Naam activiteit/ proces	Risico definitie fraude	Risicodefinitie M&O	Geschat risico	Beheersmaatregelen	WAAR
Algemeen					
Bedrijfsvoering	Het risico dat door onkunde, gebrek aan waarde- en normbesef of onduidelijkheid over de bedrijfsethiek medewerkers misbruik maken van hun positie.	Integriteit en betrouwbaarheid zijn basisbegrippen voor de GR Sociaal.	Laag	Dilemma's bespreekbaar maken (verplicht introductieprogramma nieuwe medewerkers), AO/ IB op orde, controles op de uitvoering, klokkenluidersregeling, ambtseed/ belofte, screening van nieuw personeel (VOG), inventarisatie nevenfuncties/ werkzaamheden.	GRS
Bedrijfsvoering (AVG)	Het risico dat medewerkers oneigenlijk toegang krijgen/ gebruik maken van persoonsgegevens/ informatie van klanten.		Laag	•Er is een SDD-autorisatiematrix op grond waarvan is bepaald welke functies, toegang moeten hebben tot welke gegevens/ systemen. Deze toegang wordt d.m.v. specifieke functies in het systemen (Suwinet, Centric Suites, etc.) verleend; •Alleen GRID-accounts kunnen autorisatie krijgen; •Toegang van personen tot gegevens/ functies in systeem vindt d.m.v. (toegang) autorisaties plaats na goedkeuring management (afdelingshoofd) en toetsing aan autorisatiematrix; Dit gebeurd door de functionele beheerders van de SDD; •(Tenminste) jaarlijks wordt de autorisatiematrix gecontroleerd/ geactualiseerd door onafhankelijke AVG functionarissen (SDD) en FG (SDD) en externe accountant (BDO) d.m.v. audit bij jaarrekening. Er vindt op dit moment een actualisatie plaats. Uitgangspunt is dat de matrix jaarlijks wordt vastgesteld door MT. Het actualiseren en controleren is een gezamenlijke taak vanuit privacy, informatieveiligheid en het betreffende afdelingshoofd. Het toezicht houden is belegd bij de FG (SDD). •Voor Suwinet vindt nog een aanvullende controle plaats (steekproef) op verstrekte toegang door de gemandateerde of de functioneel beheerder i.o.v. de gemandateerde.	GRS
Bedrijfsvoering (AVG)	Het risico dat medewerkers oneigenlijk toegang krijgen/ gebruik maken van persoonsgegevens of dat persoonsgegevens niet vertrouwelijk worden behandeld.		Laag	• Door te werken met het 'register van verwerkingen', bij wijziging op gebruik van gegevens of applicaties, wordt dit doorgegeven aan de Privacy Coördinator die dit moet melden bij de Record Manager (wijzigt in de applicatie I-Navigator het proces). • De SDD werkt met Mavim als register van verwerkingen. Dat wordt gewijzigd op aangeven van de Privacy Coorindator. Gezien het eigen register geven wij dit niet door aan de Record Manager. Daarnaast wordt er voor iedere applicatie die gebruikt wordt, voor het verwerken van persoonsgegevens, een verwerkersovereenkomst afgesloten indien dit van toepassing is. Door het inrichten van de applicaties (privacy by design) op een zodanige manier dat er vooraf wordt vastgesteld welke gegevens, welke doelbinding en welke mate van autorisatie nodig is kunnen we ook borgen dat we als SDD goed met de gegevens omgaan. Hoe de informatie up-tot-date te houden is door de Privacy Coördinatoor vastgelegd in een plan van aanpak. Daarnaast zijn binnen de organisatie naast de officiële functies ook privacy-ambassadeurs aangewezen die als extra ogen en oren fungeren. • Er is één privacy coördinator er zijn binnen de SDD ook privacy-ambassadeurs. Het zorgen dat applicaties goed worden ingericht en up-to-date blijven is een samenwerking tussen privacy, informatieveiligheid, informatiemanagement en I&A. • Er is een Functionaris Gegevensbescherming (FG) aangesteld. Een FG is een interne (onafhankelijke) toezichthouder op het gebied van privacy en op de verwerking van persoonsgegevens. De FG wordt bij de werkzaamheden bijgestaan door juridische adviseurs/ ondersteuners. Jaarlijks rapporteert de functionaris gegevensbescherming aan de algemeen directeur van de SDD over de mate van compliance en de attentiepunten op het gebied van privacy en gegevensbescherming. • Er is een privacybeleid opgesteld (vastgesteld 18-10-2020 DSB). Op dit moment wordt het privacybeleid herzien en naar verwachting wordt het in Q4 2022 opnieuw vastgesteld.	GRS

Alle processen/ activiteiten			Middel	•Adequate (verplichte) training personeel (Samen Wijzer opleidingsprogramma); •Actuele handboeken met procedurebeschrijvingen en met wet- en regelgeving. Daarnaast worden actualiteitenbijeenkomsten georganiseerd; •Vastgesteld Integriteitsbeleid en Gedragscode (6-11-2014 DSB). Integriteit maakt onderdeel uit van het personeelsgesprek; •De GRS kent een klokkenluidersregeling; •Medewerkers van de GRS hebben de mogelijkheid om de ambtseed of belofte af te leggen. Nieuwe werknemers zijn hiertoe verplicht; •Bestuurders en ambtenaren zijn verplicht om nevenwerkzaamheden die de belangen van de GRS kunnen raken te melden bij de leidinggevende; •(Integriteit)screening personeel bij indiensttreding (VOG vast personeel en inhuur); •Verbijzonderde interne-controle resulterend in een specifieke accountantsverklaring op de processen bij het SDD; •Bij het gebruik van bedrijfsmiddelen (zoals wagenpark) wordt een (kilometer-) administratie gebruikt.	GRS
