

Managementletter 2025

Veiligheidsregio Zuid-Limburg

12 december 2025

Het dagelijks bestuur van
Veiligheidsregio Zuid-Limburg
Holstraat 35
6269 AW Margraten

Heerlen, 12 december 2025

Betreft: managementletter 2025

Geachte leden van het dagelijks bestuur,

Het algemeen bestuur heeft ons opdracht gegeven de jaarrekening 2025 van Veiligheidsregio Zuid-Limburg te controleren. Als onderdeel van de jaarrekeningcontrole hebben wij procescontroles uitgevoerd. Onze belangrijkste bevindingen voortvloeiend uit deze procescontroles vindt u in de managementletter bij deze brief.

Reikwijdte managementletter

De procescontroles zijn gericht op de analyse en evaluatie van de interne beheersingsomgeving en de daarin opgenomen maatregelen van interne controle voor zover relevant voor de jaarrekeningcontrole. Wij benadrukken dat onze uitgevoerde werkzaamheden niet als doel hebben om een oordeel uit te spreken over de effectiviteit van de interne beheersing van uw organisatie. De bevindingen van deze procescontroles zijn bedoeld als kritische, constructieve aanwijzingen voor het dagelijks bestuur als onderdeel van het continue proces van het verbeteren en veranderen van de beheersing van de bedrijfsvoering en de kwaliteit van de financiële verslaggeving. De vele goed georganiseerde activiteiten en processen binnen uw organisatie worden derhalve niet benoemd, hetgeen niet betekent dat deze onopgemerkt zijn gebleven. De managementletter dient dan ook gelezen te worden voornoemde in acht nemend.

Indeling managementletter

Deze managementletter is ingedeeld in drie onderdelen. Als eerste gaan wij in op actuele externe ontwikkelingen waarvan wij het belangrijk vinden dat uw organisatie kennisneemt. Vervolgens presenteren wij in samengevatte vorm de bevindingen uit voorgaand jaar, waarbij primair wordt aangegeven in hoeverre deze bevindingen inmiddels zijn opgevolgd. Als derde onderdeel delen wij onze aanbevelingen voortvloeiend uit de procescontroles huidig jaar, waarbij elke bevinding op een schaal van hoog naar laag wordt geprioriteerd.

Disclaimer

Deze managementletter is uitsluitend opgesteld voor het dagelijks bestuur van Veiligheidsregio Zuid-Limburg en mag derhalve zonder onze uitdrukkelijke toestemming vooraf niet aan derden verstrekt worden. Als gevolg hiervan accepteren wij geen aansprakelijkheid of verantwoordelijkheid tegenover enige andere persoon die dit verslag in handen of ter inzage krijgt.



Tot slot

Tot slot willen wij van de gelegenheid gebruik maken uw medewerkers te bedanken voor de constructieve samenwerking. Wij vertrouwen erop u hiermee van dienst te zijn geweest. Mocht u op enig moment nog nadere vragen hebben over de inhoud van deze managementletter, kunt u uiteraard contact met ons opnemen.

Met vriendelijke groet,

RSM Netherlands Accountants N.V.

Digitaal ondertekend door:

Stefan Prevoo
12 december 2025 13:28 +01:00

drs. S.J.M. Prevoo RA

Agenda

Externe ontwikkelingen	5
Opvolging bevindingen voorgaande rapportage	10
Bevindingen huidig jaar	13

1. Externe ontwikkelingen

Toelichting externe ontwikkelingen

Onderstaand hebben wij een aantal actuele ontwikkelingen beschreven die wij voor uw organisatie van belang achten om kennis van te nemen.



Vanaf 17 april 2025 gelden de geactualiseerde versie van het BBV en Bado. Tevens is in het najaar van 2025 Kadernota Rechtmatigheid van de Commissie BBV geactualiseerd. De hiervoor genoemd geactualiseerde regelgeving en kadernota leiden tot een aantal wijzigingen die van invloed zijn op uw organisatie. Voor uw inzicht hebben wij de belangrijkste wijzigingen onderstaand voor u samengevat.

Onderwerp	Tot en met 2024	Vanaf 2025
Goedkeuringstolerantie	Maximaal 1% voor fouten en 3% voor onzekerheden	Maximaal 2% voor fouten en onzekerheden gezamenlijk.
Rechtmatigheidsverantwoording	Vrijwillige toelichting in de jaarrekening.	Een verplicht hoofdoverzicht in de jaarrekening
Verantwoordingsgrens in rechtmatigheidsverantwoording	Grensbedrag bedraagt maximaal 3%	Grensbedrag bedraagt maximaal 2%
Omvangsbasis voor de goedkeuringstolerantie en de verantwoordingsgrens	Totale lasten, <u>inclusief</u> toevoegingen aan reserves	Totale lasten, <u>exclusief</u> toevoegingen aan reserves

In aanvulling op bovenstaande wijzigingen is naar aanleiding van de Wet open overheid (Woo) een verplichting toegevoegd om een openbaarheidsparagraaf op te nemen in begrotingen en jaarrekeningen. Deze paragraaf moet inzicht geven in hoe de organisatie invulling geeft aan transparantie en openbaarheid van bestuur.

