Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Onderzoek AFAS autorisatieconcept

Definitief

Colofon

Titel	Onderzoek AFAS autorisatieconcept
Uitgebracht aan	Directeur Caribisch Nederland
Datum	8 november 2021
Kenmerk	2021-0000217272
Referentienummer	2021-BZK-001

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

De "unit Finance" van het Openbaar Lichaam St Eustatius (afgekort OLE) heeft een nieuw informatiesysteem (AFAS OLE) ingevoerd met behulp van een consultant van AFAS. AFAS OLE bestaat uit de AFAS-modules HRM, Payroll en Finance. Dit systeem wordt gebruikt voor de ondersteuning van de processen omtrent personeelszaken, salarisverwerking en financiën (HRM, Payroll en Finance).

Het project voor de invoering van AFAS OLE is gestart in 2018 en in maart 2020 afgerond. De helpdesk van OLE dient als aanspreekpunt met de softwareleverancier, AFAS. Het IT-beleid wordt in samenwerking met Rijksdienst Caribisch Nederland (RCN) uitgewerkt. In lijn daarmee zal het IT Beheer door OLE opnieuw worden ingericht. Na implementatie van informatiesysteem AFAS OLE is door de directeur bedrijfsvoering, openbaar lichaam Sint-Eustatius de wens uitgesproken voor een onderzoek. De directeur heeft hiervoor een verzoek gedaan bij het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK), de opdrachtgever, Directeur Caribisch Nederland bij DGKR heeft vervolgens aan de Auditdienst Rijk (ADR) gevraagd om een onderzoek te doen naar de processen omtrent het gebruikersbeheer.

1.2 Doelstelling en onderzoeksvragen

De doelstelling van dit onderzoek was een nulmeting uitvoeren op het gebruikersbeheer van 3 instanties op St Eustatius die gebruik maken van AFAS voor HRM, Payroll en Finance. Met als doel OLE-inzicht te geven in welke processen verbeterd/opgezet moeten worden om tot een beheerst identiteits- en gebruikersbeheerproces te komen. De 3 instanties waar het onderzoek betrekking op heeft zijn het Openbaar Lichaam Eustatius, de luchthaven en zeehaven.

De volgende onderzoeksvragen worden beantwoord in deze rapportage:

1. Tot en met welk volwassenheidsniveau van de twee identiteits- en toegangsbeheernormen hebben de AFAS-administraties voor zee, lucht en OLE de voorgeschreven bewijsdocumenten beschreven, geaccordeerd en ingevoerd?
2. Welke verbeteringen zijn mogelijk in het gebruikersbeheer voor de AFAS-administraties voor zee, lucht en OLE ten behoeve van het behalen van een hoger volwassenheidsniveau?

1.3 Afbakening

De scope is het gebruikersbeheer van drie AFAS-systemen die door het openbaar lichaam Sint-Eustatius gebruikt worden. Het gaat om de volgende AFAS-systemen:

1.	OLE	Openbaar Lichaam Sint-Eustatius
2.	ZEE	Openbaar Lichaam Sint-Eustatius – Zeehaven
3.	LUCHT	Openbaar Lichaam Sint-Eustatius - Luchthaven

Hierbij zijn twee normen uit "identiteits- en toegangsbeheer" van het NBA-volwassenheidsmodel-informatiebeveiliging van januari 2019 onderzocht. Het gaat om de norm ID.01 Access Rules en ID.02 Access rights administration. Het onderzoek is vanaf het laagste niveau van start gegaan en zodra er van een niveau bewijsstukken ontbraken zijn de overige bewijsstukken van dit niveau en het daaropvolgende niveau nog verwerkt en zijn de andere niveaus buiten scope van dit onderzoek geplaatst.

Het onderzoek is uitgevoerd op basis van informatie/documentatie die is aangeleverd door het centrale contactpersoon die voor de 3 dienstonderdelen het aanspraakpunt is. Daarnaast zijn er interviews afgenomen met de betrokkenen in de processen om vast te stellen dat wat beschreven staat in de bewijsdocumenten ook is ingevoerd. De opdracht is uitgevoerd in opzet (geaccordeerde beschrijving) en bestaan (invoering).

1.4 Leeswijzer

In het hoofdstuk 2 staat een overzicht van de bevindingen beschreven. De bevindingen zijn verdeeld in 2 paragrafen (Access Rights Administration en Access Rules). De paragrafen beginnen met een samenvatting van de bevindingen en vervolgens zijn per niveau uit het volwassenheidsmodel de bevindingen verder uitgeschreven. Met dit hoofdstuk wordt antwoord gegeven op onderzoeksvraag 1.

In hoofdstuk 3 worden aanbevelingen gegeven. De aanbevelingen zijn verdeeld in de paragrafen Access Rights Administration en Access Rules. Deze aanbevelingen geven antwoord op onderzoeksvraag twee.

In hoofdstuk 4 is de verantwoording van het onderzoek opgenomen.

