Voorlegger vergadering Raad van Bestuur UWV

	Vergadering Raad van bestuur		
Datum	5 maart 2024		
Agendapunt	Agendapunt 13	Nummer	24 – 079
Onderwerp	Verklaring over Informatiebeveiliging 2023		
Directeur	CIO/Concern ICT		
Opsteller	CISO		
Portefeuillehouder RvB	René Steenvoorden		

Directeur	**Onderwerp heeft instemming van** **Toelichting**
Functionaris Gegevensbescherming	Nadat de BIO doelstellingen van 2021 en 2022 slechts ten dele zijn gehaald is ook de eerste mijlpaal om per 1 januari 2024 aantoonbaar in control te zijn op alle processen en normen van de BIO in ten minste opzet en bestaan niet gehaald. UWV heeft bovendien nog niet duidelijk wat het totaal aan informatiesystemen en processen is dat beveiligd moet worden. De FG heeft eerder geadviseerd de algemeen directeuren te vragen om tot een aanpak van de BIO te komen, waar meer urgentie uit spreekt en prioriteit te geven aan de activiteiten. Deze notitie laat zien dat daar nu werk van gemaakt wordt en directies gedwongen worden aandacht en prioriteit te geven aan BIO compliance. Dat is positief. Toch moet rekening gehouden worden dat sommige bedrijfsonderdelen een aanzienlijke vertraging zullen moeten rapporteren ten opzichte van de einddatum van 1 januari 2026
Directeur FEZ	FEZ deelt het geschetste beeld over de voortgang. Een aantal bedrijfsonderdelen hebben achterstanden in te lopen. De aanvullende sturingsmaatregelen gaan hieraan bijdragen. Waar mogelijk zullen de staf afdelingen de bedrijfsonderdelen daarbij ondersteunen om de afgesproken doelstellingen te behalen.

Door Raad van Bestuur te nemen besluiten

1. Kennis te nemen van de UWV Verklaring over Informatiebeveiliging 2023;
2. Kennis te nemen van de aandachtspunten in deze voorlegger;
3. Kennis te nemen van de stappen om de sturing over de BIO te versterken:
   a) Uniform BIO dashboard
   b) Bespreking van het onderwerp in de RvB; 4 maandelijks
   c) Bespreking van het onderwerp in de kwartaalgesprekken met de directeuren
   d) Bespreking van het onderwerp in de IV board; maandelijks
4. Evaluatie in Q3 2024 van de effectiviteit aanscherping sturing ten aanzien van realisatie van mijlpalen inclusief advies vervolgaanpak
5. Opdracht te geven aan de Algemeen Directeuren om onderstaande acties uit te voeren, zodat er een versnelling plaatsvindt om de ambitie van de RvB te behalen om in 2026 volledig compliant te zijn met de Baseline Informatiebeveiliging Overheid (BIO);
   a) Divisies en directies waar een achterstand is ontstaan stellen uiterlijk per 31 maart 2024 een plan van aanpak op om de opgelopen achterstand ten opzichte van het geambieerde BIO-groeipad in te halen en de mijlpaal te behalen (*UWV heeft voor alle belangrijke processen en systemen de informatiebeveiliging (IB) op orde in opzet, bestaan en werking*); Bij het opstellen van het plan dient rekening gehouden te worden met de volledigheid van de processen en systemen alsmede de vastgestelde uniforme werkwijze en maatregelenset.

Samenvatting onderwerp en reden bespreking

Context en ambitie Raad van Bestuur

Om de diensten van UWV aan cliënt en burger te kunnen leveren, is het cruciaal dat informatie adequaat beveiligd is. UWV stelt jaarlijks (sinds 2021) een Verklaring over Informatiebeveiliging op waarin wordt verantwoord over informatiebeveiliging en de voortgang van de BIO implementatie. In januari 2022 heeft de RvB de volgende ambitie vastgesteld per 1 januari 2026: 'UWV heeft haar Informatiebeveiliging op orde en voldoet in haar geheel aan de BIO voor alle processen en systemen in opzet, bestaan en werking.'