Tevens wordt volgens het gewijzigde artikel 24 lid 3 van het BBV de sectie "Overige gegevens" een verplicht onderdeel van de jaarrekening. Deze sectie bevat onder andere de accountantsverklaring.



Geïntegreerde aanpak NIS2 en BIO2.0

Publieke organisaties staan voor de uitdaging om te voldoen aan zowel de Europese NIS2-richtlijn als het vernieuwde nationale normenkader BIO2.0. Beide kaders zijn gebaseerd op een risicogebaseerde aanpak en sluiten aan op de ISO 27001/27002:2022-normen. BIO2.0 vervangt de eerdere compliance-gebaseerde benadering door een dynamisch risicomanagementsysteem (ISMS) en is sinds september 2025 vastgesteld, terwijl NIS2 (cyberbeveiligingswet) aanvullende eisen stelt zoals meldplicht, zorgplicht, toeleveranciersbeheer (toezicht) en bestuurlijke verantwoordelijkheid.

Wij onderkennen een verhoogd risico op fragmentatie van inspanningen, inefficiëntie en inconsistenties, indien NIS2 en BIO2.0 los van elkaar worden geïmplementeerd, hetgeen kan leiden tot:

- Dubbele audits en rapportages;
- Onvoldoende afstemming van risicobeoordelingen;
- Onvolledige dekking van toeleveranciers in het beveiligingsbeleid;
- Verhoogde kans op non-compliance bij incidenten of toezicht;
- Verschillende invalshoeken met afwijkende inschattingen.

Wij adviseren het management om een geïntegreerde aanpak te hanteren voor de implementatie van NIS2 en BIO2.0. Hierbij zijn de volgende stappen van belang.

- Voer een gezamenlijke nulmeting op basis van beide kaders uit waarbij overlap tussen beide kaders wordt geïdentificeerd.
- Start met een risicogerichte benadering, waarbij de belangrijkste risico's in kaart worden gebracht.
- Heb aandacht voor uitbestede diensten en neem het voortouw richting leveranciers.
- Richt één ISMS in dat voldoet aan de eisen van zowel BIO2.0 als NIS2, inclusief meldprocedures en leveranciersclassificatie.
- Stel een multidisciplinair projectteam aan dat verantwoordelijk is voor de coördinatie van beide trajecten.
- Gebruik bestaande BIO-compliance als het fundament voor NIS2-verplichtingen, zoals risicobeoordeling en awareness-trainingen.
- Betrek bestuurders actief via gerichte opleidingen over hun rol en aansprakelijkheid onder NIS2.
- Houd er rekening mee dat zodra de Cyberbeveiligingswet is vastgesteld, deze direct in werking treedt en u hieraan dient te voldoen.

Door NIS2 en BIO2.0 als één samenhangend geheel te benaderen, kan de organisatie haar digitale weerbaarheid versterken, voldoen aan wettelijke verplichtingen en tegelijkertijd kosten en tijd besparen alsook inconsistenties voorkomen. Dit vereist strategische sturing en een bestuurlijke betrokkenheid.

Impact van duurzaamheid op financiering

In eerdere rapportages hebben wij actualiteiten gemeld op het gebied van duurzaamheidsverslaggeving, onder meer aan de hand van de Handreiking duurzaamheidsrapportage en -verantwoording van de zogeheten 'Coalition of the Willing'.

BNG Bank heeft sinds 2022 een eigen klimaatplan, "Going Green", waarin doelstellingen zijn opgenomen ten aanzien van hoe de bank bijdraagt aan de reductie van CO₂-emissies, zoals overeengekomen in het Klimaatakkoord van Parijs. In de afgelopen jaren hield de BNG Bank al rekening met de CO₂-emissie als gevolg van haar kredietverlening.

Met ingang van 2025 heeft BNG Bank meer aandacht voor de verduurzamingsstrategieën en -doelstellingen van haar klanten en of deze in lijn zijn met het Klimaatakkoord van Parijs. Wij geven in overweging om duurzaamheid een grotere rol te laten spelen binnen de strategie van uw organisatie.



Btw over pensioenpremies

Er speelt momenteel een discussie over btw-heffing op pensioenpremies naar aanleiding van recente uitspraken van het Gerechtshof Arnhem-Leeuwarden, waarbij het Hof heeft geoordeeld dat de dienstverlening van bedrijfstakpensioenfondsen aan werkgevers niet onder de btw-vrijstelling voor verzekeringen valt, omdat het uitvoeren van de pensioenregeling een dienst betreft die btw-belast is.