Lonen en Salarissen					
Personeels- en salarisadministratie	Risico tot onrechtmatige betalingen/ ongeautoriseerde salarismutaties: • onjuiste inschaling/ periodiek; • personen die niet in dienst zijn; • variabele vergoeding etc.		Middel	Door interne beheersmaatregelen worden foutieve mutaties voorkomen: • controle technische functiescheiding, onderliggende (getekende) stukken en betaling; • In AFAS worden alle mutaties m.b.t. personeel ingevoerd incl. motivatie door leidinggevende en daarna verwerkt door P&O (SGD); • De verbijzonderde interne controle ziet deels toe op de juiste uitvoer van het proces. Deze controlewerkzaamheden worden getoetst door de accountant (onderdeel van de het auditplan); • Daarnaast zijn er diverse (standaard) rapportage mogelijkheden die het mogelijk maken om (zelfstandig) controles uit te voeren; • Leidinggevende controleert en autoriseert (salaris-)mutaties; • Periodieke aansluiting salarisadministratie en financiële administratie.	GRS/ SGD
Declaraties (/ onkostenvergoedingen)	Het risico dat niet-gemaakte kosten worden gedeclareerd en/ of het risico dat privé-uitgaven worden gedeclareerd.		Middel	• Declaraties worden door medewerker ingediend en leidinggevende dient deze te controleren en te autoriseren; • Bij MT-leden declareren binnen AFAS personeelssysteem, deze worden geaccordeerd door de directeur; • Directeur declareert binnen AFAS en deze wordt geaccoordeerd door plaatsvervanger directeur; • P&O is uitbesteed aan de SGD, deze wordt gecontroleerd door de VIC van de SGD en de accountant.	GRS
Tijdsverantwoording	Risico dat niet-gewerkte uren als werktijd worden verantwoord. • vaste medewerkers; • inhuur krachten.		Middel	Inhuur: uren declaratie wordt gecontroleerd en geaccordeerd door budgethouder (afdelingshoofd/ projectleider). Bij vaste medewerkers wordt er gestuurd op de output.	GRS
Auto's	Risico op prive gebruik van de auto (totaal mag er belastingtechnisch maar 500 km prive mee worden gereden). Risico dat bekeuringen voor rekening SDD komen.		Middel	Er zijn 11 lease wagens en 1 eigen wagens (BBD 12 jaar oud) Gebruik van de auto van BBD zit geen controle op. Bij de lease wagens is dit wel geregeld: Er zijn twee beheerders van het wagenpark, dat zijn de FA medewerkers van middelen. • Ieder geautoriseerde bestuurder heeft een eigen tag (mag niet afgegeven worden), waarmee zij/ hij met de auto kan rijden; • Bij het in ontvangst nemen van de sleutel, moet de bestuurder een (kleine) overeenkomst tekenen met de voorwaardes van gebruik; • Bekeuringen en dergelijke komen voor rekening van de bestuurder die de auto op dat moment gebruikte, wordt ingehouden op salaris. Bij inhuur wordt er een rekening gestuurd; • Er is een track en trace systeem, waarbij gevolgd kan worden waar de auto's zich begeven. Dit wordt steekproefsgewijs door FA gecontroleerd.	SDD
Nevenwerkzaamheden	Het risico dat als gevolg van nevenwerkzaamheden de werkzaamheden als ambtenaar/ bestuurder niet onafhankelijk plaatsvinden.		Laag	• Er is beleid waarbij nevenfuncties gemeld moeten worden en toestemming gegeven moet worden door afdelingshoofd. Afdelingshoofden melden dit bij betreffende MT, ect. • Het geactualiseerde integriteitsbeleid (inclusief regeling nevenwerkzaamheden) is op 6-11-2014 vastgesteld.	GRS
Parkeerabonnementen	Risico dat er teveel parkeerabonnementen verstrekt worden		Laag	Een aanvraag voor een parkeerabonnement moet altijd door een afdelingshoofd worden gedaan. Het afdelingshoofd moet aangeven of dat het parkeerabonnement voor de afdeling bestemd is of voor een medewerker met een medische indicatie. Tevens kan het een onderdeel zijn van de arbeidsvoorwaarden.	GRS
Belastingen en sociale premies					

Loonheffing, omzetbelasting e.a.	Het risico dat aangiften niet juist, tijdig en/ of volledig worden ingediend en betaald.		Laag	• Verbandscontroles BTW/ BCF worden uitgevoerd door FA van SGD; • De VIC bij SGD ziet deels toe op de juiste uitvoer van het proces. Deze controlewerkzaamheden worden getoetst door accountant (onderdeel van de het auditplan SGD); • Het SGD heeft groen licht gekregen om een tax control framework (TCF) op te zetten. In 2016 is het TCF op het gebied van BTW volledig ingevoerd en geborgd in de SGD-organisatie. Er is ook extra ingezet op loonbelasting door de inzet van een fiscalist loonbelasting; • Voor de vennootschapsbelasting wordt een externe fiscalist ingeschakeld.	GRS/ SGD
Subsidies					
Het verstrekken van subsidies	Subsidies worden (bewust) onterecht verstrekt aan organisaties, waarin een bestuurder of ambtenaar een privébelang heeft. Onrechtmatig/ onwettig subsidieaanvragen of verstrekken.	Subsidies worden onterecht of te hoog verstrekt o.b.v. onjuiste en onvolledige informatie. Vs op subsidie worden verstrekt zonder dat er een aanvraag en of besluit is.	Laag	• Bestuurders en ambtenaren worden gescreend op nevenfuncties. • Er is een subsidieverordening vastgesteld door het DB en door gemeenten. Ook zijn er nadere regels vastgesteld, waarin e.e.a. omtrent de subsidie verder is uitgewerkt. • Er is een controletechnische functiescheiding aangebracht in het subsidieproces. Tevens inhoudelijke toetsing op de ingekomen stukken en controle achteraf (steekproef); • Ondertekeningsbevoegdheid is in de mandaatregeling geborgd; • Afrekening vindt plaats o.b.v. de verantwoording van de subsidie door de gesubsidieerde instelling.	SDD
