WNK PERSONEELSDIENSTEN
Hertog Aalbrechtweg 32 - 1823 DL ALKMAAR
Postbus 9150 - 1800 GD ALKMAAR
Telefoon: (072) 56 78 890
Fax: (072) 56 78 800
Email: i.tromp@wnk.nl
Website: www.wnk.nl

N O T I T I E

Aan	:	Dagelijks bestuur
Kopie aan	:	
Van	:	I. Tromp, Manager Finance & Control
Kenmerk	:	D19.001/Itr
Onderwerp	:	Managementletter 2018
Datum	:	22 januari 2019

Zoals elk jaar heeft onze accountant een interim-controle uitgevoerd. Deze controle is primair gericht op de analyse en evaluatie van de interne beheersingsomgeving en de daarin opgenomen maatregelen van interne controle. De bevindingen zijn verwoord in de managementletter 2018.

De implementatie van AFAS heeft veel effect gehad op de administratieve organisatie en interne beheersing. Om deze reden zijn er dit jaar meer bevindingen en inzichten dan voorgaande jaren (bevinding is een constatering die naar mening van de accountant opgepakt dient te worden om de financiële beheersing te waarborgen, en een inzicht is een punt dat naar mening van de accountant bijdraagt aan een nog betere beheersing of een efficiencyslag, maar waar geen sprake is van een significante tekortkoming). Een reactie per bevinding is op zijn plaats, als begeleiding bij de managementletter. Zie onderstaande deze reactie.

Nacalculatieregels - Bevinding
Bij de diverse omzetprocessen (zoals termijnfacturatie) hebben wij geconstateerd dat het mogelijk is dat een senior medewerker van de financiële administratie zowel nacalculatieregels (urenregistratie) invoert als autoriseert. Wij vernamen dat dit uit praktische overwegingen is ingeregeld, zodat de facturatie tijdig kan plaatsvinden indien van de nacalculatieregels niet tijdig worden geautoriseerd. U loopt hier het risico dat de control technische functiescheiding tussen invoer en autorisatie van de nacalculatieregels doorbroken wordt, hetgeen als beheersmaatregel dient om te borgen dat de registratie correct verloopt. Uit de eerste bespreking met uw financieel management is gebleken dat u onderzoekt hoe u een controle kunt inrichten op het doorbreken van de functiescheiding. Desgewenst denken wij hierin graag met u mee. In dit kader merken wij op dat creditnota's ook als (negatieve) nacalculatieregels worden verwerkt. Alhoewel uit bespreking met uw medewerkers blijkt dat deze in opzet in functiescheiding worden verwerkt, blijkt uit een voorgaande bevinding dat het systeem dit niet afdwingt. Wij verzoeken u om daarom per jaareinde een analyse uit te voeren op de creditnota's, waarbij u nagaat of zij in functiescheiding tot stand zijn gekomen en of zij juist en rechtmatig zijn opgesteld.

Reactie
Het gaat hier om handmatig ingevoerde nacalculatieregels (regie-opdrachten) zoals detachering op urenbasis en post. Het nacalculatieregels proces is in maart aangepast. De desbetreffende projecten hebben allemaal interne projectleiders. Deze projectleiders accorderen de nacalculatieregel waarna door een senior/teammanager de ingevoerde regel wordt gecontroleerd en gereed gemeld. De groepsdetachering in Opmeer vormt hierop een uitzondering. Voor deze groepsdetachering is reeds geaccordeerde informatie beschikbaar, wat de basis is voor de invoer en wordt dus volledig op de financiële administratie verwerkt en gecontroleerd. Op dit moment een dubbele stap, maar deze stap is ingebouwd zodat de eindcontrole bij de afdeling Financiën ligt. Het proces voor creditnota's is hetzelfde. De rechtmatigheid is geborgd bij de controle van de nacalculatieregel door de interne projectleider.

NOTITIE

Managementletter 2018
22 januari 2019

Volledigheidsanalyse - Bevinding
Tot en met 2016 genereerde u periodiek een controlelijst waarmee inzichtelijk werd gemaakt of er op orderniveau verschillen waren tussen de geproduceerde aantallen (conform inleverbon) en gefactureerde aantallen (conform pakbon en de factuur). Deze controle dient als extra controlemiddel om te signaleren of er verschillen bestaan tussen productie en facturatie, hetgeen u daarna mogelijk nog kunt herstellen. Wij vernamen dat u inmiddels een vergelijkbare controlelijst in AFAS aan het inrichten bent, zodat u een extra waarborg heeft dat uw omzetverantwoording over 2018 volledig is.

Reactie
Wij hebben het overzicht/analyse, - geproduceerd versus gefactureerd -, gemaakt.