2 Bevindingen (onderzoeksvraag 1)

In dit hoofdstuk gaan wij in op de bevindingen van ons onderzoek. Het hoofdstuk is verdeeld in de paragrafen Access rights administration en Access Rules. Per onderwerp is er eerst een antwoord op de onderzoeksvraag beschreven, in de daaropvolgende paragraaf staan de bevindingen die het antwoord hebben vormgegeven verder uitgewerkt. De bevindingen staan hierin per niveau uit het volwassenheidsmodel beschreven.

2.1 Antwoord Onderzoeksvraag 1: Access Rights Administration

Er wordt gebruik gemaakt van de standaard AFAS-workflows voor het indienst-, uitdienst- en doorstroom-proces. Een verdere uitwerking van het proces tot werkinstructies/procedures/beleid ontbreekt. De workflows zijn voorzien van een vierogen principe door verschillende autorisatierollen stappen uit het proces te laten uitvoeren (opzet). Echter is uit ons onderzoek naar voren gekomen dat een medewerker de rollen bezit om beide goedkeuringen in het proces te geven en hiervan gebruik heeft gemaakt. Hiermee is het vierogen principe doorbroken (bestaan).

Het AFAS-systeem houdt van ieder doorlopen workflow (Indienst, doorstroom en uitdienst) een administratie bij, hierdoor is een overzicht te maken welke medewerkers de verschillende stappen per workflow hebben doorlopen. Dit zijn alleen de stappen die binnen de AFAS-applicatie worden doorlopen, de stappen die buiten de applicatie om plaatsvinden staan niet in een centrale administratie opgenomen. Hierdoor is niet inzichtelijk wie de gebruikersaccount/rollen heeft aangevraagd bij de OOB-manager/HR-functionaris.

Voor de inrichting van de autorisatierollen/functies is geen risicoanalyse uitgevoerd door OLE. De toegangsrechten worden uitgeven door het koppelen van een autorisatierol aan de gebruiker. De autorisatierollen zijn volgens de standaard inrichting van AFAS, met een aantal uitzonderingen voor specifieke functies van OLE.

Medewerkers die niet meer op de payroll staan worden automatisch van de “medewerker” rol afgehaald, waardoor het gebruikersaccount niet meer als standaardeindgebruiker kan inloggen. Echter is uit ons onderzoek gebleken dat een gebruikersaccount van een medewerker nog de rollen bevatte om toegang te krijgen tot de AFAS-Profit module na de uitdiensttredingsdatum. Met de huidige inrichting en uitvoering ontbreken er stukken om aan de norm van niveau 2 te voldoen, hierdoor wordt dit niveau niet bereikt.

2.1.1 *Access Rights Administration: Niveau 1 Initial*[1]

Maturity Level 1 (Initial) Controls are not, or only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	
Requirement	**Situation OLE**
1. Absence of policy for user accounts and related privileges.	**Opzet en bestaan** Niveau 1 is het niveau waarbij er nog geen policy's, functiescheiding en controles in plaats zijn. Dit is een niveau dat bij systemen waar gebruikersaccounts gebruikt worden voldaan wordt zonder het hebben van een proces, beschrijving of andere proces ondersteunende stukken. Derhalve wordt aan dit niveau voldaan.
2. No administration procedure for users and access groups(roles).	
3. Access rights are granted and revoked on an ad hoc basis, depending on individuals.	
4. Users could access more information than based on 'need-to-know/have' principle.	

2.1.2 *Access Rights Administration: Niveau 2 Repeatable*[1]

Maturity Level 2 (Repeatable) Controls are in place and executed in a structured and consistent, but informal, manner.	
Requirement	**Situation OLE**
5. Informal policy in place on all accounts and access rights (internal, external, administrators), and all circumstances (normal, emergency).	**Opzet** OLE beschikt niet over een procesbeschrijving. OLE gebruikt de standaard AFAS workflows voor indienst, doorstroom en uitdienst processen. Van deze workflows is een beschrijving in de applicatie AFAS opgenomen. Verdere documentatie over het proces en de borging hiervan op de werkvloer ontbreekt. Ook geen procesbeschrijving over een verschillende aanpak van eindgebruikers, externen en beheerders *Calamiteit* Daarnaast is het onder de geïnterviewden niet bekend of er een noodproces is om in geval van een calamiteit snel autorisaties toe te kennen of af te nemen. **Bestaan** Deze norm gaat over het hebben van specifieke beleidstukken (Opzet).
6. An administration procedure for accounts and related privileges has been defined but not formalized.	**Opzet** Er is geen proces/beleid voor het bijhouden van een administratie voor accounts en gerelateerde privileges. **Bestaan** Er is in de AFAS-applicatie een overzicht van de doorlopen workflows. Hiermee is er een administratie die geautomatiseerd wordt bijgehouden. Echter kan indien er bij het opstellen van het proces/beleid

[1] De processen voor ZEE, LUCHT en OLE zijn één keer onderzocht doordat het een uniform proces betreft. Zie paragraaf 4.1 voor meer informatie.