De achtergrond van deze discussie is gelegen in het feit dat voor de btw-vrijstelling voor verzekeringen geldt dat premiebetaling een voorwaarde moet zijn voor het recht op uitkering. Bij pensioenregelingen is dat niet het geval. Een werknemer behoudt recht op pensioen, ook als de werkgever de premie niet betaalt. Dit betekent dat het directe verband tussen premie en uitkering ontbreekt met als gevolg dat over de volledige pensioenpremie (niet alleen de uitvoeringskosten) 21% btw verschuldigd zou zijn. Volledigheidshalve merken wij op dat in afwachting van het mogelijke cassatieverzoek van pensioenfondsen vooralsnog geen actie hoeft te worden ondernomen.

Voor overheidsinstellingen kan dit tot een directe lastenverzwaring leiden, wanneer zij deze btw niet kunnen verrekenen.

In het nieuwe stelsel van de Wet toekomst pensioenen (Wtp) is de dienstverlening van pensioenuitvoerders en vermogensbeheerders (grotendeels) vrijgesteld van de heffing van btw.

2. Opvolging bevindingen voorgaande rapportage

Opvolging bevindingen voorgaande rapportage

Als regulier onderdeel van onze procescontroles besteden wij aandacht aan de interne opvolging van de door ons in de voorgaande rapportage gedeelde bevindingen. In algemene zin bevelen wij aan een continue verbetering van de administratieve organisatie en interne beheersing te bewerkstelligen. Onderstaande bevindingen zijn aangedragen met het oog op het faciliteren van een dergelijke verdere verbetering van uw interne organisatie. Voor de volledige weergave van de bevindingen van vorig jaar verwijzen wij naar de bijlagen. In onderstaand voorbeeld staat *V* voor de prioritering van vorig jaar en *H* voor de prioritering die het punt in huidig jaar heeft, rekening houdend met de ondernomen acties. In het geval dat een bevinding uit voorgaande rapportage is opgevolgd, is geen prioritering voor huidig jaar gepresenteerd.

Voor zover bevindingen uit voorgaande rapportage niet of deels zijn opgevolgd, hebben wij de betreffende bevindingen van voorgaand jaar, inclusief het managementcommentaar, opgenomen in de bijlage bij deze managementletter.

Bevindingen in voorgaande rapportage		Prioritering		Mate van opvolging in huidig jaar	
Wachtwoordbeleid netwerk en applicaties					
De bevinding ten aanzien van de applicatie Motion is vanwege de migratie naar een nieuwe applicatie niet meer van toepassing. Het instellen van MFA is in opzet ingericht voor de organisatie. Echter constateren wij dat MFA nog niet is ingesteld voor alle gebruikersaccounts.		HOOG V LAAG H		Deels opgevolgd	
Regievoering op uitbestede IT-diensten					
Wij hebben vernomen dat nog niet concreet wordt geëvalueerd of door IT-leveranciers aan de geldende afspraken en voorwaarden wordt voldaan, bijvoorbeeld aan de hand van Service Level Reports. Vanwege het toenemende belang van functioneel applicatiebeheer en leveranciersmanagement, onder meer door toenemende eisen vanuit de regelgeving, hebben wij de prioritering voor huidig jaar verhoogd.		HOOG H LAAG V		Niet opgevolgd	
Controle inkooprechtmatigheid					
De controle inkooprechtmatigheid is in 2025 zodanig ingericht dat de daadwerkelijke lasten voor de afgelopen 4 jaren worden betrokken in de beoordeling die door de organisatie wordt uitgevoerd.		HOOG LAAG V		Opgevolgd	

Jubileumuitkering personeelsproces

Bij de uitvoering van onze werkzaamheden ten aanzien van het personeelsproces is geen dergelijke bevinding gedaan in 2025.



Opgevolgd

Actualisatie financiële verordening en mandaatregeling

In 2025 is onder andere de financiële verordening geactualiseerd. De financiële verordening wordt vastgesteld in de vergadering van het algemeen bestuur op 5 december 2025 en treedt met terugwerkende kracht in werking op 1 januari 2025. Omdat de regelgeving pas in de loop van 2025 is geactualiseerd, is het vooraf wijzigen en vaststellen van de financiële verordening niet mogelijk geweest. Deze bevinding is derhalve als opgevolgd geclassificeerd.



Opgevolgd

Sturend karakter controle inkooprechtmatigheid

De controle inkooprechtmatigheid kent vanaf 2025 een sturend karakter. Bij de beoordeling van de lasten per crediteur per opdracht worden aanvullend de verwachte lasten voor de komende 2 jaren inzichtelijk gemaakt. Hierdoor komen mogelijke toekomstige overschrijdingen tijdig aan het licht, en kan tijdig een nieuwe aanbesteding worden gestart. Deze bevinding is derhalve opgevolgd.