Het ontvangen van subsidies (ESF of gelden via Gemeenten die zij hebben ontvangen voor specifieke werkzaamheden)	• Het risico dat subsidievoorwaarden niet worden nageleefd en/of subsidies onrechtmatig worden gedeclareerd. • Opbrengsten worden niet ontvangen door de GR Sociaal, maar overgemaakt op een andere rekening • Gelden worden niet verantwoord naar/ afgerekend met de verstrekker		Laag	• Het aanbrengen van controletechnische functiescheiding tussen het aanvragen, uitvoeren en controleren van de subsidie; • Centrale coördinatie van doeluitkeringen/ subsidies (P&C); • De aanvraag en nadere correspondetie wordt gecontroleerd met de bijgeleverde stukken; • Als onderdeel van de reguliere P&C-cyclus wordt gecontroleerd wat de stand van zaken is van de doeluitkering/ subsidie; • Overzicht wordt bijgehouden door P&C; • Subsidies worden opgehaald (begroot) via P&C documenten; • Afrekening gaat via burap/ jaarrekening.	SDD
Inkopen/ aanbestedingen					
Budgetbeheer	Het risico dat er ongeautoriseerde betalingen worden verricht. Het risico dat er valse facturen door medewerkers worden ingediend.	Het risico dat facturen worden gestuurd aan de organisatie waar geen tegenprestatie aan te grondslag ligt.	Middel	• Budgetbeheerder legt de opdrachten ter ondertekening voor conform mandaatregeling; • Opdrachtverstrekking wordt vastgelegd, prestatie moet worden gecontroleerd; • Controle op echtheid factuur en tenaamstelling (4-ogen principe codeur en controleur); • Controle technische functiescheiding bij inkoop: verstrekken opdracht door mandaathouder conform mandaatregeling, controle door budgethouder/ projectleider en vastlegging en betaling door financiën. Door RMO wordt er jaarlijks een VIC uitgevoerd op o.a. prestatieverklaringen. D.m.v. data-analyse controleert de accountant bij de eindejaarscontrole integraal alle inkoopfacturen.	GRS/ SDD
Ontvangst en controle	Het risico dat (fictieve) facturen worden betaald waarvoor geen overeenstemming is tussen de factuur en de geleverde prestatie.		Middel	• Voor elke factuur wordt door team P&C/ FA nagevraagd bij de verantwoordelijke of de prestatie geleverd is en de prijs conform afspraak is. Ook wordt de factuur gecontroleerd op echtheid en tenaamstelling;	SDD
Bestellen en gunnen	Risico op belangenverstrengeling of niet onafhankelijke selectie.		Middel	• Het 4-ogen principe is onderdeel van het inkoop- en aanbestedingsbeleid. Daarnaast is veel aandacht voor integriteit en 4-ogen principe voor factuur afhandeling (budgethouder en geleverde prestatie). Er wordt zoveel mogelijk gewerkt met preferred suppliers waarmee onder de aanbestedingsgrens ook aandacht is voor dit risico;	SDD
Het afhandelen van inkoopfacturen	Het risico dat privé uitgaven ten laste van de organisatie worden gebracht. Het risico dat inkoopfacturen betaald worden zonder dat er een prestatie geleverd is.	Facturen waar geen tegenpresentatie ten grondslag ligt worden betaald.	Hoog	• Declaraties van medewerkers worden geaccordeerd door de leidinggevende. Hierdoor vindt er controle op declaraties plaats. Alleen goedgekeurde declaraties worden door personeelsadministratie verwerkt. Door middel van interne controle wordt hierop toegezien. Indien een declaratie via de crediteurenadministratie loopt dan doorloopt deze een standaard route. Hierdoor vindt er functiescheiding plaats; • Facturen worden afgehandeld volgens een standaard routing. Hierdoor vindt controletechnische functiescheiding plaats tussen budgethouders en financiële administratie. Daarnaast vindt jaarlijks een rechtmatigheidscontrole plaats waarbij onder andere wordt gekeken naar vastlegging van de prestatie (autorisatie van de inkoopfacturen door de budgethouder); • Bij MT-leden is het afhankelijk van het bedrag en Budgethouderschap, afhankelijk of het bedrag binnen mandaat blijft; • In principe worden betalingen altijd gedaan met toevoeging van een factuur, deze zijn te controleren door de accountant en/ of RMO; • Controletechnische functiescheiding boeken versus betalen (SGD).	SDD/ SGD

Inkoop en aanbesteding	Risico het niet na leven van Europese en interne richtlijnen. Risico niet naleven contract voorwaarden.		Middel	• Periodiek wordt het inkoop- en aanbestedingsbeleid Drechtsteden geactualiseerd. Dit beleid wordt door het DB vastgesteld. Duidelijke communicatie vindt plaats (o.a. d.m.v. regionale bijeenkomsten) naar medewerkers wanneer interne en/ of externe wetgeving wijzigt; • Daarnaast vindt jaarlijks een GRS breed rechtmatigheidsonderzoek plaats naar inkoop- en aanbesteden (spendanalyse); • Binnen GRS zijn een tweetal contractmanagers werkzaam. Eentje voor de GRS brede contracten en daarnaast één specifiek voor IT; • Bij afwijkingen (lager dan Europees aanbestedings norm) moet een afwijkingsmemo gemaakt worden, deze wordt getekend door budgetverantwoordelijke conform mandaatregeling.	GRS