	er andere vereisten bijkomen, dat deze administratie niet toereikend is en uitgebreid moet worden om meer velden te administreren. Zoals bijvoorbeeld de aanmelder die de wijziging-/accountaanvraag indient bij de HR-functionaris/manager OOB.
7. Access to information is defined as a result of risk management, and complies with policy and security demands.	**Opzet en bestaan** Er is geen risicoanalyse gemaakt voor het huidige gebruikte autorisatieontwerp.
8. Accounts and related access rights are blocked/revoked if a user resigns or is fired.	**Opzet** Er wordt gebruik gemaakt van de uitdienst workflow beschrijving die in de AFAS-applicatie beschikbaar is. Bij uitdiensttreding wordt een medewerker van de payroll afgehaald, het systeem voert elke dag een controle uit of een medewerker nog onderdeel is van de payroll, indien dit niet het geval is wordt de medewerkersrol verwijderd. Op deze manier herkent het systeem de gebruiker niet meer als medewerker en kan deze niet meer inloggen op het portaal en profit modules. Volledig verwijderen/blokkeren van gebruikers gebeurt niet aangezien dit zou leiden tot definitieve uitsluiting van deze persoon tot alle AFAS-applicaties. Bijvoorbeeld de module voor het reageren op vacatures zou dan in het vervolg niet meer door de ex-medewerker geraadpleegd kunnen worden. **Bestaan** Tijdens een interview met OLE is een observatie uitgevoerd op een medewerker die uitdienst is gemeld. Deze medewerker beschikte nog over toegang tot de profit omgeving. De uitdiensttreder beschikt hierdoor nog over zijn rollen en bijbehorende rechten binnen profit na de uitdiensttredingsdatum.

2.1.3 Access Rights Adminisration: Niveau 3 Defined[1]

Maturity Level 3 (Defined) Controls are documented and executed in a structured and formal manner. Execution of control can be proved, is tested and effective.	
Requirement	**Situation OLE**
9. Policy and procedures for all accounts and access rights/privileges are defined, documented, formalized and communicated.	**Opzet** OLE heeft in een interview aangegeven niet te beschikken over een procedure/beleid voor het gebruikersbeheer omtrent AFAS. **Bestaan** Deze norm gaat over het hebben van specifieke beleidstukken/procedures (Opzet).
10. Includes approval procedure outlining the data/system owner granting access privileges.	**Opzet en bestaan** OLE beschikt niet over een mandaatlijst met wie goedkeuringen mag/moet verstrekken vooraf het uitgeven van autorisaties.
11. Adequate SoD in place for requesting, approving, implementing or revoking user access rights.	**Opzet** De workflows voor indienst, doorstroom en uitdienst van medewerkers hebben een functiescheiding tussen de rollen Business Unit Manager OOB en salarisadministratie. Deze processen zien er als volgt uit: - Gebruikers met de rol management kunnen een verzoek inschieten bij Unit Manager OOB - Unit Manager OOB beoordeelt aanvraag

	- Bij akkoord van Unit Manger OOB komt verzoek binnen bij salarisverwerking - Na goedkeuring door salarisverwerking is de workflow doorlopen en voert het systeem de aanvraag uit. **Bestaan** Uit ons onderzoek blijkt dat één medewerker beide goedkeuringen uitvoert, omdat deze medewerker beide rollen/functies bezit (Unit Manager OOB en Salarisverwerking). De functiescheiding in de AFAS-workflow is hierdoor niet van kracht.
12. Employee access rights are implemented through role-based access	**Opzet** Er is geen autorisatiematrix of andere beschrijving van een SOLL-situatie beschikbaar. **Bestaan** Er wordt gebruik gemaakt van rollen bij het toebedelen van rechten. Er zijn veelal standaard AFAS-rollen gebruikt. Daarnaast zijn er ook specifieke rollen aangemaakt die de autorisaties voor specifieke functies verstrekken. Deze specifieke rollen zijn veelal in gebruik door één enkele eindgebruiker. Voor het bestaan is enkel gekeken naar de rollen/functies die in het AFAS-systeem zijn gekoppeld aan actieve medewerkers, de ongebruikte rollen zijn niet bekeken. Omdat er nog geen risicoanalyse en eigen autorisatiematrix is vormgegeven, kan het zijn dat de huidige configuratie/verdeling van autorisaties volgens de AFAS standaard rollen/functies niet past bij de wensen van de organisatie.

2.1.4 Access Rights Administration: Niveau 4 en 5

Bij niveau 2 miste er al benodigde informatie derhalve is niveau 3 nog onderzocht en is niveau 4 en 5 buiten scope van het onderzoek geplaatst.

2.2 Antwoord Onderzoeksvraag 1: Access Rules

Bij het beheer van access rules wordt voornamelijk gebruik gemaakt van de expertise van AFAS. Zowel de processen voor het aanmaken van gebruikersaccounts als de inrichting voor de meeste functies/rollen zijn standaard AFAS-inrichtingen.

Er zijn geen procesbeschrijvingen, een autorisatiematrix, beleidsstukken of andere ondersteunende beschrijvingen aanwezig voor het op een uniforme/gestructureerde manier verwerken van een aanvraag, mutatie en verwijdering van gebruikersaccounts.

