

A.B. 26/11

Onderwerp: Managementletter 2025

Inleiding

Op 31 oktober 2025 heeft de Publieke Sector Accountants (PSA) de Management Letter 2025 gepresenteerd aan SVHW. In dit document zijn de bevindingen en aanbevelingen opgenomen met betrekking tot de interne beheersing in de processen en de IT-omgeving. De algehele conclusie is dat de accountant tevreden is met de ontwikkelingen binnen onze organisatie en dat er flinke stappen zijn gezet in 2025 (o.a. op het gebied van fraudebeheersing). Dit ook realiserend, dat deze stappen zijn gezet naast de implementatie van een nieuw financieel en HRM systeem (AFAS).

Naast nieuwe bevindingen heeft de accountant ook een overzicht opgesteld van de bevindingen uit eerdere Management Letters, onderverdeeld in: opgelost, niet opgelost en in behandeling. Slechts één bevinding uit eerdere jaren staat in 2025 nog als 'in behandeling' en is daarom opgenomen in onderstaand overzicht. Drie bevindingen uit voorgaande jaren zijn inmiddels opgelost en één bevinding is als 'niet opgelost' aangemerkt, omdat automatisering hiervoor niet mogelijk lijkt. Deze vier bevindingen zijn daarom niet opgenomen in onderstaand overzicht.

Onderstaand overzicht bevat de bevindingen van het huidige jaar, aangevuld met concrete voorstellen om de aanbevelingen praktisch te implementeren binnen SVHW. Wat opvalt aan de bevindingen van de accountant is dat de nadruk vooral ligt op het meer vastleggen van werkzaamheden die wij al doen.

In de bijlagen treft u aan:

- De Managementletter 2025 (A.B. 26/12);

Gewenste behandeling

U wordt verzocht kennis te nemen van de Managementletter 2025.

Toelichting

PSA heeft in de Managementletter 2025 de volgende (proces)bevindingen en aanbevelingen vermeld. In het onderstaande worden de bevindingen van de accountant vermeld inclusief de getroffen c.q. nog te treffen maatregelen vanuit de staande organisatie:

1 Controle invoeren tarieven belastingverordeningen

Bevinding accountant:

Het proces is te complex, namelijk er zijn te veel (dezelfde) controles uitgevoerd door meerdere personen, waarbij onduidelijk is wie waarvoor verantwoordelijk is. Het is niet duidelijk en zichtbaar welke controles zijn uitgevoerd door de verschillende functionarissen.

Opvolging bevinding:

Bij de invoer op de tarieven 2026 pakken we dit punt direct op.

Om dit te doen passen wij de procesbeschrijving voor dit onderwerp aan waarbij wij duidelijk beschrijven welke medewerkers welke controles uitvoeren en op welke manier zij deze documenteren.



Aanvullend op deze procesbeschrijving stellen wij een checklist op die afdwingt dat de controles zichtbaar worden vastgelegd, op welk moment deze controles zijn uitgevoerd en door wie dat is gedaan.

2 Controle publicatie belastingverordeningen

Bevinding:

SVHW controleert of de belastingverordeningen door de gemeenten zijn gepubliceerd, maar deze controle wordt niet zichtbaar vastgelegd. Hierdoor is niet aantoonbaar waarop is gecontroleerd, wie dit heeft gedaan en wanneer dit is gebeurd.

Opvolging bevinding:

Ook deze bevinding kan snel worden opgepakt (Q4 2025) door deze te koppelen aan voorgaande bevinding. Door het toevoegen van de controlestap in de genoemde checklist: vastgesteld dat verordening is gepubliceerd.

3 Contractregistratie

Bevinding:

Contracten kunnen geregistreerd worden in AFAS zonder een contractwaarde in te vullen. Hierdoor worden regelmatig contracten zonder waarde ingevoerd, terwijl er wel sprake is van een financiële verplichting of van een maximale waarde (bijvoorbeeld bij raamcontracten).

Opvolging bevinding:

In het systeem kan verplicht worden gesteld dat bij ieder contract een contractwaarde wordt ingevuld. Echter sommige contracten zijn afhankelijk van het volume van het af te nemen product en daarom is een contractwaarde niet per definitie hard vast te leggen. Wij zullen in Q2 van 2026 onderzoeken op welke wijze wij de waardes van raamcontracten het beste vast kunnen leggen en hoe wij de interne controle hierop inrichten.

4 Prestatielevering

Bevinding:

Er is momenteel geen uniforme format voor het vastleggen van prestatielevering. Hierdoor bepalen medewerkers zelf hoe zij de prestatielevering registreren, wat leidt tot verschillen in de kwaliteit en volledigheid van de vastlegging.

Opvolging bevinding:

Wij zijn momenteel bezig met de ontwikkeling van een format voor prestatielevering. Deze wordt in januari 2026 ter vaststelling aangeboden aan het MT. Door gericht aandacht aan het onderwerp prestatielevering te besteden vanuit Financiën is de verwerking hiervan in AFAS al verbeterd.

5 Logische toegangsbeveiliging – Autorisatiematrix

Bevinding:

Er is geen autorisatiematrix voor AFAS. Gebruikersrechten worden daarom handmatig en zonder vaste richtlijnen toegekend door IT, vaak door rechten te kopiëren van andere medewerkers. Hierdoor bestaat het risico dat medewerkers meer toegang krijgen dan noodzakelijk is.