Memoriaalboekingen					
Memoriaalboekingen	Het risico dat memoriaalboekingen niet juist, tijdig en volledig zijn geautoriseerd en verwerkt, waardoor het identificeren van afwijkingen wordt bemoeilijkt.		Laag	• Een memoriaalboeking is een interne boeking die wordt beoordeeld via het 4-ogen principe. De financieel adviseur stelt hem met verpichte bijlage/ verantwoording. SGD verwerkt de memoriaalboekingen; • Memoriaalboekingen worden jaarlijks via een thema onderzoek gecontroleerd door de verbijzonderde interne controle (aselect).	GRS
Crediteuren					
Betaling/ factuur	Risico van ongeautoriseerde betalingen en betalingen aan niet-rechthebbenden. (Onrechtmatige onttrekking van GRS gelden.)		Hoog	Controletechnische functiescheiding tussen opdrachtverstrekking, verwerken van inkoopfacturen, factuur controles (zoals controle op echtheid opdrachtverstrekking, prestatieverklaringen e.d.) en betalen. 4-ogen principe bij betalingen en bij mutatie crediteurengegevens (SGD). De verbijzonderde interne controle ziet deels toe op de juiste uitvoer van het proces. Deze controlewerkzaamheden worden getoetst door accountant (onderdeel van het auditplan SGD). Deze zit in de controle prestatielevering die door de VIC (RMO) wordt gedaan.	SDD/ SGD
Vorderingen					
Debiteuren	Risico tot niet betalen van rekeningen en daarmee geen invulling aanmaning. Tevens vorderingen ongeautoriseerd afboeken. Risico dat betalingen bewust worden afgeboekt op andere debiteuren.		Laag	• Budgethouder geeft bij indiening van nota aan welke acties bij niet betaling worden genomen; • Inschakeling deurwaarder na contact met de budgethouder; • Regelmatig contact met de budgethouder over niet betaalde nota's; • Debiteurenbewaking; • Aansluiting deb. = grootboek; • Onderdeel van de jaarlijkse accountantscontrole.	SDD/ SGD
Debiteuren (uitkeringen)	Het risico dat vorderingen bewust worden afgeboekt, door een niet bevoegde medewerker.		Laag	• Bij een afboeking debiteur, moet altijd door een afdelingshoofd worden goedgekeurd (via een beschikking en/ of handtekening op rapportage); • RMO controleert hierop d.m.v. steekproeven.	SDD
Overige opbrengsten					
Opbrengsten GRS	Het risico dat er bewust te weinig gefactureerd wordt aan gemeenten volgens de bijdrageverordening en er een liquiditeitsprobleem ontstaat. Het risico dat opbrengsten niet worden geïnd op een bankrekening van de GRS en hierdoor geld aan de GRS wordt onttrokken.		Laag	De bijdragen en verdeelsleutels van de gemeenten zijn vastgelegd in de begroting van de GR Sociaal. In de jaarrekening wordt hier op gerapporteerd, een afwijking is niet mogelijk. Alle inkomsten komen binnen op een bankrekening van de GRS. Periodiek vinden er controles plaats op de openstaande posten.	GRS
Alle opbrengsten	Het risico dat deze opbrengsten niet worden geïnd op een bankrekening van GRS en hierdoor geld aan GRS wordt onttrokken. Het risico dat opbrengsten bewust tegen een te laag bedrag worden opgehaald.		Middel	Voorbedrukte formats/ briefpapier met hierop het bankrekening van de GRS. SGD verstuurt de nota's. Medewerker van GRS kan daar niet bij/ heeft deze bevoegdheid niet. De brieven en nota's worden gecontroleerd op de juiste gegevens. Er vindt controle plaats op de gefactureerde opbrengsten en de begroting.	GRS

Waarde documenten/ ov reispassen t.b.v. re-integratie, kasgeld.	Het risico dat medewerkers van de SDD bewust oneigenlijk gebruik maken van middelen van de SDD (waarde documenten/ ov-reispassen) en bewust kasgelden ontvreemden ter zelfverrijking.		Middel	• Alle waardedocumenten worden opgeslagen in een kluis; • Er wordt periodiek een sluitende verbandscontrole uitgevoerd op de mutatiestroom van waarde documenten: beginvoorraad + ingekochte waarde documenten -/- vernietigde waarde documenten -/- eind voorraad = verkochte waarde documenten; • De voorraad wordt periodiek door ten minste twee personen geïnventariseerd (4-ogen); • De toegang tot de hoofdvoorraad waarde documenten is beperkt tot slechts enkele personen; • Overdracht van waarde documenten gebeurt middels kwijting (ondertekening).	SDD
Wet op de lijkbezorging	Bij overlijden van een persoon waarbij niemand beschikbaar is om de zaken te regelen, wordt een huisbezoek afgelegd om middelen veilig te stellen waarmee de kosten van begrafenis/ crematie (deels) kunnen worden voldaan. Het risico is dat de medewerker(s) van de SDD deze middelen niet registreren en nlever(t)(en) bij de SDD.		Laag	• De 2 medewerkers die samen het huisbezoek afleggen nemen de (kleine) zaken van waarde mee en leveren die zaken in bij de Financiële Administratie; • Van de meegenomen zaken wordt een lijst gemaakt, die door beide medewerkers wordt geparafeerd; • De Financiële Administratie checkt of alle zaken op de lijst daadwerkelijk ook ingeleverd worden en plaatsen het in de kluis; • De lijst wordt opgeslagen in het dossier. (Aan de deze maatregel wordt momenteel gewerkt.)	SDD
Bezwaar en beroep					