Opgevolgd

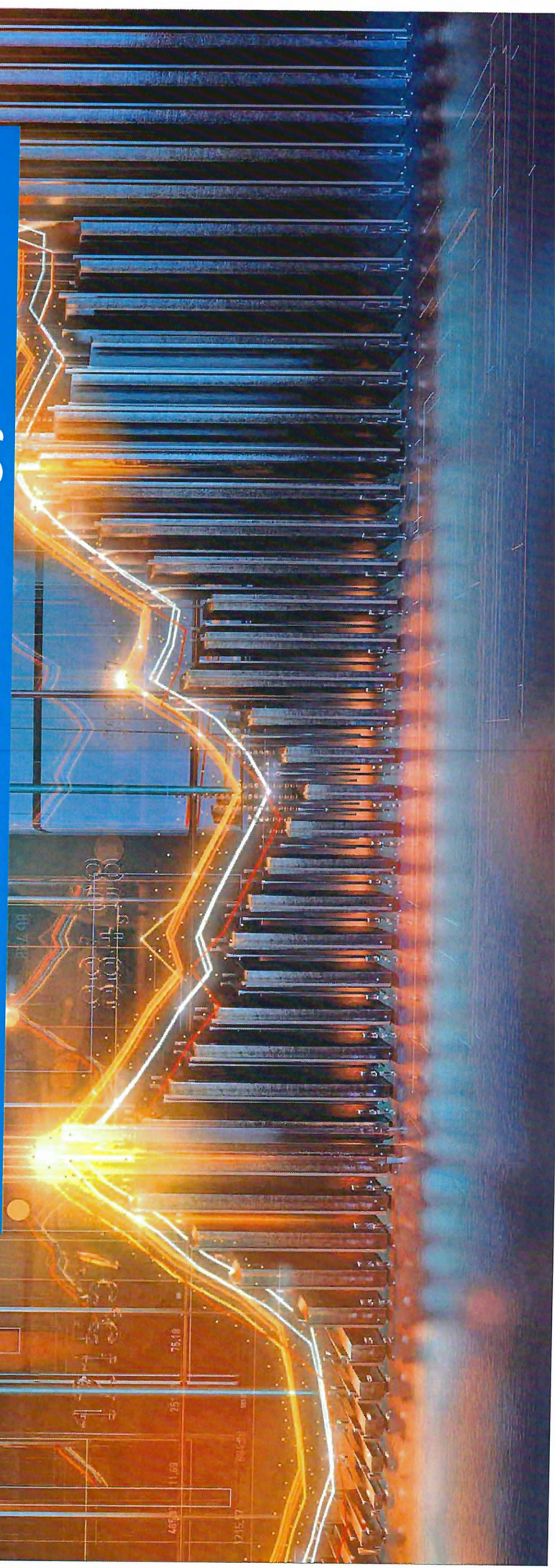
Bezwaartermijn gunning aanbestedingen

Vanuit interne afwegingen binnen Veiligheidsregio Zuid-Limburg wordt het niet noodzakelijk geacht om bezwaartermijnen op te nemen in de gunningsbrief. Deze interne afwegingen zijn ook voorgaand jaar in het managementcommentaar, zoals in de bijlage opgenomen, vervat.



Niet opgevolgd

3. Bevindingen huidig jaar



Bevindingen huidig jaar

Regievoering op uitbestede IT-diensten applicaties

Vorig jaar hebben wij geconstateerd dat het functioneel beheer voor de gehanteerde applicaties binnen de gebruikersgroep van de betreffende applicatie is belegd, waarbij het functioneel beheer zich met name op het gebruikersbeheer richt. De noodzaak van onze bevinding uit de voorgaande rapportage wordt naar wij begrijpen door Veiligheidsregio Zuid-Limburg onderschreven. Wij constateren dat de regievoering op uitbestede IT-diensten nog versterking behoeft ten aanzien van de regievoering door functioneel applicatiebeheerders op leveranciers.

De aankomende Cyberbeveiligingswet (Cbw), die de Europese NIS2-richtlijn implementeert, legt organisaties een expliciete zorgplicht op voor de beveiliging van hun netwerk- en informatiesystemen. Deze zorgplicht strekt zich niet enkel uit binnen de eigen organisatie, maar omvat ook de toeleveringsketen. Organisaties moeten aantoonbaar grip hebben op de risico's die ontstaan door uitbesteding en afhankelijkheden van leveranciers. Dit betekent dat leveranciersmanagement een cruciaal onderdeel vormt van de naleving van het beheer van applicaties, zodat eventuele kwetsbaarheden tijdig opgemerkt worden.

Een cyberincident bij een leverancier kan directe gevolgen hebben voor de continuïteit van de processen, de beschikbaarheid van systemen en de bescherming van persoonsgegevens. De Cbw vereist daarom dat organisaties:

- Leveranciers structureel beoordelen en monitoren op hun cybersecuritymaatregelen;
- Passende eisen opnemen in contracten, zoals beveiligingsstandaarden, incidentmeldingsplichten en auditrechten;
- Risicoanalyses uitvoeren op uitbestede processen en digitale koppelingen;
- Documentatie en aantoonbaarheid van deze maatregelen borgen voor toezicht en verantwoording.