Functiescheiding - Insight
Binnen het proces van de afdeling van Montage & Verpakking is een aantal functiescheidingen ingericht. Zo is er sprake van functiescheiding tussen het bedrijfsbureau, de productiemedewerkers, het magazijn en de facturatie. Deze functiescheiding blijkt uit de productieorder waarop de verschillende functionarissen hun paraaf zetten wanneer zij hun activiteiten binnen het proces hebben uitgevoerd. Afgelopen jaar hebben wij u gerapporteerd dat destijds niet in alle gevallen deze functiescheiding zichtbaar uit de productieorder bleek. Wij vernamen dat u naar aanleiding van de bevinding uit voorgaand jaar actief laat monitoren of alle productieorders in functiescheiding zijn ondertekend.
In het nieuw ingerichte proces vindt de technische functiescheiding ook plaats op de hardcopy productieorders, hetgeen nog diverse handmatige handelingen inhoudt. Wij geven u in overweging om deze functiescheiding in AFAS als afzonderlijke processtappen in te richten. Hiermee waarborgt u dat productieorders in functiescheiding worden verwerkt, beperkt u het aantal handmatige vastleggingen dat u dient te maken (en te administreren) en hoeft u achteraf geen controle uit te voeren om na te gaan of de handmatig ingerichte functiescheiding altijd aanwezig was.

Reactie
Bij facturatie van een order worden de fysieke inleverbonnen gecontroleerd op juiste aantallen en volledigheid parafen. Dit proces is moeilijk in AFAS vast te leggen, omdat digitale verwerking van dit proces onwerkbaar is voor de leiding op de werkvloer.

Registratie prijsafspraken - Insight
Wij hebben vernomen dat schriftelijke prijsafspraken met afnemers doorgaans niet standaard in AFAS worden opgeslagen. U geeft aan dat schriftelijke prijsafspraken op dit moment doorgaans in de mail of in een hardcopy map worden bewaard. Wij geven u in overweging om de prijsafspraken standaard te registeren in AFAS zodat de afspraken voor alle betrokkenen centraal te lokaliseren zijn, hetgeen eventueel benodigde controles later in het proces gemakkelijker maakt.

Reactie
In het maandelijks overleg met Montage en Verpakking is afgesproken om dit vast te leggen. Er is ook een apart dossieritem in AFAS voor aangemaakt. Er wordt nu nagedacht om de verkoopofferte ook vast te leggen AFAS.

NOTITIE

Managementletter 2018
22 januari 2019

Functiescheiding registratie verzuim - Bevinding
Bij de facturatie van detacheringen wordt op de voorgenomen facturatie een handmatige korting toegepast in het geval van langdurig ziekteverzuim van de gedetacheerde. Deze handmatige correctie wordt in het huidige proces niet gecontroleerd door een onafhankelijke medewerker. Daarmee loopt u het risico dat foutieve correcties niet worden gesignaleerd, waardoor er mogelijk een foutieve factuur verstuurd kan worden.
Wij adviseren u om een controle in te richten op de mutaties die worden doorgevoerd op de facturatierun uit AFAS om te borgen dat er geen onjuiste correcties plaatsvinden.

Reactie
Er is functiescheiding aangebracht tussen de invoer en controle van de mutaties.

Geen analyse op € 0-tarieven - Insight
U heeft de mogelijkheid om een detacheringstarief van € 0 overeen te komen, bijvoorbeeld voor een gewenningsperiode. Wij vernamen dat u niet met een vaste periodiciteit toetst of de tarieven bijgesteld moeten worden. Hierdoor loopt u het bedrijfsrisico dat u mogelijk te lang een tarief van € 0 in rekening brengt, waardoor u opbrengsten misloopt. Wij adviseren u om een periodieke analyse op de € 0-tarieven in te richten, zodat beoordeeld kan worden of het detacheringstarief niet herzien dient te worden.

Reactie
Vanaf laatste kwartaal 2018 wordt dit elk kwartaal gedaan.

Genereren detacheringsovereenkomsten - Insight
Uit bespreking met uw administratief medewerkers hebben wij vernomen dat de detacheringsovereenkomsten nog niet automatisch worden gegenereerd uit AFAS; de overeenkomsten worden nog handmatig opgesteld. Het handmatig opstellen van de overeenkomst verhoogt de kans op fouten en is daarnaast meer arbeidsintensief. Wij adviseren u om te onderzoeken in hoeverre u deze stap kunt automatiseren.

Reactie
De detacheringsovereenkomsten zijn omgedoopt tot opdrachtovereenkomsten en worden inmiddels vanuit AFAS gegenereerd.

Termijnfacturatie - Bevinding
Onderdeel van het proces van termijnfacturatie is het aanmaken van een project in AFAS en het invoeren van de projecteigenschappen op basis van de achterliggende overeenkomst. Aan de hand van het aantal ingevoerde termijnen en de totale aanneemsom berekent AFAS het uiteindelijk te factureren termijnbedrag. Wij hebben vastgesteld dat AFAS na het invoeren van een project geen controle en autorisatie op de invoer afdwingt. Hierdoor loopt u het risico dat de ingevoerde projecteigenschappen niet conform de getekende overeenkomst zijn. Wij adviseren u een dergelijke autorisatie door AFAS af te laten dwingen om het risico op invoerfouten te mitigeren.