Resultaten op het gebied van informatiebeveiliging in 2023
In 2023 heeft UWV verder gewerkt aan de ambitie aan de BIO te voldoen. BIO In Control Verklaringen (ICV) zijn per divisie opgeleverd. De divisies hebben een grote inzet gedaan en verdere verbeteringen gerealiseerd op het gebied van informatiebeveiliging. Enkele divisies lopen voor op de doelstellingen voor 2023, echter zijn er ook divisies waar achterstanden zijn ontstaan. UWV-breed is nog onvoldoende voortgang geboekt voor de doelstellingen in 2023 omdat 3 organisatieonderdelen significant achterblijven ten opzichte van de planning (K&S, GD en GIV). K&S heeft een route gekozen waarbij ze wel aan hun eigen planning hebben voldaan, maar niet de mijlpalen van de RvB hebben behaald. UWV-breed zijn de processen voor 69% beoordeeld en de systemen zijn voor 46% beoordeeld. Als gevolg van deze achterstanden is het behalen van de ambitie om volledig en UWV-breed aan de BIO te voldoen per 1-1-2026 onzeker. Hierdoor is er geen totaal zicht op de kwetsbaarheden, waardoor de informatiebeveiligingsrisico's groter worden.

Aandachtspunt

Versterking van kwaliteitsborging door BC&K in samenwerking met CISO
De inrichting van kwaliteitsborging is beschreven in de IB&P governance en opgenomen in de 'werkset maandrapportage' van FEZ. In de praktijk wordt er bij verschillende divisies nog niet volledig conform de afspraken gewerkt voor het borgen van kwaliteit op het gebied van IB&P. Het borgen van de kwaliteit is primair een verantwoordelijkheid van de lijn. De BC&K afdelingen hebben hierbij ook een verantwoordelijkheid, namelijk de controle van de werking van het kwaliteitssysteem. Om de ambities van de RvB te realiseren dient de kwaliteitsborging door BC&K in samenwerking met CISO versterkt te worden om de IB&P governance in de praktijk te laten functioneren. Ter kennisname geven we aan dat het aankomende jaar FEZ, de BC&K afdelingen en CISO samenwerken aan het uniformeren van de diepgang ten aanzien van de verantwoording over de BIO.

Ondernomen stappen om de sturing over de BIO te versterken

Uniform BIO dashboard
CISO Office heeft een uniforme maatregelenset en uniforme werkwijze vastgesteld die wordt ondersteund door Governance, Risk en Compliance Software (GRCControl). Dit draagt bij aan de RvB ambitie om op een uniforme wijze inzicht te geven in en te kunnen verantwoorden over informatiebeveiliging. Het uniforme BIO dashboard wordt de basis van de voortgangsgesprekken in de genoemde gremia's

Bespreking van het uniforme BIO dashboard
Op basis van de verklaring over de informatiebeveiliging 2023 is geconstateerd dat de sturing op de implementatie van de BIO niet op alle niveaus in de organisatie heeft plaatsgevonden. Dit heeft als gevolg dat tijdige en adequate sturing, om de ambities van de RvB te behalen, beperkt heeft plaatsgevonden. Om de juiste sturing op het juiste niveau te laten plaatsvinden zijn aanvullende maatregelen genomen. Dit betekent concreet dat het onderwerp 4 maandelijks wordt besproken in de RvB op basis van de IB&P tertaalrapportage. Daarnaast zal in de kwartaalgesprekken met de directeuren dit een standaard onderwerp op de agenda zijn en zal in het IV board maandelijks de voortgang en eventuele belemmeringen worden besproken en geadresseerd.