De gebruikersaccounts die opgevoerd zijn in AFAS, zijn te herleiden naar een natuurlijk persoon door het naam veld dat ingevuld is bij de gebruikersaccounts. Voor het loggen en monitoren van gebruikersactiviteiten mist nog een analyse naar welke activiteiten risicovol zijn om inzage te krijgen voor welke activiteiten monitoring ingericht moet worden. Met de huidige inrichting en uitvoering ontbreken er stukken om aan de norm van niveau 2 te voldoen, hierdoor wordt dit niveau niet bereikt.

2.2.1 Access Rules: Niveau 1 Initial[1]

Maturity Level 1 (Initial) Controls are not, or only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	
Requirement	**Situation OLE**
13. No policy to control access to information.	**Opzet en bestaan** Niveau 1 is het niveau dat er nog geen policy's, autorisatie matrices beschreven zijn en dat activiteiten niet/nauwelijks te herleiden zijn naar natuurlijke personen. Dit is een niveau dat bij systemen waar gebruikersaccounts gebruikt worden voldaan wordt zonder het hebben van een proces, beschrijving of andere proces ondersteunende stukken. Derhalve wordt aan dit niveau voldaan.
14. Absence of complete SOLL authorization matrix	
15. Not all user activities can be traced to uniquely identifiable users.	

2.2.2 Access Rules: Niveau 2 Repeatable[1]

Maturity Level 2 (Repeatable) Controls are in place and executed in a structured and consistent, but informal, manner.	
Requirement	**Situation OLE**
16. Informal policy implemented about access to information.	**Opzet** OLE maakt gebruik van de standaard AFAS workflows voor indienst/doorstroom/uitdienst processen. Dit proces ziet er als volgt uit: - Gebruikers met de rol management kunnen een verzoek inschieten bij Unit Manager OOB - Unit Manager OOB beoordeelt de aanvraag - Bij akkoord van Unit Manger OOB komt het verzoek binnen bij salarisverwerking - Na goedkeuring door salarisverwerking is de workflow doorlopen en wordt de aanvraag doorgevoerd. De beschrijving geeft aan hoe het systematisch is ingesteld om een gebruikersaccount aan te maken. Er is niet beschreven welke handelingen OLE moet uitvoeren bij het aanvragen, beoordelen en goedkeuren. **Bestaan** Deze norm gaat over het hebben van specifieke beleidstukken (Opzet).
17. A SOLL authorization matrix	**Opzet** Er is geen autorisatiematrix aanwezig.

has been defined but Not formalized.	**Bestaan** Deze norm gaat over het bezitten van een autorisatiematrix (Opzet).
18. Activities of high privilege users are traceable to uniquely identifiable users.	**Opzet** OLE heeft geen beeld welke autorisaties als "high privilege" moeten worden gezien. Daarom is er geen specifieke logging op te vragen waarmee inzichtelijk te maken is of activiteiten van gebruikers met "high privilege" herleidbaar zijn naar een gebruikersaccount. **Bestaan** Er is een overzicht van de AFAS-gebruikersaccounts beschikbaar. Hierin staan de gebruikersaccounts gekoppeld aan de naam van de eigenaar van het gebruikersaccount.
19. Defined roles and user access rights are in line with business needs.	**Opzet** OLE beschikt niet over een autorisatiematrix of inrichtingsdocument waarin een vertaling van de eisen vanuit de bedrijfsvoering gemaakt is naar autorisaties. **Bestaan** De groepen zijn gelabeld met de bijhorende functienaam, hierdoor is te zien welke functie bij welke autorisatiegroep hoort. Voor deze groepen is veelal gebruik gemaakt van AFAS-standaard rollen. De afweging of de AFAS-standaard rollen in lijn zijn met de bedrijfsbenodigdheden is niet vastgelegd.
20. Job requirements are attached to user identities	**Opzet en bestaan** Er is geen beschrijving of andere vorm van bewijs dat er eisen (Screening/competenties etc.) aan de gebruikers/functies zijn gesteld voor het toebedeeld krijgen van autorisaties.

2.2.3 Access Rules: Niveau 3 Defined[1]

Maturity Level 3 (Defined) Controls are documented and executed in a structured and formal manner. Execution of control can be proved, is tested and effective.	
Requirement	**Situation OLE**
21. Policy and SOLL matrix for access rights/privileges of users and groups (roles) have been defined, documented, formalized, communicated and punctually updated.	**Opzet** OLE beschikt niet over een beleid en SOLL-matrix voor toegangsrechten/privileges. **Bestaan** Deze norm gaat over het hebben van specifieke beleidstukken/matrices (Opzet).
22. Identification, authentication and authorization of users implemented and enforced.	**Opzet** OLE maakt gebruik van de standaard AFAS workflows voor indienst/doorstroom/uitdienst processen. Dit proces ziet er als volgt uit: - Gebruikers met de rol management kunnen een verzoek inschieten bij Unit Manager OOB - Unit Manager OOB beoordeelt de aanvraag - Bij akkoord van Unit Manger OOB komt het verzoek binnen bij salarisverwerking - Na goedkeuring door salarisverwerking is de workflow doorlopen en wordt de aanvraag doorgevoerd. **Bestaan** De beoordeelde procesuitvoeringen vallen buiten de vooraf bepaalde onderzoeksperiode aangezien er in deze periode geen indiensttreder/doorstromer/uitdiensttreder hebben plaats gevonden. Om toch een beeld te vormen zijn een indiensttreder/doorstromer en uitdiensttreder geselecteerd