Reactie
Degelijke autorisatie is niet afdwingbaar. Om dit op te vangen wordt er een print screen gemaakt van projecteigenschappen. Deze wordt zichtbaar gecontroleerd door de interne projectleider en toegevoegd aan het dossier.

NOTITIE

Managementletter 2018
22 januari 2019

Urenregistratie – Insight
Wij constateerden dat de geplande uren op een opdracht, zoals dat plaatsvond in DBS, niet als voorcalculatorische uren worden geregistreerd op project. Wij geven u in overweging om deze geplande uren alsnog te registeren, zodat u beter inzicht heeft in het rendement van een project. Deze informatie kan dienen als basis voor eventuele budgetonderhandelingen voor volgende jaren of voor meerwerkgesprekken, indien een opdracht niet het gewenste rendement oplevert.

Reactie
Wij zullen dit onderzoeken.

Scheiden dagboeken - Bevinding
In de administratie van WNK worden verschillende dagboeken gebruikt voor memoriaalboekingen. Er zijn aparte dagboeken ingericht voor systeemboekingen en er is een apart dagboek voor handmatige memoriaalboekingen. Wij hebben vastgesteld dat de dagboeken die zijn bedoeld voor systeemboekingen en andersoortige dagboeken (zoals inkopen) niet afgesloten zijn voor handmatige correcties. Doordat handmatige boekingen ook in andere dagboeken gemaakt kunnen worden, loopt u het risico dat u het overzicht over de handmatige correcties verliest. Ook de interne beheersing die u inricht op het dagboek memorialen kan hiermee vermeden worden. Wij adviseren u om te onderzoeken hoe u de dagboeken zo veel mogelijk kunt afsluiten voor ongewenste handmatige correcties.

Reactie
De verschillende dagboeken zijn niet af te sluiten voor memoriaalboekingen. Wij schatten dit risico het hoogst in bij debiteuren en crediteuren. Er zal per kwartaal worden geanalyseerd of deze kaarten andere mutaties bevatten dan systeemboekingen en zo ja of dit terechte correcties zijn.

Geen autorisatie memoriaalboekingen - Bevinding
Binnen het proces van het verwerken van memoriaalboekingen heeft u ingeregeld dat boekingen worden voorzien van een bijlage met onderbouwende documentatie. Wij vernamen dat er geen controle is ingericht om na te gaan of de gemaakte boeking aansluit op de (geautoriseerde) bijlage. Uit afstemming met uw medewerkers blijkt dat een eventuele foutieve boeking (voor zover van relevante omvang) wel zou worden gesignaleerd vanuit de periodieke analyses in het kader van de tussentijdse informatievoorziening. Desalniettemin adviseren wij u om de memoriaalboekingen standaard intern te laten toetsen voordat de boekingen worden verwerkt, om foutieve boekingen in zijn geheel te voorkomen.

Reactie
Wegens het afwijkend karakter van een memoriaalboeking zijn de kennis, expertise en bevindingen essentieel bij het opstellen en controleren van de boeking. Dit is niet over te dragen aan een andere collega. De uitleg heeft immers direct effect op de controle van de ander.

Periodeafsluiting - Insight
Op dit moment is het mogelijk om in AFAS met terugwerkende kracht in voorgaande periodes boekingen of correcties door te voeren. Hierdoor loopt u het risico dat na het genereren van tussentijdse rapportages onterecht wijzigingen worden aangebracht in voorgaande periodes. Wij geven u in overweging om een harde periodeafsluiting in AFAS in te regelen om te voorkomen dat er nog correcties in voorgaande periodes kunnen worden geboekt.

Reactie
In theorie is dit een prima voorstel, maar in de praktijk onwerkbaar, vanwege diverse terugwerkende kracht mutaties, die zowel intern als extern worden veroorzaakt, door gewijzigde informatie. Er is aandacht om deze terugwerkende kracht mutaties te beperken c.q. te stoppen. Zodra dit succesvol is doorlopen, zullen wij de periodes gaan afsluiten.

Workflow inkoopfacturen - Bevinding
Binnen het goedkeuringsproces van inkoopfacturen is ingeregeld dat er functiescheiding is tussen (i) autorisatie voor levering en (ii) autorisatie voor budget. Deze functiescheiding borgt dat er geen inkoopfacturen betaalbaar worden gesteld die niet daadwerkelijk zijn geleverd. Uit onze interim-controle blijkt dat niet wordt afgedwongen dat voorgenoemde functies altijd door 2 verschillende personen worden uitgevoerd. Hiermee loopt u het risico dat de ingeregelde functiescheiding doorbroken wordt waarmee het risico ontstaat dat er mogelijk voor goederen of diensten wordt betaald die niet (aan WNK) zijn geleverd. Wij adviseren u om te onderzoeken of u de functiescheiding kunt afdwingen of periodiek door middel van een review op de activiteitenlog van AFAS te toetsen of de functiescheiding is doorbroken.

Reactie
Het is niet mogelijk om de gewenste functiescheiding aan te brengen in AFAS. Wij zullen periodiek een review doen op de activiteitenlog.

Mutaties crediteurenstambestand - Bevinding
Bij het muteren van stamgegevens, zoals bankrekeningnummers, is in het primaire proces geen control technische functiescheiding ingeregeld. Dit zorgt ervoor dat een controle op de mutatie niet is afgedwongen. Hierdoor loopt u het risico dat er (bewust of onbewust) een foutieve mutatie in de stamgegevens plaatsvindt, hetgeen tot een foutieve betaling kan leiden. Wij vernamen van uw manager Finance & Control dat u het proces inmiddels gewijzigd heeft, waarbij u gewijzigde bankrekeningnummers controleert voordat een nieuwe betaling plaatsvindt. Wij merken hierbij op dat u steunt op de functionaliteit van AFAS dat gewijzigde bankrekeningnummers zichtbaar worden op de concept betaallijst. Wij adviseren u om te onderzoeken of deze functionaliteit alle wijzigingen toont, ook bij bijvoorbeeld handmatige betalingen of wanneer een bankrekeningnummer wordt gewijzigd naar een reeds bestaande bankrekening in AFAS (wat geen nieuwe invoer is, maar een gewijzigde koppeling in de bankrekeningentabel).

Reactie
Er vinden geen handmatige betalingen meer plaats. Bij het muteren van een reeds bestaand rekeningnummer, is deze mutatie zichtbaar op de betaallijst. Deze mutatie wordt gecontroleerd via het bestaande proces.

Contractenregister - Insight
Binnen AFAS is een contractenregister ingericht waarin aangegane verplichtingen worden geadministreerd. Wij hebben vernomen dat nog niet altijd een contractwaarde als verplichting wordt geregistreerd. Door het registeren van de contractwaarden vergroot u de waarde van uw contractenregister omdat (i) u inzicht heeft in de kwantitatieve verplichting die u nog heeft uitstaan en (ii) u bij het ontvangen van inkoopfacturen kun toetsen of de inkoopfactuur overeenkomt met de door u aangegane verplichting. Wij adviseren u om te onderzoeken of u de contractwaarde als een verplicht in te vullen veld kunt aanmerken, zodat geborgd is dat er altijd een contractwaarde wordt geregistreerd.

NOTITIE

Managementletter 2018
22 januari 2019

Reactie
Contractwaarde is een basis inrichting in AFAS en kan niet verplicht worden gesteld. Dit is ook logisch, omdat niet alle contracten een vaste contractwaarde hebben. Wij zullen elk jaar via een analyse controleren of de juiste contractwaarde is ingevuld.

3-way match - Insight
Momenteel heeft u nog geen 3-way match ingericht in uw workflows. Een 3-way match is mogelijk als u naast een inkooporder ook de ontvangstbevestiging registreert. Wanneer een inkoopfactuur binnenkomt en overeenkomt met zowel de inkooporder als de geregistreerde ontvangstbevestiging, dan kan de factuur automatisch betaalbaar worden gesteld zonder benodigde handmatige controles en autorisaties. Wij geven u in overweging om te onderzoeken of een 3-way match voor u van toegevoegde waarde is en valt te implementeren in AFAS.

Reactie
Het proces van inkooporder en ontvangst is alleen toepasbaar bij Montage en Verpakking. Voor de overige inkopen zal dit proces vastlopen in bureaucratie. Tevens is voor heel veel inkopen vooraf niet precies te bepalen welke kosten gaan worden gemaakt.

Controle premiepercentages - Bevinding
Bij de interim-controle constateerden wij dat er over de eerste helft van 2018 een foutief percentage voor de arbeidsongeschiktheidsverzekering is ingehouden. Deze fout is ook door u geconstateerd toen u een gewijzigde Werkhervattingskas beschikking van de belastingdienst ontving en verwerkte in de salarisadministratie. Wij adviseren u om te onderzoeken of de controle op de invoer van de percentages aangescherpt moet worden, om in de toekomst te voorkomen dat er foutieve percentages worden ingehouden.

Reactie
Bij een wijziging van percentages zal de teammanager FA-OB de invoer zichtbaar controleren.

Formatieanalyse - Bevinding
Met een toenemende digitalisering van processen bent u meer afhankelijk van de betrouwbare werking van AFAS voor een juiste en volledige verwerking van personele mutaties. Wij adviseren u om periodiek een analyse uit te laten voeren door de leidinggevenden op hun formatie, waarbij zij toetsen of hun formatie juist is en alle mutaties (zoals wijzigingen van dienstverbanden, wijzigingen van kostenplaatsen en uitdiensttredingen) juist en volledig zijn verwerkt. Daarmee signaleert u als wijzigingen niet juist of niet volledig zijn verwerkt.