Bezwaar en beroep	Het risico dat de behandeling van bezwaar- en beroepschriften bewust door een niet onafhankelijke medewerker plaatsvindt.	Het risico dat onjuiste of onvolledige informatie wordt verstrekt teneinde de uitspraak op het bezwaar- of beroepschrift te beïnvloeden.	Laag	• Er is een procedure voor bezwaar en beroep vastgesteld; • Er is een bezwarencommissie; • Leden van de bezwarencommissie vervullen geen politieke of ambtelijke functie; • Er is een registratie van het aantal binnengekomen bezwaar- en beroepszaken en de resultaten (SDDMI).	SDD
Schuldhulpverlening					
Schuldsanering	Het risico dat het behandelen van schuldsaneringsaanvragen bewust niet onafhankelijk plaatsvindt of het risico dat bewust vermenging van privéschulden en zakelijke schulden van cliënten plaatsvindt.	Het risico dat onjuiste of onvolledige informatie wordt verstrekt teneinde voor schuldsanering in aanmerking te komen.	Laag	• Medewerkers hebben bij in dienst name een verklaring omtrent het gedrag (VOG); • Functiescheiding tussen behandeling schuldsaneringsaanvraag, toekenning en registratie is nog niet gerealiseerd. De intakes worden weliswaar opgeboekt door de back-office, maar een check op toekenning, behandeling of registratie d.m.v. functiescheiding vindt niet plaats; • Duidelijke voorwaarden voor schuldsaneringstrajecten; • Goede dossiervorming; • De aanvrager wordt verzocht zich te legitimeren; • De door de aanvrager verstrekte gegevens worden geverifieerd met bewijsstukken (voor zover mogelijk van derden) en t.b.v. het dossier gekopieerd; • Inlichtingen bij derden inwinnen; • De SDD krijgt een zeer uitgebreide audit (1x in de drie jaar) vanuit NVVK met bevraging op zeer veel kwalitatieve (en enkele kwantitatieve thema's). Fraude is nu geen onderdeel van de audit. Het is wel zinvol om aan de NVVK mee te geven dat dit een onderdeel van de audit zou kunnen zijn als borging van mogelijke kwetsbaarheid op dit gebied. • Er is geen kwaliteitsplan welke relateert met een interne controle en een accountantscontrole. Dit zou er wel moeten komen ingaande. Dossieronderzoek d.m.v. interne controle vindt nu dan ook niet plaats. Dit moet wel ingebed worden voor de rechtmatigheidsverantwoording ingaande 2023 wordt dit ingebed in het RMO jaarplan.	SDD
Betalingen schuldhulpverlening via Allegro, dus niet via Key2Finance (budgetbeheer/bewindvoering, vrij te laten bedrag, uitbetaling schuldeisers etc.)	Het risico dat betalingen bewust onjuist plaatsvinden.	Betalingen worden onterecht of te hoog verstrekt door het niet volgen van de juiste betaalprocedure.	Laag	• Functiescheiding opdrachtgever (consulent ABS) en betaler (FA ABS); • Bij alle betalingen vindt een 2e handtekening plaats door een andere collega (deze zijn zowel 1 als 2e betaler wordt geroeleerd=risico) Er kan niet voor dezelfde batch door dezelfde persoon een 1e en 2e handtekening worden gezet, systeem dwingt dit af (info FA); • Nieuwe relaties worden op verzoek van consulenten ABS ingevoerd door secretariaat (naw gegevens), waarbij IBAN-nummer alleen door FA ABS kan worden toegevoegd. • Bij verzoeken tot invoeren van nieuwe relaties in Allegro wordt een bewijsstuk gevraagd (bankpas of nota derde). • Maandelijkse controle door BO II medewerker bij nieuw ingevoerde relaties voor check of IBAN-nummer overeenkomt met relatie.	SDD
Uitkeringsverstrekking					

Uitkeringen (beleid)			Laag	• Functiescheiding tussen het vaststellen van de verordening en beleid en de uitvoering door de GS.	SDD
Uitkeringen (juiste persoon)	Het risico dat bewust valse cliënten worden opgenomen in de uitkeringenadministratie en hierdoor te veel uitkeringen worden verstrekt.	Het risico dat onjuiste of onvolledige informatie wordt verstrekt teneinde voor een uitkering in aanmerking te komen.	Hoog	Functie scheiding tussen het behandelen van de aanvraag en dossiervorming, het besluiten op de aanvraag en voorstel tot betaling. (Functiescheiding behandelen aanvraag, besluiten en voorstel zit bij de regisseur FO is 1 pers. Invoering voor betaling en afgeven beschikking ligt bij de BO); • functiescheiding doelgroepaanvragen: De 'doorsnee' doelgroep aanvragen worden beoordeeld door de BO II aan de hand van een werkinstructie en Handboek Schulinck - intermediairslijst, zij vullen vervolgens ook het uitkeringsdossier. Indien de situatie van de klant afwijkend is, worden deze doelgroep aanvragen door gefaseerd naar de FO (inkomensadviseur) om de beoordeling te doen. Vervolgens krijgen we de aanvraag met een advies/besluit terug om het uitkeringsdossier te vullen en een beschikking te sturen. De doelgroep aanvragen die wij beoordelen gaan nog langs de FO om een regisseur aan de klant te laten koppelen. • De eisen, voorwaarden en normbedragen met betrekking tot het verstrekken van een uitkering zijn vastgelegd in een normenkader. (RMO heeft een normenkader, de overige afdelingen werken m.b.v. vastgesteld beleid, werkinstructies en Handboek Schulinck); • Een functionaris (steekproef RMO) stelt vast of de procedure wordt nageleefd en/ of het besluit in overeenstemming is met het intern en extern wettelijk kader; • Deugdelijke dossiervorming op basis van archiveringsrichtlijnen; • Het verstrekken van een uitkering vindt plaats op basis van authentieke documenten; • Alle toekenningen worden vastgelegd in de uitkeringenadministratie (Suite); • Periodiek vaststellen van de aansluiting tussen de financiële administratie en de uitkeringenadministratie. • Er vind maandelijks een IBAN controle plaats op de BO om te voorkomen dat uitkeringen naar de verkeerde bankrekeningen worden overgemaakt. • De SDD heeft een M&O-beleid.	SDD