Het niet naleven van deze verplichtingen kan leiden tot sancties, reputatieschade en verhoogde kans op datalekken of verstoringen. Wij adviseren om leveranciersmanagement als onderdeel van het functioneel beheer van applicaties concreter vorm te geven, daar dit een essentieel onderdeel van risicobeheersing en continuïteitsborging betreft.

**Bevinding, risico en
aanbeveling**

Prioriteit

Managementcommentaar

HOOG

LAAG

We erkennen dat de regie op onze IT-diensten nog versterking nodig heeft. De functie voor functioneel beheer is opgenomen in de formatie voor 2026, waarmee we dit structureel willen borgen.

Formaliseren van afspraken netwerkbeheer

Bevinding, risico en aanbeveling

In 2025 heeft een migratie van de netwerkgeving plaatsgevonden, waarbij de netwerkgeving niet langer volledig wordt beheerd door Solido. Na de migratie zal een deel van het beheer door Veiligheidsregio Zuid-Limburg zelf worden uitgevoerd. Wij hebben vernomen dat nog geen concrete afspraken zijn gemaakt welke partij verantwoordelijk is voor welke beheertaken. Momenteel geldt nog een overeenkomst uit 2016, die verouderd is en niet meer de volledige en huidige situatie dekt. Het ontbreken van actuele en formeel vastgelegde afspraken over verantwoordelijkheden en beheer van de netwerkgeving vergroot het risico op onduidelijkheid bij incidenten, onvoldoende (preventieve) beveiligingsmaatregelen en niet-naleving van wettelijke verplichtingen (zoals continuïteits- en beveiligingsnormen). Dit kan leiden tot vertragingen bij calamiteiten, verhoogde kwetsbaarheid voor cyberrisico's en mogelijke aansprakelijkheidskwesties.

Wij adviseren om de afspraken omtrent het beheer van de netwerkgeving op korte termijn te formaliseren in een geactualiseerde overeenkomst. In deze overeenkomst dienen de bevoegdheden, verantwoordelijkheden, taken van Veiligheidsregio Zuid-Limburg en Solido, alsmede het gewenste service level concreet te zijn beschreven ter borging van adequaat netwerkbeheer.

Prioriteit

HOOG

LAAG

Managementcommentaar

De huidige afspraken over het netwerkbeheer sluiten niet meer aan bij de situatie na de migratie. Dit jaar worden de verantwoordelijkheden, taken en servicelevels tussen VRZL en Solido formeel vastgelegd in een geactualiseerde overeenkomst. Hiermee wordt duidelijkheid en continuïteit in het netwerkbeheer geborgd.

Tijdige blokkade van gebruikersaccounts uitdiensttreders AFAS en AG5

Bevinding, risico en aanbeveling

Binnen de applicaties AFAS en AG5 worden de rechten van een uit dienst tredende medewerker geblokkeerd vanaf de ingevoerde uitdiensttredingsdatum. Wij hebben echter geconstateerd dat voor drie medewerkers in de applicatie AFAS de gebruikersrechten niet tijdig na uitdiensttreden zijn geblokkeerd. Voorts hebben wij voor drie andere medewerkers vastgesteld dat de gebruikersrechten in de applicatie AG5 niet tijdig zijn geblokkeerd na uitdiensttreding. Vorenstaande wordt veroorzaakt door het feit dat de ingerichte systeemtechnische blokkade niet heeft gefunctioneerd.

Het niet tijdig blokkeren van gebruikersaccounts van uit dienst getreden medewerkers leidt tot mogelijke onrechtmatige toegang tot de applicatie en vertrouwelijke gegevens. Tevens hebben wij vernomen dat geen periodieke controle wordt uitgevoerd op de juiste en tijdige blokkering van accounts van uitdiensttreders, waardoor geen sprake is van een repressieve controle op dergelijke uitval.

Volledigheidshalve vermelden wij dat de betreffende gebruikersaccountants direct na onze constatering alsnog door de organisatie zijn geblokkeerd. Voorts hebben is onze constatering ten aanzien van de systeemtechnische blokkade in AG5 is opgevolgd, waarbij naar wij begrijpen een structurele oplossing is gevonden in de vorm van het direct deactiveren accounts per uitdiensttredingsdatum.

Wij bevelen aan om periodiek een controle uit te voeren waarbij de lijst van actieve gebruikers wordt aangesloten met de medewerkers met een actief dienstverband c.q. actieve inhuur. Tevens adviseren wij om alle vormen van uitdiensttreding in het kader van het blokkeren van gebruikersrechten volgens eenzelfde procedure te laten verlopen.

Prioriteit

HOOG

LAAG

Managementcommentaar

De procedure voor het blokkeren van accounts is aanwezig. De geconstateerde uitzonderingen pakken we op binnen de interne controle en worden waar nodig direct gecorrigeerd.