	die eerder in 2021 hebben plaatsgevonden. De AFAS workflows zijn gevolgd zoals deze geprogrammeerd zijn. Echter beschikt één enkele medewerker over de rollen Business Unit Manger OOB en salarisverwerking. In de drie geselecteerde gevallen heeft dezelfde medewerker het gehele proces doorlopen en is er geen vier ogen principe gebruikt. Een autorisatiematrix is er momenteel niet waarin de beoogde scheiding tussen de rollen vastgelegd wordt. OLE heeft in een interview aangeven dat het niet wenselijk is dat 1 persoon alle handelingen uit het proces kan uit voeren.
23. Access rights derived from the SOLL matrix are frequently compared to the IST situation.	**Opzet en bestaan** Er is geen proces ingericht, hierdoor vindt er geen review/vergelijking plaats van de uitgegeven autorisaties.
24. Activities of users are traceable to uniquely identifiable users.	**Opzet** Er is geen beleid of andere beschrijving aanwezig die de eis van het herleiden tot een natuurlijk persoon aan de gebruikersaccounts oplegt. **Bestaan** Er is een overzicht van de actieve gebruikers binnen AFAS beschikbaar. Wij hebben vastgesteld dat gebruikersaccounts zijn terug te herleiden naar een natuurlijk persoon op basis van de gekoppelde naam bij het account.
25. User identities and access rights are maintained in a central repository.	**Opzet** Geen beleid/proces aanwezig waarin de administratie van toegangsrechten beschreven staat. **Bestaan** De AFAS-applicatie slaat de gebruikers met functies op in een tabel die te downloaden is naar een Excel format. Hiermee is een overzicht te genereren dat inzichtelijk maakt welke rollen/functie ieder gebruikersaccount bezit.

2.2.4 Access Rules: Niveau 4 en 5

Bij niveau 2 miste er al benodigde informatie derhalve is niveau 3 nog onderzocht en is niveau 4 en 5 buiten scope van het onderzoek geplaatst.

3 Aanbevelingen (Onderzoeksvraag 2)

In dit hoofdstuk staan de aanbevelingen weergeven. De aanbevelingen zijn verdeeld in de Access Rights Administration en Access Rules, zodat deze aansluiten op hoofdstuk twee. Omdat de aanbevelingen in enkele gevallen voor beide normen van toepassing zijn, is er gekozen om deze aanbeveling bij de paragraaf op te nemen waar de auditors deze het meest passend vonden.

3.1 Antwoord Onderzoeksvraag 2: Access Rights Administration

Om de administratie van autorisaties voor de onderzochte AFAS-systemen naar volwassenheidsniveau drie te brengen hebben wij een vijftal aanbevelingen. De aanbevelingen zijn middels een nummer aan de normen gekoppeld (zie paragraaf 2.1.1 t/m 2.2.4).

1. Stel een beleidsdocument op waarin alle eisen aan de autorisaties en het beheren (procesbeschrijvingen) ervan staan vastgelegd. Formaliseer dit document en communiceer dit met de betrokkenen. Hierin kunnen verwijzingen opgenomen worden naar de verschillende documenten die in de aanbeveling 1 en 3 bij Access Rules zijn genoemd. (5, 9)

2. Analyseer of de workflow administratie van AFAS de gewenste informatie bevat om sturing te kunnen geven om tot beheerste processen (Indienst, uitdienst en doorstroom) te komen en pas eventueel de workflow administratie aan. Leg daarnaast vast hoe deze administratie beheert (aangevuld/bijgehouden) en gebruikt (analyses) dient te worden. (6, 25)

3. Voer een risicoanalyse/procesanalyse uit om inzichtelijk te maken welke risico's er gepaard gaan met de toegang tot informatie. Hiermee kan een inschatting gemaakt worden welke informatie benodigd is voor een functie en/of er rest risico's overblijven waarop mitigerende maatregelen getroffen moeten worden en wordt voldaan aan overig beleid en security vereisten. (7)
    a. Vergelijk de uitkomsten van de risicoanalyse/procesanalyse met de huidige inrichting van AFAS-standaard rollen en de beperkte hoeveelheid specifieke rollen, om inzage te krijgen of de toegang die deze rollen verschaffen gewenst is en pas bij verschillen aan. (12)

4. Stel een mandaatlijst op ten behoeve van het gebruikersbeheerproces. Daarop staat wie aanvragen/wijzigingsverzoeken voor gebruikersaccounts mag indienen en wie deze aanvragen goed mag keuren voor doorvoering. (10)