Opvolging bevinding:

Het opstellen van een autorisatiematrix voor AFAS en andere sleutelapplicaties staat hoog op de prioriteiten lijst binnen de organisatie.

De autorisatiematrix voorziet in een heldere procedure waarin per functie de benodigde rechten zijn vastgelegd en die vervolgens aansluiten op de gewenste functiescheidingen binnen de organisatie. Daarnaast kan SVHW een gestandaardiseerde procedure inrichten voor het aanvragen, toekennen, wijzigen en intrekken van rechten in AFAS. Bij dubbelrollen of ongewenste vermenging van rechten kunnen we dan weloverwogen de risico's in kaart brengen en besluiten dit te accepteren of niet. Aanvullend kunnen we een periodieke beoordeling laten uitvoeren (bijv. per kwartaal) door leidinggevenden of de toegekende rechten nog actueel en passend zijn.

Deze aanbeveling ligt in het verlengde van het ISO 27001 traject wat al in gang is gezet en sluit ook aan op de voorschriften vanuit de BIO en NIS2 waar wij aan moeten voldoen. Conform onze ICT Roadmap staat opvolging gepland voor Q3 2026.

6 Logische toegangsbeveiliging – Superuser rechten

Bevinding:

Binnen AFAS en Key2Belastingen zijn superuser rechten toegekend aan medewerkers met een operationele functie. Daarnaast is één superuser account overbodig bij Key2Belastingen.

Opvolging bevinding:

Als gevolg van het hebben van een efficiënte bedrijfsvoering is het niet altijd mogelijk om superuser rechten (oftewel beheeraccounts) te scheiden van medewerkers die werken in de uitvoering. Ondanks dat wij controles inrichten om misbruik van deze rechten te voorkomen onderschrijven wij ook het risico wat de accountant hieromtrent signaleert.

Een aanvullende maatregelen dat getroffen kan worden om het risico te beperken is om de superuser accounts te bewaren in de kluis en dat ze alleen gebruikt kunnen worden op het moment dat het nodig is (vastlegging daarvan). Dit zorgt voor een extra borging en controle op de activiteiten die met dit account worden uitgevoerd.

In 2026 onderzoeken wij in hoeverre dit mogelijk is en of dit praktisch uitvoerbaar is. Ook zal worden onderzocht of andere oplossingen misschien beter passend zijn om dit risico verder te mitigeren.

7 Logische toegangsbeveiliging – Periodieke review autorisaties

Bevinding:

SVHW voert jaarlijks een review uit op rechten in de Active Directory, maar niet op de rechten binnen de applicaties zelf zoals Key2Belastingen en AFAS. Hierdoor blijven risico's op ongeautoriseerde toegang en doorbroken functiescheiding mogelijk onopgemerkt.

Opvolging bevinding:

Het opleveren van een autorisatie matrices voor Key2 Belastingen alsmede AFAS en het opstellen van en borgen van de autorisatiereviews zijn opgenomen in de ICT Roadmap 2026 (opleveren in Q3 2026).



8 Change management – Wijzigingsbeheer

Bevinding:

Het wijzigingsbeheerproces is operationeel ingericht, maar belangrijke stappen zoals formele beoordeling, testresultaten, vastlegging en akkoord vóór productie ontbreken of verlopen informeel. Hierdoor is niet aantoonbaar dat wijzigingen volledig zijn getest, beoordeeld en goedgekeurd vóór de productie. Dit brengt risico's met zich mee voor fouten, onjuiste koppelingen en de betrouwbaarheid van het systeem.

Opvolging bevinding:

In 2026 formaliseren we dit proces en leggen daarin minimaal vast dat:

1. Release notes vooraf worden beoordeeld en schriftelijk vast wordt gelegd welke onderdelen getest moeten worden
2. Testplannen per release aan worden gepast op basis van de beoordeelde release notes.
3. Opvolging van de bevindingen schriftelijk vast worden gelegd, bijvoorbeeld door in het testplan een kolom op te nemen met datum en status van afhandeling.

9 Continuïteit – Restoretests

Bevinding:

Er zijn nog geen restoretests uitgevoerd voor Key2Belastingen en AFAS Online. Ook is binnen de eigen omgeving geen back-up aangevraagd en getest. Hierdoor is niet aantoonbaar dat systemen na een calamiteit correct kunnen worden hersteld. Dit brengt risico's met zich mee op dataverlies en verstoring van de continuïteit van de dienstverlening

Opvolging bevinding:

In 2025 zijn de door de accountant genoemde restoretests wel uitgevoerd en gelogd maar niet formeel volgens een vastgestelde werkprocedure doorlopen. In 2026 formaliseren we deze procedures en leveren dit op in Q2 2026.

Aandachtspunten Jaareinde:

De accountant heeft voor de controle op de jaarverantwoordingen en jaarrekening 2025 een aantal aandachtspunten gesignaleerd.

Deze aandachtspunten zijn bij de organisatie bekend en zijn meegenomen in de planning voor de jaarverantwoordingen en jaarrekening 2025.

Overig

n.v.t.

Klaaswaal, 4 februari 2026