Beheerrechten AFAS en procedure toekenning hoge rechten

Bevinding, risico en aanbeveling

Wij hebben vernomen dat voor het toekennen van hoge rechten in de applicatie AFAS geen vaste procedure is ingericht en voorsnog geen richtlijnen zijn opgesteld. Wij hebben geconstateerd dat meer dan 10 functionarissen beheerrechten hebben in de applicatie, waaronder medewerkers van Veiligheidsregio Zuid-Limburg, maar ook diverse consultants. Het relatief omvangrijke aantal gebruikersaccounts met beheerrechten is een gevolg van de migratie naar AFAS, zodat voldoende ondersteuning geboden kon worden gedurende het migratieproces en dit proces adequaat vormgegeven kon worden.

Omdat de migratie inmiddels is afgerond, adviseren wij na te gaan voor welke gebruikers de applicatiebeheerrechten ingeperkt kunnen worden, zodat het aantal gebruikers met beheerrechten tot een strikt minimum is beperkt. Tevens adviseren wij om richtlijnen te bepalen waarin wordt geduid welke medewerkers over beheerrechten dienen te beschikken en om een procedure in te richten om het toekennen en intrekken van beheerrechten beheerst te laten verlopen.

Prioriteit

HOOG

LAAG

Managementcommentaar

Voor het toekennen van beheerdersrechten is nog geen vaste procedure ingericht. We nemen deze bevinding mee in onze planning voor 2026 en zullen een duidelijke richtlijn opstellen waarin wordt vastgelegd wie welke rechten mag hebben.

Toets op voldoen aan afspraken in offerte

Bevinding, risico en aanbeveling

Als onderdeel van onze controlewerkzaamheden ten aanzien van het inkoopproces volgen wij een inkoopproces van offerte tot betaling. Bij de uitvoering van deze zogeheten lijncontrole op het inkoopproces hebben wij geconstateerd dat in de offerte is overeengekomen dat een inkoopfactuur van een urenverantwoording wordt voorzien, maar dat deze urenverantwoording feitelijk niet is bijgesloten bij de betreffende inkoopfactuur. Wij hebben begrepen dat deze urenverantwoording ook niet door de organisatie is opgevraagd. Naar wij begrijpen wordt de inkoopfactuur goedgekeurd op basis van rechtstreeks onderling contact.

Hoewel wij begrijpen dat een prestatie op basis van rechtstreeks contact kan worden vastgesteld, adviseren wij om te allen tijde er zorg voor te dragen dat de afspraken in de overeenkomst worden nageleefd. Tevens vinden wij het voor de aantoonbaarheid van de prestatielevering belangrijk dat de organisatie erop toeziet dat zij een onderbouwing verkrijgt van de gefactureerde prestaties, in casu door middel van de in de offerte genoemde urenverantwoording.

Prioriteit

HOOG

LAAG

Managementcommentaar

Wij zien op dit punt geen wijziging nodig, omdat onze interne werkwijze voldoende waarborgen biedt voor de beoordeling van facturen. Dit punt wordt daarom niet verder opgepakt.

Versterking verbijzonderde interne controle

In huidig jaar is een verbetertraject gestart met betrekking tot de verbijzonderde interne controle. Voorbeeld hiervan betreft het versterken van het sturend karakter van de controle inkooprechtmatigheid. Voorafgaand aan het jaar wordt het interne controleplan opgesteld, waarin onder andere de kaders, aanpak en wijze van rapporteren zijn beschreven. In de managementrapportages worden beknopt de belangrijkste bevindingen en de opvolging van onze managementletter beschreven. De hiervoor genoemde ontwikkelingen en de ingezette lijn onderschrijven wij als positief. Om deze ontwikkelingen verder vervolg te geven delen wij hierna een aantal vervolgstappen die de verbijzonderde interne controle verder kunnen versterken.

Wij hebben vernomen dat voor diverse processen de interne controlewerkzaamheden nog niet volledig zijn afgerond. Volgend hierop zijn voor deze processen nog geen conclusiememoranda of rapportages beschikbaar. Wij adviseren om interne controlewerkzaamheden periodiek uit te voeren, waarbij ook periodiek – bijvoorbeeld elk kwartaal – terugkoppeling plaatsvindt naar de organisatie inclusief wederhoor ten aanzien van de geconstateerde bevindingen. Hierdoor wordt een actievare en tijdigere monitoring op processen en interne beheersingsmaatregelen geïnitieerd, waardoor reeds tussentijds bijgestuurd kan worden waar dit nodig wordt geacht.

Voor de werkbestanden van de verbijzonderde interne controle adviseren wij om de uitkomsten van de individuele waarnemingen te vertalen naar een algehele conclusie ten aanzien van het betreffende proces. Deze conclusie kan vervolgens een basis vormen voor de in de conclusiememoranda te rapporteren aandachts- en adviespunten.

Voorts geven wij in overweging om in conclusiememoranda de bevindingen en adviezen tevens te vertalen naar voorgestelde actiepunten voor de organisatie. Hiermee wordt bewerkstelligd dat aan de organisatie handvatten worden aangereikt om bevindingen concreet en effectief op te volgen en biedt het de mogelijkheid om in een eerstvolgende interne rapportage te reflecteren op de opvolging van de actiepunten uit deze eerdere rapportage.