Uitkeringen (hoogte)	Het risico dat bewust niet of niet alle gegevens van cliënten worden gecontroleerd en hierdoor te veel uitkeringen worden verstrekt		Hoog	• Er wordt gebruik gemaakt van standaardtabellen waarin de normbedragen van de uitkeringen zijn vastgelegd; • Wijziging van normbedragen is alleen mogelijk middels het toepassen van het 4-ogenprincipe. (BO kan wel mutaties doen die niet gecontroleerd worden. Er wordt jaarlijks afspraken gemaakt over steekproef controle op soort werkprocessen). Het systeem dwingt dit af; • Halfjaarlijks (bij bekendmaking van de nieuwe normbedragen) vindt er een interne controle (thema RMO) plaats, gericht op de juistheid van de normbedragen; • Er vindt interne controle plaats (steekproef RMO) op de toekenning van de juiste normvergoedingen aan de cliënten; • Er is een helder en eenduidig beleid vastgesteld ten aanzien van de hoogte van de uitkering.	SDD
Uitkeringen (dossier)	Het risico dat niet of niet alle gegevens van cliënten worden gecontroleerd en hierdoor te veel uitkeringen worden verstrekt.		Hoog	• Belangrijke cliëntgegevens worden gekopieerd ten behoeve van het dossier. (Alle aangeleverde documenten worden gescand in het digitale dossier); • De besluitvorming ten aanzien van de toekenning of continuering worden schriftelijk gemotiveerd in het cliëntdossier; • Een functionaris (steekproef RMO) stelt vast of de procedure wordt nageleefd en/ of het besluit in overeenstemming is met het intern en extern wettelijk kader; • Steekproefsgewijs worden cliëntdossiers integraal gecontroleerd.	SDD
Uitkeringen (uitstroom)	Het risico dat geen aandacht wordt besteed aan de uitstroom van cliënten en hierdoor te veel uitkeringen worden verstrekt.		Hoog	• Er is beleid geformuleerd ten aanzien van de uitstroom van cliënten; • Er is functiescheiding tussen de consulent die belast is met de uitstroombevordering en de functionaris die belast is met de controle op de rechtmatigheid van de te verstrekken uitkering. (afd. die de klantsignalen van het inlichtingenbureau behandeld).	SDD
Verstrekkingen (juiste persoon/ organisatie)	Het risico dat bewust: • ten onrechte voorzieningen worden verstrekt aan bestaande cliënten; • voorzieningen worden verstrekt aan niet bestaande cliënten; • te hoge vergoedingen worden verstrekt.	Het risico dat onjuiste of onvolledige informatie wordt verstrekt teneinde voor een verstrekking in aanmerking te komen. (medewerkers maken uitkeringen naar zichzelf over/aanmaken van fictieve uitkeringsgerechtigden)	Hoog	• Functiescheiding tussen het vaststellen van de verordening, behandelen van de aanvraag en dossiervorming, het besluiten op de aanvraag en voorstel tot betaling. (Zie ook Uitkering (Juiste persoon)); • Een functionaris stelt vast (steekproef RMO) of aan de bepalingen in de verordening is voldaan en of de juiste tarieven zijn toegepast; • Betaling vindt plaats op basis van een geautoriseerde beschikking BO doet zelf invoering en maken de beschikking n.a.v. rapport FO, daarnaast doen ze de vereenvoudigde aanvragen volledig zelf toekennen en invoeren en beschikking) (BO maakt begin van het jaar lijsten wat er collegiaal wordt gecontroleerd m.b.v. steekproef); • Periodieke aansluiting tussen uitkeringenadministratie en de financiële administratie.	SDD

Verstrekkingen (Peuterspeelzalen, Kinderopvang, maaltijden en zorgverzekering)	Het risico dat bewust onjuiste of onvolledige informatie wordt verstrekt teneinde voor een verstrekking in aanmerking te komen.		Hoog	• Jaarlijks steekproefsgewijs onderzoek op rechtmatigheid op kinderopvang en maaltijden door de BO; • Er wordt een steekproefcontrole uitgevoerd op alle de deelnemers aan de zorgverzekering die geen klant (meer) zijn. • RMO controleerd de controle van de BO.	SDD
Verstrekkingen (indicaties) intern	Het risico wordt gelopen dat er bewust onterecht indicaties worden afgegeven. Het risico wordt gelopen dat er bewust wordt verlengd zonder nader onderzoek		Hoog	• Functiescheiding tussen behandelen van de aanvraag en dossiervorming, het besluiten op de aanvraag en voorstel tot betaling. (Zie ook Uitkering (Juiste persoon)); • Een functionaris stelt vast (steekproef RMO) of aan de bepalingen in de verordening is voldaan en of de juiste tarieven zijn toegepast; • Betaling zorgverleners gaat via het Zorglokaal, Betaling PGB via SVB en vervoervergoeding via BO; • Periodieke aansluiting tussen uitkeringenadministratie en de financiële administratie.	SDD