5. Monitor of bij uitdiensttreding/doorstroom de juiste autorisaties tijdig worden verwijderd. Pas indien nodig het proces/programmatuur aan indien het vaker voor blijft komen dat een medewerker autorisaties behoudt die al verwijderd hadden moeten zijn. (8)

3.2 Antwoord Onderzoeksvraag 2: Access Rules

Om de toegang tot data en uitvoering van processen omtrent AFAS naar volwassenheidsniveau drie te brengen hebben wij een viertal aanbevelingen. De aanbevelingen zijn middels een nummer aan de normen gekoppeld (zie paragraaf 2.1.1 t/m 2.2.4)

1. Stel een procedure op voor het gebruikersbeheer waarin onder andere de volgende onderwerpen uitgewerkt zijn (16):
    a. Indienst, uitdienst en doorstroom van medewerkers; (8, 11, 22)
    b. Noodproces voor versneld aanvragen/innemen van autorisaties; (8)
    c. Enveloppe procedure voor accounts met de hoogste autorisaties; (8)
    d. Review op de uitgegeven autorisaties, om periodiek inzage te krijgen of gebruikers nog steeds de autorisaties nodig hebben voor het uitoefenen van hun functie. (23)
    e. Monitoring van gebruik high privilege accounts. (18, 24)

2. Analyseer of de procesinrichting in AFAS aan de eisen van de organisatie voldoet en ondersteunend is voor de processen die gebruik maken van de applicatie. Pas waar nodig de workflows in AFAS aan om in lijn te zijn met de organisatiebenodigdheden. (19)

3. Voer een risicoanalyse uit van de processen die gebruik maken van de AFAS-applicatie. Stel op basis van de uitkomsten van de risicoanalyse de volgende producten op:
    a. Een autorisatiematrix, waarin zichtbaar is welke autorisaties/rollen niet met elkaar mogen kruisen met als doel om tot een gewenste functiescheiding te komen voor de processen. Denk hierbij tevens na over de beoogde functiescheiding voor het beheren van gebruikers en de AFAS-applicatie. (17, 21, 22)
    b. Monitoringsplan, met hierin de risicovolle handelingen in de processen waarop logging en monitoring plaats moet vinden. (18, 24)
    c. Functieprofielen, een lijst met benodigde kennis en/of screening voordat een gebruiker bepaalde autorisaties toebedeeld mag krijgen. (20, 22)

4. Informeer medewerkers en leidt ze op zodat iedereen op de hoogte is van de procesgang en op een uniforme manier de processen doorloopt. (1-25)

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

We zijn tot de bevindingen gekomen door het Informatiebeveiliging Volwassenheidsmodel te vertalen naar een aantal essentiële opzet documenten en benodigde voorbeelden die laten zien dat de inrichting en uitvoering zoals beschreven is ingevoerd. Deze vertaling is in een documentatieverzoek beschreven en met OLE gedeeld. OLE heeft de gevraagde gegevens aangeleverd en vervolgens is er een documentstudie uitgevoerd. En zijn er vervolgens interviews uitgevoerd om meer informatie te verkrijgen over de processen/inrichting en uitvoering. De onderzoeksperiode was van 1-3-2021 t/m 15-5-2021.

Daarmee hebben we de overeengekomen werkzaamheden conform de opdrachtbevestiging uitgevoerd. Na het uitvoeren van de werkzaamheden zijn op 18-5-2021 de bevindingen afgestemd met de AFAS-contactpersoon en het centrale aanspreekpunt voor AFAS.

De inhoudelijke afstemming van dit rapport heeft plaatsgevonden met de gedelegeerd opdrachtgever. In de bijgevoegde managementreactie heeft de gedelegeerd opdrachtgever aangegeven hoe de bevindingen/aanbevelingen opgepakt worden.

Het gebruikersbeheer onderzoek bij OLE is uitgevoerd voor de instanties OLE (Openbaar Lichaam Sint-Eustatius), ZEE (OLE Zeehaven) en LUCHT (OLE Luchthaven). Tijdens het onderzoek kwam aan het licht dat al deze instanties dezelfde procesgang/contactpersoon hanteren voor het beheren van gebruikers voor de AFAS-applicatie. Daarom zijn de bevindingen op de drie instanties van toepassing en zijn de bestaanschecks per proces eenmaal uitgevoerd.

Het onderzoek is als het volgt afgebakend:

- Twee normen uit “identity & access management” van het NBA-volwassenheidsmodel-informatiebeveiliging van januari 2019 zijn onderzocht. Het gaat om de norm ID.01 Access Rules en ID.02 Access rights administration.
- Het onderzoek voor beide normen is stopgezet na niveau 3 omdat er documenten bij niveau 2 van het volwassenheidsmodel ontbraken. Het onderzoeken van niveau 3 is gedaan om gerichter aanbevelingen te kunnen geven.
- De selectie voor de bestaanscontrole van de processen voor indienst, uitdienst en doorstroom van medewerkers is buiten de onderzoeksperiode gevallen, omdat er tijdens de onderzoeksperiode geen indienst-, uitdienst- en doorstromers zijn geweest. Om een beeld te kunnen vormen over of de processen uitgevoerd zijn zoals beschreven is er gekozen om de selectie van eerder in 2021 te laten vallen.

