

Frauderisicoanalyse

(versie oktober 2024)

Naam activiteit/proces	Risicodefinitie fraude	Kans (waarschijnlijkheid)	Beheersmaatregelen
Opbrengsten			
Alle opbrengsten	Het risico dat deze opbrengsten niet worden geïnd op een IBAN-rekeningnummer van SSC DeSom en hierdoor geld aan SSC DeSom wordt onttrokken.	Laag	- Digitale facturen/briefpapier met hierop het IBAN-rekeningnummer van SSC DeSom; - Controle op openstaande debiteuren; - Controle op juistheid, tijdigheid en volledigheid van factureren.
Lonen en salarissen			
Personeels- en salarisadministratie	Het risico dat in de personeels- en salarisadministratie personen zijn opgenomen die niet in dienst zijn.	Laag	- Personeels- en salarisadministratie wordt door SSC DeSom zelf uitgevoerd; - Invoer van nieuwe medewerkers kan alleen op basis van een onderliggend persoonsdossier met daarin een door de directeur ondertekend aanstellingsbesluit; - Bij SSC DeSom is sprake van functiescheiding tussen invoer (P&O) en controle (salarisadministratie).
	Het risico dat personeelsleden een hogere beloning en/of hogere (variabele) emolumenten krijgen, daar waar zij op grond van hun functie en/of prestatie recht op hebben.	Laag	- Controle wordt uitgevoerd door de personeels- en salarisadministratie van SSC DeSom.
Onkostenvergoedingen	Het risico dat niet-gemaakte kosten worden gedeclareerd en/of het risico dat privé-uitgaven worden gedeclareerd.	Laag	- Declaraties worden akkoord gegeven en betaald via AFAS Insite (bewijs moet worden toegevoegd) of gaat via declaratie in Key2Finance waarbij budgethouder akkoord geeft, er zit altijd een controle op.
Inkopen/aanbestedingen			
Inkopen/aanbestedingen	Het risico dat valse facturen door ambtenaren worden ingediend (facturen zonder tegenprestatie).	Laag	- Functiescheiding tussen inkoop, budgethouder, registratie facturen en betaling facturen; - Alleen originele facturen worden verwerkt; - Bij nieuwe crediteuren raadpleegt medewerker Administratie en Contractbeheer de Kamer van Koophandel; - Iedere factuur wordt minimaal volgens het vierogenprincipe goedgekeurd; - Controle levering in Topdesk.
	Het risico dat privé-uitgaven ten laste van de organisatie worden gebracht.	Laag	- Alleen op de SSC DeSom te naam gestelde facturen worden verwerkt; - Iedere factuur wordt minimaal volgens het vierogenprincipe goedgekeurd.
	Het risico dat de Europese en/of interne aanbestedingsrichtlijnen niet worden nageleefd.	Gemiddeld	- Inkoop- en aanbestedingsbeleid SSC DeSom; - Opnemen in interne controle.
Belastingen en sociale premies			
Loonheffing en sociale lasten, omzetbelasting en vennootschapsbelasting	Het risico dat aangiften niet juist, tijdig en/of volledig worden ingediend en betaald.	Laag	- Afdrachten loonheffing en sociale lasten worden berekend door Simplex en vervolgens gecontroleerd en afgedragen door SSC DeSom; - Omzetbelasting per kwartaal aan de hand van een export uit Kredietbewaking; - Vennootschapsbelasting per jaar aan de hand van een export uit Kredietbewaking.
	Het risico dat onrechtmatige fiscale constructies worden opgezet.	Laag	- Betrokkenheid bestuur.