De bovengenoemde stappen om de sturing over de BIO te versterken worden halverwege het jaar geëvalueerd en indien nodig worden hier passende vervolg acties op genomen. De evaluatie vindt plaats op directie niveau en besluitvorming over mogelijke interventies op bestuurlijk niveau

Acties

Actie 4a: Divisies en directies waar achterstanden zijn ontstaan stellen een plan van aanpak op
Op basis van de Verklaring over Informatiebeveiliging 2023 lopen enkele divisies en directies achter op het geambieerde BIO-groeipad omdat niet alle processen, systemen en normen zijn getoetst in opzet en bestaan. Divisies en directies die achterlopen dienen een plan van aanpak op te stellen om de achterstand ten opzichte van het geambieerde BIO-groeipad in te halen en tevens de mijlpaal voor 1-1-2025 te behalen: 'UWV heeft voor alle belangrijke processen en systemen de informatiebeveiliging (IB) op orde in opzet, bestaan en werking'. Bij het opstellen van het plan dient rekening gehouden te worden met de volledigheid van de processen en systemen alsmede de vastgestelde uniforme werkwijze en maatregelenset.
Op dit moment moeten de organisatieonderdelen het BIO scopeformulier voor 2024 uiterlijk per 29 februari 2024 aan CISO office opleveren. Het PvA moet uiterlijk per 31 maart 2024 aangeleverd worden waarin opgenomen hoe achterstanden op een tijdige manier ingehaald worden en waarin ook een doorkijk wordt

gegeven naar de laatste mijlpaal RvB op 1 januari 2026. Middels kwartaalsturing houdt CISO office hier ook grip op.

Gevolgen voor mensen

Het niet voldoen aan de BIO kan tot negatieve gevolgen leiden voor de bescherming van persoonsgegevens en de (geautomatiseerde) gegevensverwerking. Als gevolg hiervan kan informatie van cliënt, burger, medewerker en partners in verkeerde handen komen, uitkeringen worden niet of niet tijdig overgemaakt of cliënten kunnen niet (tijdig) worden begeleid naar werk.

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

Er zijn kansen om de opgelopen achterstand op het gebied van de BIO in te halen, door het uitvoeren van de voorgestelde acties. Er zijn risico's omdat (cyber)dreigingen en de potentiële schade significant is. Dit wordt ook door het Nationaal CyberSecurity Centrum bekrachtigt in het 'Cybersecuritybeeld Nederland 2023 (CSBN). Voorbeelden van negatieve effecten zijn:

- Verstoringen van dienstverlening richting cliënt, burger, medewerker en partners van UWV;
- Grootschalige negatieve media-aandacht voor UWV;
- Privacy schending van cliënt, burger en/of medewerker;
- Overtreding van wettelijke regelingen zoals de AVG.

Strategische aspecten van het besluit

De gevraagde besluiten hebben op de volgende aspecten uit de UWV Strategie 2021-2025 betrekking:

- **UWV en de buitenwereld:** Uitlegbaar en doenlijk
- **UWV en de eigen organisatie:** Eén UWV, Lerende organisatie & ICT

Bedrijfsvoering (personeel/financieel)

Om de achterstand in te lopen op het gebied van informatiebeveiliging en compliance met de BIO dienen divisies en directies een jaarplan op te stellen inclusief een personele en financiële planning. Een efficiëntieslag in de bedrijfsvoering kan gemaakt worden door het implementeren van de uniforme werkwijze.

Duurzaamheid

Pijler Maatschappij
Impact op maatschappelijke thema's – De gevaren en schades aan de informatievoorziening worden steeds groter en ernstiger. Het implementeren van het normenkader BIO levert een grote bijdrage aan het mitigeren van risico's en reduceren van impact op de beschikbaarheid, integriteit en de vertrouwelijkheid van de gegevens van de burgers.

Vervolgtraject besluitvorming

Na besluitvorming moet de Groepsraad worden betrokken bij verdere besluitvorming over prioriteitsstellingen en ambities inzake informatiebeveiliging.

Communicatie

Communicatie vindt plaats via reguliere kanalen.

Openbaarheid

Deze documenten kunnen openbaar gemaakt worden:

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.

Metadata

Omschrijving: Verklaring over informatiebeveiliging in 2023, waaronder de verantwoording over de Baseline Informatiebeveiliging Overheid (BIO).
Trefwoorden: Verklaring over informatiebeveiliging, Baseline Informatiebeveiliging Overheid, BIO, In-Control Verklaring, ICV