Reactie
Wanneer de formatie niet correct zou zijn, wordt de leidinggevende dagelijks geconfronteerd met een afwijkende bezetting op zijn/haar afdeling door het ontbreken van de mogelijkheid van boeken van verlof, ziek- en hersteld meldingen. Het (tenminste) jaarlijks houden van functioneringsgesprekken waarop hij/zij zal worden aangesproken is zeker onderdeel van de behoefte om zijn bezetting up to date te houden. Wanneer er een overplaatsing of urenwijziging plaats vindt, wordt dit geïnitieerd door de direct leidinggevende en/of werkleider. Betrokkene heeft, door een intensievere toepassing van Afas steeds meer zelf de regie over het personeel op de afdeling. Tevens ziet de leidinggevende “slechts” het eigen personeel in Afas waardoor een directere focus op de eigen bezetting wordt bewerkstelligd. Het is om die redenen niet nodig nog een extra controle op de formatie te laten uitvoeren.

NOTITIE

Managementletter 2018
22 januari 2019

Indiensttreding - Insight
Bij een mutatie voor een (her)indiensttreding wordt momenteel de leidinggevende per mail akkoord gevraagd bij de ingevoerde mutatie. Wij geven u in overweging om te onderzoeken of deze processtap ingericht kan worden in de workflow in AFAS, zodat u communicatie buiten AFAS zo veel mogelijk beperkt en u tevens waarborgt dat de juiste autorisatie is verkregen voordat een mutatie definitief wordt verwerkt.

Reactie
De procedure is dusdanig aangepast dat elke nieuwe indiensttreding via InSite moet worden aangeleverd. De HRM-consulent is in deze procedure verantwoordelijk voor het proces van (her-)indiensttreding. De opdracht in InSite komt eerst weer bij de instuurder terug, zodat deze de gelegenheid heeft om aanvullende documenten of een opmerking toe te voegen. Hierna zal de opdracht naar de HRM-consulent gaan en, nadat deze heeft geaccordeerd, gaat de workflow door naar de werkleider van de afdeling. Vervolgens gaat de workflow naar de manager waar de afdeling onder valt en, na diens akkoord, gaat de workflow naar de personeelsadministratie. In elke stap dient goedkeuring plaats te vinden om naar de volgende stap te gaan. Bij afkeur zal de workflow weer terug keren naar de HRM-consulent. De personeelsadministratie zal uiteindelijk de administratieve afhandeling van de indiensttreding verzorgen en de arbeidsovereenkomst opstellen. Bij nieuwe dienstverbanden die niet rechtstreeks voortvloeien uit de uitvoer van een wettelijke regeling (WSW en Participatiewet), is ook akkoord nodig van de directeur.

Declaraties - Insight
Uit een waarneming in AFAS constateerden wij dat bij enkele declaratieworkflows (zoals studiekosten) niet door het systeem wordt afgedwongen dat er onderbouwende documentatie (zoals een factuur) wordt toegevoegd. Wij vernamen dat wel beoogd is dit altijd verplicht te stellen. Wij adviseren u te toetsen of voor alle workflows het bijvoegen van onderbouwende documentatie verplicht is en waar nodig uw workflows aan te passen waar dit nog niet het geval blijkt te zijn.

Reactie
Inmiddels is bij alle declaraties, behalve uren- en kilometerdeclaraties, onderbouwende documentatie verplicht.

'Begeleid werken'-betaling - Bevinding
De betalingen van de 'begeleid werken'-subsidies worden in AFAS voorbereid als negatieve nacalculatieregels. Deze nacalculatieregels kunnen handmatig aangepast worden, voordat tot betaling overgegaan wordt. Op de eventueel doorgevoerde wijziging vindt nog geen controle plaats. Daarmee loopt u het risico dat er foutieve aanpassingen worden gemaakt, hetgeen tot een foutieve uitbetaling van de 'begeleid werken'-subsidie kan leiden. Wij adviseren u om een controle in te regelen op de nacalculatieregels, voordat u tot betaling overgaat.

Reactie
Hierop is het proces inmiddels aangepast. Alles wat handmatig wordt ingevoerd en dus ook door middel van een analyse wordt ingelezen, moet gecontroleerd en geaccordeerd worden door een andere medewerker.

Procesmatige aandachtspunten - Bevinding
Eind oktober hebben wij kennis genomen van de interne controle op de uitvoering van de dienstencatalogus en hebben wij zelfstandig enkele gegevensgerichte werkzaamheden uitgevoerd.