Verstrekkingen (indicaties) Zorglokaal	Het risico wordt gelopen dat er een onrechtmatige verstrekking plaatsvindt doordat er geen zicht is op de financiële afhandeling door het Zorglokaal.		Hoog	• De accountantsverklaring wordt opgevraagd bij de leveranciers; • Met betrekking tot deze accountantsverklaring heeft afstemming plaatsgevonden tussen de accountants van de GRD/ SDD en het Zorglokaal; • Het Zorglokaal beschikt over de indicaties die door de SDD zijn afgegeven en gebruikt die bij de beoordeling; • Reactie van de klant bij financiële benadeling (piepsysteem); • Voorschotten worden periodiek verstrekt. Om de 4 weken krijgen we de realisatie en daarop worden voorschotten aangepast.	SDD
Verstrekkingen (HHT)	Het risico wordt gelopen dat er een onrechtmatige verstrekking plaatsvindt doordat er geen zicht is op de digitale aanvraag van de dienstencheque en de beoordeling hiervan door Zorglokaal.		Hoog	• De accountantsverklaring wordt opgevraagd bij Zorglokaal; • Met betrekking tot deze accountantsverklaring vindt afstemming plaats tussen de accountants van de SDD en Zorglokaal.	SDD
Treasury					
Betalingen BNG	Risico dat medewerkers in de BNG kunnen, terwijl dit niet nodig is. Risico dat er bedragen naar de medewerker zelf worden overgeboekt?		Hoog	Er is een autorisatiematrix voor de toegang tot de BNG (wordt bewaakt door FA SDD en treasury SGD). Controle technische functiescheiding bij betalingen: klaarzetten betaalstaat, controle van de betaalstaat, 1e en 2e betaler. Risico dat geconstaeerd is bij Drechtwerk, wordt in door de SGD uitgerold worden en zal de invoer van het hashtotaal in het 2e halfjaar van 2023 worden geactiveerd.	SDD/ SGD
Beheer netwerk/ automatisering					
Beheer netwerk/ automatisering (SDD-applicaties)	Het risico dat onbevoegden bewust toegang wordt verleend tot het netwerk en/ of applicaties en bewust (onjuiste) wijzigingen kunnen aanbrengen in het netwerk en/ of de applicaties.	Het risico dat derden onbevoegd toegang verkrijgen tot het netwerk, applicaties, gegevens van de gemeentes/ GRS.	Hoog	• Afsluitbare serverruimte bij SGD; • Beveiliging netwerk, beheer netwerk, gebruikers en wachtwoordbeheer (SGD); • Toegangsbeveiliging netwerk intern: periodiek vaststellen dat vertrokken personeel geen toegang meer heeft tot netwerk en applicaties (keycards inleveren, codes afmelden); • Toegangsbeveiliging netwerk extern: maatregelen die voorkomen dat via (externe) internetverbinding toegang kan worden verkregen met bedrijfsinformatie (open poort); • Logging van mislukte pogingen tot verkrijgen toegang tot systeem; • Rolgebaseerde bevoegdheden toewijzen voor (vereenvoudiging) beheer van bevoegdheden; • Op onbeheerde werkplekken (pauze, vergaderen etc.) schermbeveiliging met wachtwoord; • Er vindt jaarlijks een IT-audit plaats door BDO.	SDD/ SGD
Beheer netwerk/ automatisering	Het risico dat het netwerk/ applicaties voor onbevoegden toegankelijk is/ zijn en/ of dat onbevoegden wijzigingen aanbrengen in het netwerk en/ of applicaties.	Het risico dat derden onbevoegd toegang verkrijgen tot het netwerk, applicaties en/ of gegevens van SGD (en klanten).	Middel	Naast de interne beheersmaatregelen op in-, door- en uitstroom van personeel (IDU-proces) en het inrichten van controle op extern beheer op afstand (EBOA inclusief bijbehorende procedures) wordt door de accountant jaarlijks een IT-audit uitgevoerd. Dit is onderdeel van de managementletter. Per 1 maart 2018 is de volgende fase van het IDU-proces afgerond, met een eenduidig wijzigingsproces. Onderdeel daarvan is het ESS-MSS (Employee Self Service en Manager Self Service). Vanaf 2020 is het proces IDU geborgd in de organisatie met de koppeling van een proces eigenaar aan dit proces.	SGD
Archivering					
Archivering	Het risico dat stukken niet gedurende de wettelijke bewaartermijnen worden bewaard.		Laag	Er zijn duidelijke richtlijnen ten aanzien van archiveren opgesteld. Toezicht op de informatie- en archiefbeheer GRS is belegd bij de gemeentearchivaris van Dordrecht.	SGD

Drechtwerk/risico	Kans	impact	Conclusie		
Treasury					
Kas restaurant (incl. snoepautomaten)	ZW	L	Middel	Drechtwerk heeft een centrale kluis. Hiervoor zijn diverse beheersmaatregelen opgezet, zoals: De code van de kluis is bij slechts enkele medewerkers bekend en wordt periodiek gewijzigd, ook worden er, worden wekelijks kastellingen uitgevoerd, etc.(Onze doelgroep vereist dat contante betalingen in het restaurant noodzakelijk blijven). Vanuit de VIC wordt diverse malen per jaar meegekeken bij een kastelling.	DW
Hit-and-run BNG	OW	H	Middel	Binnen de betaalapplicatie van de BNG Bank wordt een 4-ogen principe (twee handtekeningen) afgedwongen waardoor er sprake is van controle-technische functiescheiding in het betaalproces. Enkel door middel van samenspanning kunnen middelen onrechtmatig de organisatie verlaten. Daarnaast is tevens sprake van betaallimieten waardoor dit risico enigszins beperkt wordt. De bank monitort verder ongebruikelijk betaalmomenten en bedragen, echter het is niet duidelijk in hoeverre de BNG Bank tijdig signaleert. Vanuit de VIC vinden jaarlijks controles plaats op juistheid van de ingevoerde procuratiehouders. Ook wordt het intern mandaatbeleid jaarlijks tegen het licht gehouden en gecontroleerd met de bankbevoegdheden.	DW