Naam activiteit/proces	Risicodefinitie fraude	Kans (waarschijnlijkheid)	Beheersmaatregelen
Liquide middelen			
Betalingsverkeer	Het risico dat op onrechtmatige wijze gelden aan de IBAN-rekeningnummers worden onttrokken.	Laag	- Screening medewerkers (VOG-verklaring); - Tweehandtekeningenstelsel; - Bij afwezigheid is er adequate vervanging aanwezig; - Functiescheiding tussen klaarzetten betaling en de feitelijke betaling (2e handtekening); - Aansluiting banksaldo op bankafschrift en controle op dagboekmutaties; - Interne controle.
Crediteuren			
Beheer crediteuren	Het risico dat informatie in het crediteurenstambestand niet betrouwbaar en niet juist is.	Laag	- Autorisatie bankrekening door tweede persoon.
Leningen			
Aantrekken van geldleningen	Het risico dat het aantrekken van leningen niet onafhankelijk plaatsvindt.	Gemiddeld	- Procedure offerteaanvraag vastleggen (altijd meerdere); - Overzicht leningen; - Functiescheiding tussen aanvrager en beslisser.
Tussenrekeningen/memoriaalboekingen			
Tussenrekeningen	Het risico dat onrechtmatige handelingen door het oneigenlijk gebruik van tussenrekeningen wordt gemaskeerd.	Laag	- Gebruik tussenrekeningen wordt zoveel mogelijk beperkt; - Periodiek specificatie van tussenrekeningen.
Memoriaalboekingen	Het risico dat memoriaalboekingen niet juist, tijdig en volledig zijn geautoriseerd en verwerkt, waardoor het identificeren van afwijkingen wordt bemoeilijkt.	Gemiddeld	- Gebruik memoriaalboekingen is beperkt; - Periodiek controle op memoriaalboekingen.
Verslaggeving			
Rapportering	Het risico dat in de verslaggeving of budgetten (extern en intern) bewust aanpassingen plaatsvinden om prestatiecijfers, afrekeningen et cetera te beïnvloeden.	Laag	- Aansluiting met grootboek; - Analyse van afwijkingen ten opzichte van budgetten; - Vaststelling door bestuur.
Reserves	Het niet inzichtelijk maken van de beklemming van de reserves, waardoor een grotere bestedingsruimte aanwezig lijkt dan in werkelijkheid het geval is.	Laag	- Functiescheiding tussen besluitvorming en administratieve verwerking; - Gebruik reserves is beperkt.
Beheer netwerk/automatisering			
Beheer netwerk/automatisering	Het risico dat het netwerk/applicaties voor onbevoegden toegankelijk is en/of dat onbevoegden wijzigingen aanbrengen in het netwerk en/of de applicaties.	Gemiddeld	- Servers van SSC DeSom zijn ondergebracht in professionele datacenters met een streng beveiligingsregime met bijbehorende maatregelen, alleen geautoriseerd personeel krijgt onder strenge voorwaarden toegang tot deze locaties en daarnaast staan de servers van SSC DeSom in apart beveiligde, afgesloten kasten; - Beveiliging netwerk, beheer netwerk, gebruikers en wachtwoordbeheer; - Inleveren keycards, afmelden gebruiker bij vertrek personeel; - Op onbeheerde werkplek vergrendelen werkplek en schermbeveiling met wachtwoord.
Pishing/skimming	Het risico van phishing/skimming naar gegevens/betaling van SSC DeSom.	Gemiddeld	- Betreft externe fraude; - Bewustwording creëren in de organisatie; - Antivirus en firewall up to date.

Naam activiteit/proces	Risicodefinitie fraude	Kans (waarschijnlijkheid)	Beheersmaatregelen
Archivering			
Archivering	Het risico dat (belangrijke) stukken niet gedurende de wettelijke bewaartermijnen worden bewaard.	Gemiddeld	- Facturen zijn digitaal gekoppeld aan Key2Finance; - Duidelijke richtlijnen ten aanzien van het archiveringsproces; - Zaaksysteem.
	Het risico dat belangrijke en/of vertrouwelijke informatie uit het archief niet vertrouwelijk wordt behandeld.	Gemiddeld	- Toegang zaaksysteem door middel van inlogcodes.
Nevenwerkzaamheden			
Nevenwerkzaamheden	Het risico dat als gevolg van nevenwerkzaamheden de werkzaamheden als ambtenaar/bestuurder niet onafhankelijk plaatsvinden.	Gemiddeld	- Inzicht in nevenfuncties van sleutelfunctionarissen.
Integriteit			
Oneigenlijk gebruik	Het risico dat een medewerker oneigenlijk gebruik maakt van faciliteiten van SSC DeSom zoals printers, papier, auto's, et cetera.	Gemiddeld	- Personeelshandboek SSC DeSom.
Inzet medewerkers privé	Het risico dat werkzaamheden door medewerkers van SSC DeSom worden verricht voor privé situaties in werktijd van SSC DeSom.	Gemiddeld	- Personeelshandboek SSC DeSom.
Verkoop uit dienst genomen goederen	Het risico dat uit dienst genomen goederen van waarde heimelijk worden verkocht.	Gemiddeld	- Inventariseren van binnenkomende goederen van waarde en deze volgen tot vernietiging of verkoop aan derden.
Ophalen nieuw bestelde goederen	Het risico dat nieuw bestelde goederen door 'de verkeerde' derden worden opgehaald.	Laag	- Tekenen voor ontvangst (bruikleenovereenkomst).