Uit deze werkzaamheden volgen enkele detailbevindingen waarbij het raadzaam is te onderzoeken of er interne beheersmaatregelen ontbreken welke deze fouten hadden kunnen voorkomen.
Het verdient aandacht om de ingevoerde tarieven in AFAS te controleren op juiste invoer, daar er op het prijscomponent enkele bevindingen zijn geconstateerd. Ook bij nieuwe diensten buiten de Dienstencatalogus om dient u deze check uit te voeren om ervoor te zorgen dat er geen onjuiste tarieven in AFAS staan opgenomen en uit worden gefactureerd.
Verder kan het voorkomen dat uit te factureren documenten in projecten terecht zijn gekomen, waarna wordt gefactureerd door de trajectadministratie, terwijl deze documenten niet bij het juiste project zijn opgenomen. Hierdoor bestaat het risico dat mogelijk dubbel wordt gefactureerd of aan de verkeerde gemeente wordt gefactureerd. U heeft aangegeven dat dit vaak al in het proces wordt opgemerkt door de medewerkers bij de projecten en dit dan wordt hersteld. U heeft verder aangegeven dat dit zeer beperkt voorkomt en dit risico minimaal is en daar geen verdere actie op te zullen ondernemen omdat dit leidt tot onnodige efficiencybeperkingen. Naar aanleiding van deze bevinding heeft u wel gepland een herstellende integrale controle uit te voeren waar u ook de collega's uit het primaire proces bij zult betrekken. Op deze manier creëert u ook bewustzijn van het belang van een juiste en volledige primaire registratie bij de medewerkers uit het primaire proces. Wij zullen in december een aanvullende deelwaarneming uitvoeren om vast te stellen of de aanvullende interne controle van voldoende niveau is uitgevoerd.

Reactie
Ook de prijzen 2019 zijn handmatig in AFAS gezet en inmiddels door een andere collega zichtbaar gecontroleerd. Daarnaast is de concept Dienstencatalogus 2019 aangepast met de bijbehorende codes, zodat de juiste verkoopprijzen makkelijker te controleren is.

Beheersing serviceorganisaties
Met het implementeren van AFAS Online en de outsourcing van de algehele IT-omgeving naar Lemon Tree bent u voor de continuïteit van de IT-omgeving afhankelijk geworden van deze partijen. Belangrijke middelen om dit te beheersen zijn de Service Level Agreements (hierna: SLA) en een eventueel aanwezige ISAE 3402-rapportage. Wij vernamen dat u bij Lemon Tree een SLA bent overeengekomen die u eveneens periodiek evalueert. Wij vernamen dat u maandelijks een operationeel overleg en elk kwartaal een strategisch overleg heeft, waarbij u tevens evalueert of de afspraken uit de SLA worden nageleefd. Wij stelden vast dat u daarbij ook een rapportage van Lemon Tree ontvangt waarin enkele prestatie-indicatoren zijn opgenomen (zoals beschikbaarheid).
Wij begrepen dat het monitoren van de SLA van AFAS in mindere mate geformaliseerd is en dat dit met name incident gedreven is. Wanneer er sprake is van incidenten acteert u hierover richting AFAS. Wij geven u in overweging om, net als bij Lemon Tree, een periodieke toetsing uit te voeren op de naleving van de overeengekomen SLA.
Bij AFAS geldt dat er jaarlijks een ISAE 3402-verklaring wordt verkregen bij het internal control framework van AFAS. Dit houdt in dat een IT-auditor nagaat of de interne beheersingsomgeving over het afgelopen boekjaar juist heeft gefunctioneerd. Deze rapportage geeft inzicht in eventuele tekortkomingen in de beheersingsomgeving van AFAS. Ook geeft deze rapportage interne beheersingsmaatregelen weer die door de gebruikersorganisatie (in dit geval WNK) ingericht zouden moeten worden omdat dit niet is georganiseerd bij AFAS zelf (de zogenoemde gebruikersoverwegingen). Wij adviseren u om jaarlijks kennis te nemen van de ISAE 3402-rapportage om te beoordelen wat de implicaties zijn van eventuele tekortkomingen in de interne beheersing bij AFAS voor WNK. Tevens kunt u dan nagaan of u reeds invulling heeft gegeven aan de gebruikersoverwegingen in uw eigen beheersprocessen.

NOTITIE

Managementletter 2018
22 januari 2019

Reactie
Gezien de omvang van de gebruikersorganisatie van AFAS wordt de SLA op een andere manier gemonitord. Er zijn diverse bijeenkomsten en gebruikersgroepen waar WNK aan deelneemt om te borgen dat AFAS zich aan de afspraken houdt. De jaarlijkse ISAE 3402-verklaring wordt inmiddels opgevraagd en nagelezen door de manager Finance & control. Indien hiervoor aanleiding voor bestaat, gaat hij over tot actie.

User access: Wachtwoordbeleid
Wij stelden vast dat er een 2-factor authentication is ingericht. De eerste authenticatie vindt plaats door middel van het inloggen met een unieke gebruikersnaam en wachtwoord. De tweede authenticatie vindt plaats door middel van een code die wordt toegezonden aaneen mobielnummer, die ingevoerd dient te worden in AFAS. In combinatie met een sterk wachtwoordbeleid is dit een sterke toegangsbeveiliging (hoogste maturitylevel).
Wij merkten echter op dat er enkele omstandigheden zijn die de kracht van deze toegangsbeveiliging doen afnemen. Zo stelden wij vast dat er niet wordt afgedwongen dat het wachtwoord in AFAS periodiek gewijzigd wordt. Wij vernamen dat u reeds in gesprek bent met AFAS over dit onderwerp, omdat u deze instelling niet zelf kunt wijzigen.
Daarnaast vernamen wij dat op enkele afdelingen de tweede verificatie (de sms) naar een mobiele telefoon die bestemd is voor algemeen gebruik voor de afdeling wordt gestuurd. Daarmee wordt de tweede verificatie niet meer vertrouwelijk naar een persoon gestuurd, wat de kracht van deze tweede authenticatie doet afnemen. Wij begrepen dat het uit praktische overwegingen op deze manier is ingericht, omdat meerdere medewerkers niet beschikken over een telefoon van de zaak (wat overigens ook niet noodzakelijk is) en enkele medewerker zelfs helemaal niet over een mobiele telefoon beschikken.

Reactie
Op dit moment is ervoor gekozen om niet alle AFAS gebruikers een mobiele telefoon te verstrekken. Er is een beroep gedaan op de medewerkers zonder zakelijke telefoon om hun privé telefoon te gebruiken voor de 2-factor authentication, maar dit kan en wil WNK niet afdwingen. Voor wie geen zakelijke telefoon heeft en zijn privé telefoon niet wil gebruiken voor de authentication zijn afdelingstelefoons ter beschikking gesteld. De telefoons die voor een afdeling worden gebruikt, blijven op de afdeling. Hiermee worden risico's beperkt. Mocht in de toekomst blijken dat de keuze onveilig is, wordt op dat moment opnieuw een afweging gemaakt. Op dit moment acht WNK het veilig genoeg en wordt niet gekozen voor een aanzienlijke investering in mobiele telefonie. AFAS blijkt niet bereidt hun wachtwoord beleid aan te passen, hiervoor is de 2-factor authenticatie ingericht geeft AFAS aan.

User Access: beheer van rechten en rollen
Voor het aanmaken van nieuwe accounts of voor het toewijzen van rechten kan binnen WNK gebruik gemaakt worden van een standaardaanvraagformulier dat goedgekeurd moet worden door de leidinggevende. Wij vernamen dat dit formulier niet altijd gebruikt wordt en er in sommige gevallen ook verzoeken via de mail worden ingediend; in dit geval moet er ook een akkoord aanwezig zijn voor een leidinggevende. Wij vernamen dat er wel een ticketingsysteem aanwezig is, maar dat dit ticketingsysteem niet gebruikt wordt voor mutaties in AFAS. Wij geven u in overweging om het proces van toekennen, verwijderen en wijzigen van rechten en rollen via het ticketingsysteem te laten verlopen, zodat een consistente uitvoering en documentatie van het proces worden gewaarborgd.
Ten aanzien van het verwijderen van rechten en accounts vernamen wij dat er geen automatische signaalfunctie meer is ingericht dat een account geblokkeerd moet worden nadat een medewerker uit dienst treedt. Wij vernamen dat dit in Compas wel was ingericht.

NOTITIE

Managementletter 2018
22 januari 2019

Wij adviseren u om de signaalfunctie van (naderende) uitdiensttredingen binnen AFAS in te schakelen en te koppelen aan uw ticketingsysteem, zodat er accounts tijdig geblokkeerd kunnen worden wanneer medewerkers uit dienst treden. Dit voorkomt dat medewerkers nog toegang kunnen verkrijgen tot AFAS nadat ze uit dienst zijn getreden.

Reactie
In de loop van 2019 zal de mogelijkheid worden onderzocht om voor mutaties in AFAS het ticketingsysteem van de servicedesk te gebruiken zal of dat er ander soortige vastlegging nodig is. Aan de workflow "uitdiensttreding" zal een signaal worden toegevoegd richting de servicedesk om het account te blokkeren.