Spoedbetalingen/ handmatige betalingen	ZW	L	Middel	Binnen de betaalapplicatie van de BNG Bank wordt een 4-ogen principe (twee handtekeningen) afgedwongen waardoor er sprake is van controle-technische functiescheiding in het betaalproces. Enkel door middel van samenspanning kunnen middelen onrechtmatig de organisatie verlaten. Daarnaast is tevens sprake van betaallimieten waardoor dit risico enigszins beperkt wordt. De bank monitort ongebruikelijk betaalmomenten en bedragen, echter het is niet duidelijk in hoeverre de BNG Bank tijdig signaleert. Vanuit de VIC vinden jaarlijks controles plaats op juistheid van de ingevoerde procuratiehouders. Ook wordt het intern mandaatbeleid jaarlijks tegen het licht gehouden en gecontroleerd met de bankbevoegdheden.	DW
Betaalbestanden wijzigen(Betalingen)	W	H	Hoog	De betaalbestanden worden in XML formaat op de server opgeslagen voordat deze in de BNG applicatie geüpload worden. Bij het uploaden dwingt de BNG applicatie sinds de samenvoeging met de GR Sociaal geen invoer van een hashtotaal af. Risico op onrechtmatige wijziging van betaalbestanden (XML) is derhalve onvoldoende gemitigeerd. In overleg met de GRS zal de invoer van het hashtotaal in het 2e halfjaar van 2023 weer worden geactiveerd. Vanuit de VIC worden (nog) geen aanvullende controles uitgevoerd.	DW
IT					
Crediteurenstamgegevens (bankrekeningnummers)(IT)	W	M	Middel	Logging van de mutaties in crediteurenstamgegevens vindt plaats in I-Count. Daarnaast wordt brondocumentatie met betrekking tot bankrekeningwijzigingen hard-copy gearchiveerd. Vanuit de VIC wordt een controle uitgevoerd op de digitale logging van crediteurenstamgegevens. Aan de hand van deze logging worden de nodige verdiepingswerkzaamheden uitgevoerd zoals aansluiting naar het brondocument. In 2023 gebeuren deze controles integraal.	DW
IT ransomware	ZW	H	Significant	Medewerkers worden getraind om signalen van ransomware op te pakken. Daarnaast worden laptops zoveel mogelijk dichtgezet en is het inloggen in de Drechtwerk-omgeving via privélaptops op termijn niet meer toegestaan. Vanuit de VIC worden (nog) geen aanvullende controles uitgevoerd.	DW
Detacheringen					

Uren inleners (omzet detacheringen)	W	H	Hoog	Enkele bedrijven waar personeel is gedetacheerd vullen zelf uren in in het urenregistratie systeem van Drechtwerk. Risico is dat er onjuiste registratie plaatsvindt van de productieve uren. Om dit risico te verkleinen is er een koppeling met het verlofsaldo van de medewerker. Het maximale risico blijft hierbij beperkt tot de volledige uitnutting van het verlof. Verlofopname wordt daarnaast ook gemonitord. Bedrijven hebben enkel rechten om uren in te voeren. Daarnaast geldt dat medewerkers een signaleringsfunctie hebben indien verlofsaldo of ziekteverzuim dagen niet kloppen. Vanuit de VIC worden (nog) geen aanvullende controles uitgevoerd. Wel blijft de VIC betrokken bij gesprekken over eventuele aanpassingen in de processen.	DW
Te lage tarieven detacheren(omzet detacheringen)	OW	H	Middel	Jaarlijks vinden indexeringen van tarieven plaats. Daarnaast worden tarieven up-to-date gehouden via loonwaardemetingen. Facturatie vindt plaats in functiescheiding (contractbeheerder, contracteigenaar en planning en control). Vanuit de VIC worden er factuurcontroles verricht op de juistheid van de tarieven.	DW
Personeelskosten					
Dead man on the payroll	W	M	Middel	Er is sprake van controle-technische functiescheiding tussen P&O en SA. Echter deze kan door beperkingen in de IT omgeving doorbroken worden. Er worden maandelijks bezettingsoverzichten gedeeld binnen de organisatie, echter niet met alle budgethouders c.q. afdelingshoofden. Daarnaast wordt ten aanzien van de lonen en salarissen niet op budget gestuurd. Detailcontroles op mutaties kan het risico grotendeels ondervangen. Vanuit de VIC worden controles uitgevoerd op in- en uitdienst mutaties en bijbehorende personeelsdossiers. Daarnaast worden de bankmutaties in het personeelssysteem maandelijks integraal gecontroleerd op juistheid.	DW
Inkoop					
Fictieve facturen (inkoop)	ZW	L	Middel	Alle facturen doorlopen het webgoedkeuren en landen op een budget. Afhankelijk van de ingeregelde mandaten worden de facturen door één of twee budgethouders geautoriseerd. Inkoopfacturen voor specifieke afdelingen waarbij 'slechts' één budgethouder tekent is mogelijk een 'blinde vlek'. Onderscheid tussen contracteigenaar versus contractbeheerder is van belang om proces optimaal in te richten. Vanuit de VIC wordt actief gestuurd op het up to date houden van het contractregister en het juist aanbrengen van onderscheid tussen contractbeheerder en contracteigenaar. Tevens vinden controles op inkoopfacturen plaats waarbij de factuur aangesloten wordt op offerte/orderbevestiging en pakbon/urenbriefje e.d.	DW
Kick backs inkopen (inkoop)	W	M	Middel	Drechtwerk heeft een Inkoop- en aanbestedingsbeleid en een mandaatregeling ingericht om dit risico te voorkomen. Daartussen blijft dit risico bestaan. Vanuit de VIC vinden separate analyses plaats op (potentiële) aanbestedingen. Hierbij wordt tevens gecontroleerd of het mandaatbeleid wordt nageleefd.	DW