Prioriteit

Managementcommentaar

HOOG

LAAG

De verbijzonderde interne controle wordt verder versterkt binnen het interne controleplan 2026. Het opstellen van conclusiememo's per proces wordt hierin meegenomen. De opvolging en rapportage worden structureel ingericht.

Bevinding, risico en aanbeveling

Bij het opstellen van de begroting en de jaarrekening stelt Veiligheidsregio Zuid-Limburg een risicoanalyse op ten behoeve van de paragraaf weerstandsvermogen. Een gestructureerde risicoanalyse heeft tot doel om inzicht te verkrijgen in de risico's die de organisatie loopt ten aanzien van de verschillende processen, het inschalen van deze risico's, alsmede het definiëren en prioriteren van maatregelen ten aanzien van de geïdentificeerde risico's. Wij vinden het belangrijk dat als onderdeel van een risicoanalyse voldoende aandacht wordt geschonken aan het onderscheid tussen risico's voortvloeiende uit mogelijke fouten (onbewuste afwijkingen) en risico's voortvloeiende uit mogelijke fraude (bewuste afwijkingen). Vanwege het bewuste karakter van fraude, is voor dergelijke risico's een sterkere mate van interne beheersing vereist. Om de frauderisicoanalyse gedegen vorm te geven adviseren wij deze te starten vanuit frauderisicofactoren, hetgeen factoren betreffen die individueel, dan wel in gezamenlijkheid kunnen leiden tot een risico op fraude. Hierbij is het van belang om deze frauderisicofactoren te structureren aan de hand van de frauderisicodriehoek, waarbij risicofactoren worden ingedeeld in de categorieën druk, gelegenheid en rationalisatie. Een voorbeeld van een combinatie van frauderisicofactoren die tot een frauderisico kunnen leiden is een medewerker met loonbeslag (druk) die bevoegdheden heeft in het betalingsproces (gelegenheid).

Om te toetsen dat de interne beheersing ter afdekking van geïdentificeerde risico's gedegen plaatsvindt, adviseren wij de interne controlewerkzaamheden in te schalen en prioriteren in lijn met de inschaling en prioritering van risico's zoals gedefinieerd in risicoanalyse die door de leiding van de organisatie is uitgevoerd, waarmee de risicoanalyse sturend is voor de uitvoering van de verbijzonderde interne controle werkzaamheden, inclusief het definiëren van focusgebieden.

Daarnaast adviseren wij u om tevens een onderzoeksprotocol op te stellen waarin de procedure is beschreven welke handelingen dienen plaats te vinden bij fraudesignalen, dan wel plaatsgevonden fraude.

Prioriteit

HOOG

LAAG

Managementcommentaar

In 2026 wordt gestart met het opstellen van een frauderisicoanalyse. De bevinding wordt meegenomen in de verdere versterking van onze risicobeheersing.

Bijlagen



Deels en niet opgevolgde bevindingen voorgaande rapportage

Wachtwoordbeleid netwerk en applicaties

Bevinding, risico en aanbeveling

We hebben vastgesteld dat Veiligheidsregio Zuid-Limburg geen Multi Factor Authenticatie (MFA) heeft ingericht voor het benaderen van de werkomgeving vanaf een externe locatie. Voorts hebben wij voor de applicatie Motion vastgesteld dat – ondanks dat deze applicatie rechtstreeks te benaderen is buiten de beveiligde omgeving van de organisatie om – er geen gebruik wordt gemaakt van MFA en het niet verplicht is om wachtwoorden periodiek te wijzigen.

Wij benadrukken het belang om het wachtwoordbeleid voor het netwerk en applicaties te versterken, zodat voldoende maatregelen zijn getroffen om ongeautoriseerde toegang door derden te voorkomen. Aanvullend vermelden wij dat wanneer van een externe locatie wordt ingelogd, het gebruik van MFA onder BIO (Baseline Informatiebeveiliging Overheid) 2.0 verplicht is voor overheidsorganisaties om zodoende beter aan de beveiligingsbehoeften te voldoen uitgaande van de huidige digitale dreigingen. Ook het wijzigen van wachtwoorden en het geautomatiseerd afdwingen hiervan zijn vereisten onder BIO 2.0.

Prioriteit

HOOG

LAAG

Managementcommentaar

Er is Multi-Factor Authenticatie (MFA) ingericht voor toegang tot de Viewomgeving. Dit gebeurt via een authenticator-app in combinatie met een wachtwoord. Voor Motion is er echter geen MFA beschikbaar, wat te maken heeft met het werken in twee domeinen. Dit wordt vanaf 2025 niet meer relevant, omdat Motion vervangen zal worden door AFAS, waarin deze beveiligingsaspecten beter geregeld zullen zijn. Ook is er voor Motion een verplichting om wachtwoorden regelmatig te wijzigen. De implementatie van BIO 2.0 staat gepland voor eind 2024 of begin 2025. Tegen die tijd worden verdere maatregelen getroffen om te voldoen aan de gestelde normen. Daarnaast wordt er hard gewerkt aan ISO 27001-certificering, wat voor Q3 2025 is gepland.

