliciet onder de aandacht geweest in de eindevaluatie van de Accountantsdienst. Mede als gevolg van de (voorlopige) conclusies vanuit dit onderzoek van de Accountantsdienst, heeft het projectmanagementteam zelf ook twee belangrijke leerpunten onderkend:

1 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.
2 Voor een robuuste opvolging van (IB&P-) risico's is het verstandig een (gestandaardiseerde) functie voor Risicomanager UWV-breed in te richten. Een vergelijkbare rol is vanuit dit project nieuw gecreëerd bij het Werkbedrijf. De Risicomanager kan, met behulp van de hierboven benoemde GRC-tooling, zorgdragen dat (IB&P-) risico's gestructureerd worden geïdentificeerd, geregistreerd, opgevolgd en gemonitord.

Vervolgtraject besluitvorming

N.v.t.

Communicatie

Het project is in alle opzichten succesvol uitgevoerd. Dit is inmiddels gedeeld (middels een presentatie) met SZW.

Openbaarheid

Deze documenten kunnen openbaar gemaakt worden (onderbouw ook de keuzes voor opties 2, 3 en 4):

1 ☒ Ja, in hun geheel.
2 ☐ Deels, markeer in de documenten wat niet openbaar gemaakt kan worden.
3 ☐ Nee, de bijbehorende bijlage(n) niet.
4 ☐ Nee, helemaal niet.