Onderzoeksvraag 1 is beantwoord door het normenkader naast de verkregen documentatie en interviews te leggen. Onderzoeksvraag 2 is beantwoord door te kijken welke documenten er volgens het volwassenheidsmodel nog verder uitgewerkt moeten worden of ontbreken. Daarnaast is gekeken naar de uitvoering van de processen binnen OLE en is deze kennis meegenomen in het beschrijven van de aanbevelingen.

4.2 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

4.3 Verspreiding rapport

De opdrachtgever, directeur Caribisch Nederland, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent de uitkomsten anders interpreteert dan bedoeld.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (ADR) een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van rapporten die de ADR heeft uitgebracht en plaatst dit overzicht op www.rijksoverheid.nl.

5 Ondertekening

Den Haag, 8 november 2021

IT-Auditor Auditdienst

Auditdienst Rijk

Bijlage 1: de Managementreactie

Met Zwart staan de aanbevelingen uit hoofdstuk 3 weergegeven en met rood de reactie van de directeur bedrijfsvoering, openbaar lichaam Sint-Eustatius.

Om de administratie van autorisaties voor de onderzochte AFAS-systemen naar volwassenheidsniveau drie te brengen hebben jullie een vijftal aanbevelingen. De aanbevelingen zijn middels een nummer aan de normen gekoppeld (zie paragraaf 2.1.1 t/m 2.2.4).

1. Stel een beleidsdocument op waarin alle eisen aan de autorisaties en het beheren (procesbeschrijvingen) ervan staan vastgelegd. Formaliseer dit document en communiceer dit met de betrokkenen. Hierin kunnen verwijzingen opgenomen worden naar de verschillende documenten die in de aanbeveling 1 en 3 bij Access Rules zijn genoemd. (5, 9)

Deze aanbeveling nemen we zeker in overweging. Echter wij denken een taak voor iemand met kennis van de autorisatietool om de groepen te auditen. Intern is het voorstel geopperd om functioneel beheer onder te brengen bij ICT met key-users op de afdelingen die AFAS gebruiken.
Hierdoor is een uniforme werkwijze eenvoudiger te realiseren en te borgen. Ik denk daar anders over en heb inmiddels KR op de hoogte gesteld van het feit dat we voornemens zijn een specialist AFAS voor 2 jaar in te huren die mede dit onderdeel oppakt. Positionering op Finance.

2. Analyseer of de workflow administratie van AFAS de gewenste informatie bevat om sturing te kunnen geven om tot beheerste processen (Indienst, uitdienst en doorstroom) te komen en pas eventueel de workflow administratie aan. Leg daarnaast vast hoe deze administratie beheert (aangevuld/bijgehouden) en gebruikt (analyses) dient te worden. (6, 25)

We zijn van mening dat de enige problemen die we hebben met deze flow die medewerkers betreft die handmatig in het systeem worden opgevoerd. Zoals er wordt aangegeven in het rapport blijven medewerkers in het systeem 'hangen' maar dit is met medewerkers die handmatig in het systeem zijn opgevoerd. AFAS is nu met de huidige (nieuwe) autorisatie structuur bezig (op basis van functie) om dit issue op te lossen. Door het volledige proces te automatiseren. P&O zal dan op basis van de functie de medewerker opvoeren met behulp van de 'flow'. Alleen P&O heeft dan deze mogelijkheid (sturing).

3. Voer een risicoanalyse/procesanalyse uit om inzichtelijk te maken welke risico's er gepaard gaan met de toegang tot informatie. Hiermee kan een inschatting gemaakt worden welke informatie benodigd is voor een functie en/of er rest risico's overblijven waarop mitigerende maatregelen getroffen moeten worden en wordt voldaan aan overig beleid en security vereisten. (7)
    a. Vergelijk de uitkomsten van de risicoanalyse/procesanalyse met de huidige inrichting van AFAS-standaard rollen en de beperkte hoeveelheid specifieke rollen, om inzage te krijgen of de toegang die deze rollen verschaffen gewenst is en pas bij verschillen aan. (12)

De standaard rollen van AFAS geven aan, op basis van functie wat de mogelijkheden voor dit profiel zijn. Deze standaard rollen (de blauwe autorisatie rollen) worden door AFAS onderhouden en veranderen per update omdat de nieuwe functionaliteiten op basis van module/functie worden geautoriseerd door beheerders van AFAS in

Nederland. Dit punt wordt dus voor het OLE een uitdaging. Iemand met de juiste autorisatie tool kennis zou dit onderwerp kunnen oppakken en een gedegen analyse maken per autorisatie rol.