Regievoering op uitbestede IT-diensten

Veiligheidsregio Zuid-Limburg heeft een belangrijk deel van haar IT uitbesteed aan externe leveranciers, onder meer in de vorm van SaaS-oplossingen. In het kader van de beheersing is het belangrijk om regie te voeren op deze uitbestede IT-diensten. Deze regievoering kan onder andere plaatsvinden door middel van het formaliseren van afspraken met IT-dienstverleners en het monitoren van de feitelijke prestaties in relatie tot deze afspraken. Formalisatie van afspraken vindt plaats in Service Level Agreements en dienstverleningsovereenkomsten. De monitoring vindt plaats op basis van Service Level Reports (SLR's), assurance-rapportages (bijvoorbeeld ISAE 3402) omtrent de effectieve werking van de procedures bij de IT-dienstverleners en het voeren van periodieke gesprekken waarbij wordt ingezoomd op de overeengekomen KPI's en in hoeverre hieraan wordt voldaan.

Wij stellen vast dat Veiligheidsregio Zuid-Limburg niet actief naar certificeringen, assurance-rapportages of SLR's vraagt om de noodzakelijke monitoring vorm te geven en dat binnen uw organisatie onduidelijkheid bestaat over welke functionaris verantwoordelijk is voor het voeren van regie op de IT-dienstverleners ten aanzien van de applicaties AFAS, AG5 en Motion.

Wij bevelen aan om het leveranciersbeheer te implementeren als onderdeel van het informatiebeleid van uw organisatie en om per applicatie een functionaris aan te wijzen als regievoerder. Onderdeel van het leveranciersbeheer is tevens het invoeren van een procedure voor het periodiek beoordelen van de dienstverlening door de IT-leveranciers in relatie tot de geformuleerde KPI's.



De conclusie wordt erkend. Er wordt op dit moment een specialist in functioneel beheer geworven, die samen met de Service Delivery Manager zal werken aan het verbeteren van de regievoering. Dit traject zal naar verwachting in 2025 zijn afgerond.

**Bevinding, risico en
aanbeveling**

Prioriteit

Managementcommentaar

Bezwaartermijn gunning aanbestedingen

Bevinding, risico en aanbeveling

Als onderdeel van onze werkzaamheden ten aanzien van het proces aanbesteden, voeren wij een zogeheten lijncontrole uit. In deze lijncontrole volgen wij het aanbestedingsproces van A tot Z en beoordelen wij de relevante documentatie onderliggend aan de betreffende aanbesteding. Om de gunning van de opdracht bekend te maken zijn e-mails verstuurd aan de gegunde partij en de afgewezen partijen. Voordat tot definitieve gunning overgegaan wordt, is het gebruikelijk een bezwaartermijn beschikbaar te stellen voor de afgewezen partijen. Ondanks dat deze bezwaartermijn geen verplichting betreft voortkomend uit wetgeving dan wel uit het inkoopbeleid, wordt in het inkoopbeleid waarde gehecht aan klachtenregeling en eerlijke mededinging. Wij adviseren om bij voorlopige gunning van een opdracht gunnings- en afwijzingsbrieven te versturen naar de betrokken partijen, waarin een bezwaartermijn wordt opgenomen van minimaal één week. Na het verstrijken van deze bezwaartermijn, kan worden overgegaan op definitieve gunning van de opdracht.

Prioriteit

HOOG

LAAG

Managementcommentaar

Bij een meervoudig onderhandse aanbesteding is een bezwaartermijn niet verplicht volgens wet- en regelgeving. Vanuit onze interne afwegingen achten wij het niet nodig om een dergelijke termijn op te nemen in onze procedures. Het huidige proces voldoet aan de interne richtlijnen voor klachtenafhandeling en eerlijke mededinging.

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING



RSM Netherlands Accountants N.V.

Bekkerweg 10
Postbus 6005
6401 SB Heerlen
T 045 405 5555
rsmnl.com

RSM Netherlands Accountants N.V. is een onafhankelijk lid van het RSM netwerk en handelt onder de naam RSM. RSM is de handelsnaam van elk bij het RSM netwerk aangesloten kantoor. Het RSM netwerk is een samenwerkingsverband van onafhankelijke accountants- en advieskantoren, die ieder voor eigen verantwoordelijkheid werken. Het RSM netwerk bestaat in geen enkel rechtsgebied als afzonderlijke rechtspersoon. Op alle opdrachten zijn onze algemene voorwaarden van toepassing, die op verzoek kosteloos worden toegezonden. RSM Netherlands Accountants N.V. is ingeschreven bij de Kamer van Koophandel onder 34255759.

© RSM International Association, 2024