User access: User review
Binnen AFAS worden rechten toegekend op basis van standaardprofielen, optioneel kunnen losse rechten toegekend worden. Wij vernamen dat er nog niet periodiek wordt getoetst of de toegekende rechten nog aansluiten op de gewenste situatie. Deze review omvat (i) het periodiek toetsen of de juiste profielen aan medewerkers zijn gekoppeld en (ii) toetsen of de profielen qua samenstelling van rechten aansluiten op de gewenste situatie. In dit kader adviseren wij u een functiematrix op te stellen waarin per functiegroep is opgenomen welke profielen en rechten toegekend mogen worden; dit vormt het toetsingskader voor een periodieke review. Tevens adviseren wij u in dit kader om ongebruikte profielen, waarvan wij vernamen dat daar veel van zijn, te verwijderen, zodat de review qua scope beperkt blijft. Wij wisselen graag verder met u van gedachten over de manier waarop u vorm kunt geven aan de periodieke user review

Reactie
Wij zullen periodiek (elk halfjaar) toetsen of de toegekende rechten nog aansluiten op de gewenste situatie. Hierbij zal gebruik worden gemaakt van een functiematrix.

User access
Generieke accounts betreffen accounts die niet aan natuurlijke personen te koppelen zijn; dit kunnen bijvoorbeeld leveranciersaccounts of accounts die gebruikt worden voor systeemtaken (bijv. voor de scanmodule binnen AFAS) zijn. Het gebruik van generieke accounts moet zo veel mogelijk voorkomen worden, omdat de acties binnen dit account niet herleidbaar zijn naar een natuurlijk persoon (waarmee er misbruik gemaakt zou kunnen worden van dit account). Wanneer er wel generieke accounts benodigd zijn, is het van belang dat de rechten op het desbetreffende account beperkt blijven tot de strikt noodzakelijke. Wij adviseren u om periodiek te toetsen of er sprake is van overbodige generieke accounts en bij de benodigde generieke accounts te toetsen of de toegekende rechten niet verder reiken dan strikt noodzakelijk.

Reactie
Deze review zullen wij meenemen in de periodieke controle op de toegekende rechten.

User Access: Superusers (functioneel beheerders)
Het functioneel beheren van de applicatie is momenteel belegd bij uw assistent controllers. De functioneel beheerders kunnen door hun rechten ingerichte functiescheidingen doorbreken en kunnen functionele instellingen binnen AFAS aanpassen; dit is ook noodzakelijk om de applicatie te kunnen beheersen. Wij adviseren u om enkele kritieke activiteiten te definiëren, zoals het muteren van crediteurstamgegevens, en periodiek te toetsen of deze kritieke activiteiten niet (onterecht) zijn uitgevoerd door uw functioneel beheerders.
Indien er sprake is van generieke accounts (zoals testaccounts) met vergevorderde rechten adviseren wij u om de logging van deze accounts te betrekken in de periodieke review.

NOTITIE

Managementletter 2018
22 januari 2019

Reactie
Nadat AFAS volledig is “geland” zullen wij deze kritieke activiteiten definiëren en periodiek toetsen of deze activiteiten niet (onterecht) zijn uitgevoerd door de functioneel beheerders.

Wijzigingsbeheer
Aangezien er sprake is van een cloudoplossing ligt het algemene onderhoud van de applicatie bij uw softwareleverancier AFAS. Desalniettemin liggen er mogelijkheden bij WNK als gebruikersorganisatie om instellingen in AFAS aan te passen. Dit kan uw interne beheersing beïnvloeden omdat deze instellingen ook betrekking hebben op bijvoorbeeld de inrichting van uw workflows. Wij vernamen dat er nog geen geformaliseerd beleid is voor het wijzigingsbeheer. Dit beleid omvat normaliter het ontwikkelen van wijzigingen in een aparte omgeving, het testen daarvan en het verkrijgen van goedkeuring door de applicatie-eigenaar. Momenteel is het wijzigingsbeheer georganiseerd in een informeel proces.
Wij adviseren u om een formeel beleid op te stellen en uw wijzigingsbeheerproces daarop in te richten. Wij adviseren u tevens om het wijzigingsbeheer in te regelen in het reeds bestaande ticketingsysteem, zodat u achteraf door middel van de documentatie in het ticketingsysteemkunt toetsen of wijzigingen worden doorgevoerd conform het ingestelde beleid. Wij wisselen graag met u van gedachten over de manier waarop u dit praktisch kunt inrichten.

Reactie
Nadat AFAS volledig is “geland” zullen wij een formeel beleid op te stellen en ons wijzigingsbeheerproces daarop in te richten. Op dit moment zijn er nog teveel wijzigingen en zal dit proces vastlopen bij teveel bureaucratie.

Cybersecurity
Het belang van afdoende cybersecuritymaatregelen neemt toe als gevolg van een grotere afhankelijkheid van IT en aangescherpte wet- en regelgeving (zoals GDPR). Wij vernamen dat er nog geen beleid is om periodieke pen-tests uit te laten voeren op uw IT-omgeving. Wij adviseren u om bij de eerst volgende actualisatie van uw cyberrisicoanalyse te evalueren of er noodzaak bestaat om aanvullende maatregelen te treffen.

Reactie
Wij zien het belang van het uitvoeren van periodieke pen-tests. In 2019 zal hiervoor een leverancier worden gezocht en een frequentie worden bepaald.