4. Stel een mandaatlijst op ten behoeve van het gebruikersbeheerproces. Daarop staat wie aanvragen/wijzigingsverzoeken voor gebruikersaccounts mag indienen en wie deze aanvragen goed mag keuren voor doorvoering. (10)

Dit zal de applicatie beheerder worden van het OLE. In de tussentijd, zolang deze er nog niet is zal AFAS samen met de Manager Finance deze lijst beheren.

5. Monitor of bij uitdiensttreding/doorstroom de juiste autorisaties tijdig worden verwijderd. Pas indien nodig het proces/programmatuur aan indien het vaker voor blijft komen dat een medewerker autorisaties behoudt die al verwijderd hadden moeten zijn. (8)

AFAS is nu bezig om de alle autorisatiegroepen die gebruikt worden te koppelen aan de 'Functie'. Zodat een medewerker (geautomatiseerd) zijn autorisaties ontvangt bij indiensttreding. Hierbij wordt rekening gehouden met een selectie die kijkt of de medewerker een geldig contract heeft (einddatum van het salaris is 'leeg'; onbepaalde tijd of dat de einddatum verder dan vandaag ligt). Zodra dit filter niet gevuld kan worden doordat de einddatum voor vandaag ligt wordt de medewerker niet meer meegenomen in de selectie die de medewerker autorisatie toekent. Hier zal dus geen monitoring op nodig zijn zodra dit proces afgerond is. AFAS streeft ernaar dat dit proces eind November uiterlijk eind December afgerond is.

1.2 O2: Access Rules

Om de toegang tot data en uitvoering van processen omtrent AFAS naar volwassenheidsniveau drie te brengen hebben wij een viertal aanbevelingen. De aanbevelingen zijn middels een nummer aan de normen gekoppeld (zie paragraaf 2.1.1 t/m 2.2.4)

1. Stel een procedure op voor het gebruikersbeheer waarin onder andere de volgende onderwerpen uitgewerkt zijn (16):
    a. Indienst, uitdienst en doorstroom van medewerkers; (8, 11, 22)
    b. Noodproces voor versneld aanvragen/innemen van autorisaties; (8)

Het OLE heeft behoefte aan een 'vaste' applicatiebeheerder. Een AFAS Consultant zal altijd toegang hebben tot de autorisatie tool, maar nooit een besluit nemen of zonder toestemming autorisaties toekennen of blokkeren (autorisatie mutaties worden gelogd in het logboek van de omgeving van OLE) Als back-up beschikt het OLE over een ADMIN-account. Dit is het eerste account waarmee het systeem geactiveerd wordt, en dit is tevens de product eigenaar. Een medewerker die bekend is bij AFAS als beheerder (die dus ook incidenten/ support tickets aan mag vragen) kan vragen om een account te resetten met een ander mailadres. AFAS NL kan dan dit account resetten met een nieuwe gebruiker mocht er niemand meer het systeem/ autorisatietool in kunnen, dit is natuurlijk alleen in geval van nood.

    a. Enveloppe procedure voor accounts met de hoogste autorisaties; (8)
    b. Review op de uitgegeven autorisaties, om periodiek inzage te krijgen of gebruikers nog steeds de autorisaties nodig hebben voor het uitoefenen van hun functie. (23)
    c. Monitoring van gebruik high privilege accounts. (18, 24)

Er kan heel makkelijk gekeken naar de rollen die eindigen met ‘’applicatiebeheer’’, dit zijn de rollen die je kan categoriseren als high privilege. Op dit moment zijn dat alleen de Finance afdeling m.b.t. financieel applicatiebeheer en HR m.b.t. het applicatiebeheer van de personeelsadministratie.

2. Analyseer of de procesinrichting in AFAS aan de eisen van de organisatie voldoet en ondersteunend is voor de processen die gebruik maken van de applicatie. Pas waar nodig de workflows in AFAS aan om in lijn te zijn met de organisatiebenodigdheden. (19)

Er kan altijd een audit gedraaid worden op de huidige proces inrichting en indien nodig als deze gewijzigd moeten worden kan dit met de applicatie beheerder in dit geval met AFAS besproken worden.

3. Voer een risicoanalyse uit van de processen die gebruik maken van de AFAS-applicatie. Stel op basis van de uitkomsten van de risicoanalyse de volgende producten op:
    a. Een autorisatiematrix, waarin zichtbaar is welke autorisaties/rollen niet met elkaar mogen kruisen met als doel om tot een gewenste functiescheiding te komen voor de processen. Denk hierbij tevens na over de beoogde functiescheiding voor het beheren van gebruikers en de AFAS-applicatie. (17, 21, 22)
    b. Monitoringsplan, met hierin de risicovolle handelingen in de processen waarop logging en monitoring plaats moet vinden. (18, 24)
    c. Functieprofielen, een lijst met benodigde kennis en/of screening voordat een gebruiker bepaalde autorisaties toebedeeld mag krijgen. (20, 22)

4. Informeer medewerkers en leidt ze op zodat iedereen op de hoogte is van de procesgang en op een uniforme manier de processen doorloopt. (1-25)

Momenteel bekijken wij de aanbeveling van AFAS om alle werkprocessen in de voor OLE aangemaakte bibliotheek te publiceren.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag