Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20701 2500 ES Den Haag

HDBV
MPC 58 B
Postbus 20701
2500 ES Den Haag

C-DPOD
MPC 55 A
Postbus 90004
3509 AA Utrecht

Auditdienst Rijk
Clusters Defensie

Kalvermarkt 32
2511 CB Den Haag
Postbus 20701
2500 ES Den Haag
www.rijksoverheid.nl

Inlichtingen

Ons kenmerk
ADR/2015/124

Datum 4 februari 2015
Betreft Onderzoek gebruikersautorisaties PeopleSoft HRMS

In het kader van de wettelijke taak en daaruit voortvloeiende jaarrekeningcontrole en beheeronderzoeken, steunt de controlerend accountant van de Audit Dienst Rijk (ADR) op een betrouwbare IT- en IV-dienstverlening. Het PeopleSoft HRMS systeem is een belangrijk informatiesysteem in dit kader.

De HDBV als PME en de DPOD als PMH zijn verantwoordelijk voor de invulling van het PeopleSoft autorisatiebeheer voor de gebruikers. Zij hebben naar aanleiding van eerdere nota's en aanbevelingen een verbeterslag hierop doorgevoerd.

De ADR heeft in de afgelopen periode (oktober-december 2014) een onderzoek uitgevoerd naar de nieuwe opzet en inrichting van de gebruikersautorisaties. Hierbij is getoetst of de vertrouwelijkheid middels de toegang tot het informatiesysteem alsmede tot de vastgelegde gegevens in voldoende mate is geborgd.

Het afgelopen jaar zijn belangrijke stappen gezet ter verbetering van het autorisatie proces. Het besluitvormings- en toekenningsproces van de autorisaties was voorheen bij de Defensie onderdelen belegd. In de huidige inrichting is dit proces is nu onder verantwoordelijkheid van de HDBV centraal bij de DPOD belegd. Deze centrale inrichting heeft tot harmonisering en standaardisatie geleid.

Hoewel stappen zijn gemaakt in het vervolmaken van het autorisatiebeheer van de gebruikers organisatie is nog geen sprake van een aantoonbaar beheerst proces. De belangrijkste bevindingen uit dit onderzoek worden hieronder op hoofdlijnen weergegeven.

De uitgangspunten voor functiescheiding in beleidsdocumenten zijn nog niet vertaald naar toetsbare eisen voor de inrichting van het autorisatiebeheer. Deze vertaalslag is nodig om sturend te kunnen zijn voor de daadwerkelijke inrichting van de autorisaties en om effectief te kunnen monitoren en toetsen.

In het systeem is een groot aantal rollen aangetroffen. Het terugbrengen van het aantal rollen (momenteel 104) en het verbeteren van de structuur van inrichting van autorisaties verdient aandacht. Hierbij is het cruciaal een duidelijke geformaliseerde richtlijn (functiescheidingsmatrix) op te stellen waarin onverenigbare functies/rollen worden gespecificeerd.

Het huidige Control Framework heeft niet geleid tot een geïntegreerde controleaanpak. In deze aanpak zal aandacht moeten worden gegeven aan een verdere aanscherping en formalisering van de SOLL positie van de autorisaties. Ook zal een periodieke confrontatie met de IST situatie moeten plaatsvinden waarbij verschillen verklaard worden.

De HDBV heeft aangegeven de punten ter hand te nemen en deze medio 2015 te realiseren.

CLUSTERMANAGER GEÏNTEGREERDE BEDRIJFSVOERING

BIJLAGE: BEVINDINGEN UIT HET ONDERZOEK

Tijdens ons onderzoek hebben wij vastgesteld dat de organisatie een aantal stappen in de verbetering van het proces heeft gezet. Zo is een slag gemaakt met het inzichtelijk maken van de rechten onder de systeemrollen in het PeopleSoft system. Ook is vastgesteld welke systeemrollen met welk doel in gebruik zijn. Vervolgens is een schoning op deze rollen doorgevoerd. Voor verdere vereenvoudiging is een hernieuwde opzet van de toegangslijsten noodzakelijk. Deze actie zal de komende periode worden doorgevoerd.

Een andere doorgevoerde vereenvoudiging betreft de afbouw van het aantal statische rollen. Deze rollen werden uitgegeven en gekoppeld aan een medewerker. Op dit moment worden rollen alleen nog dynamisch uitgegeven dus gekoppeld aan de arbeidsplaats. Door de dynamische koppeling volgen de autorisaties direct de wijzigingen in het personeelsbestand.

Tenslotte is het aantal Data Permissie lijsten substantieel afgenomen. Middels deze lijsten wordt toegang tot data van organisatiedelen gegeven. Er worden nu alleen Data Permissie lijsten toegepast als hiervoor de functionele behoefte is onderbouwd.

Hoewel duidelijke stappen zijn gemaakt in het vervolmaken van het autorisatiebeheer van de gebruikers organisatie is nog onvoldoende sprake van een aantoonbaar beheerst proces. De belangrijkste verbeterpunten uit dit onderzoek worden hieronder op hoofdlijnen weergegeven.

Organisatie, beleid, procedures en controles

De HDBV is als PME eindverantwoordelijk voor de beschrijving en werking van de processen binnen zijn domein op richtend niveau, inclusief de bijbehorende begrippen en gegevensmodellen. De DPOD is als PMH verantwoordelijk voor de beschrijving van de processen op inrichtend niveau binnen de door de PME gestelde kaders. De uitvoerende taken zijn belegd bij de DPOD UBOF, DCHR en voor een klein deel bij de Defensie onderdelen.

Het eigenaarschap van het proces autorisatiebeheer is middels de rollen PE, PME en PMH formeel belegd, maar de daadwerkelijke invulling is nog lopende.

Uitgangspunten voor functiescheiding in beleidsdocumenten als het Control Framework en de Principes en actieplan autorisatiebeheer zijn nog niet vertaald naar eisen voor de inrichting van het autorisatiebeheer. Deze vertaalslag is nodig om sturend te kunnen zijn voor de daadwerkelijke inrichting van de autorisaties en om effectief te kunnen monitoren en toetsen.

Door de PME is aangegeven is dat medio 2015 er een update van de beschrijving van de rollen zal worden gerealiseerd, waarbij tevens een indikking van het aantal (momenteel 104) rollen zal plaatsvinden. Voor deze rollen moet worden aangegeven uit welke taken zij bestaan. Het is cruciaal hierbij tevens aan te geven welke taken onverenigbaar zijn en niet in één functie mogen samenkomen.

Er is een procesbeschrijving op inrichtend niveau voor autorisatiebeheer binnen het P-domein. In deze procesbeschrijving zijn de taken en verantwoordelijkheden van eenieder betrokken bij het autorisatieproces eenduidig beschreven. De verdere integratie met de bestaande procesbeschrijvingen van DCHR/BKU moet nog plaatsvinden. Dit om een integraal inzicht te verkrijgen.

Begin 2015 wordt een nieuwe versie van het Control Framework vastgesteld door de HDBV. Het is van belang dat vanuit dit Control Framework een vertaling plaatsvindt leidend tot een geïntegreerde controleaanpak. Daarbij adviseren wij om de wijze van rapporteren, escaleren en het nemen van vervolgstappen expliciet op te nemen.

Aanbevelingen:
Wij bevelen aan een verdere invulling aan de PME en PMH rollen te geven, waarbij aandacht wordt besteed aan het maken van een vertaalslag van beleid naar toetsbare eisen en uitgangspunten. Deze vertaling zal moeten leiden tot een uitwerking van de gewenste functiescheiding, waarbij per rol is aangegeven welke taken deze mag vervullen en welke taken onverenigbaar zijn.

Wij bevelen aan het voor autorisaties relevante deel van het Control Framework verder uit te werken, leidend tot een geïntegreerd controleplan. Formaliseer deze periodiek uit te voeren controles en leg de rapportagelijnen en -momenten vast. Maak vervolgacties uit controles inzichtelijk en traceerbaar.

Autorisatiematrices

De toekenning van autorisaties in PeopleSoft gebeurt met rollen (systeemrollen en verzamelrollen of generieke rollen). Een systeemrol bestaat uit één of meer toegangslijsten, waarmee de toegangsmogelijkheden tot een menuonderdeel of pagina van het informatiesysteem zijn geregeld.

De huidige opzet van de autorisatiestructuur bemoeilijkt een afdoende beheersbaarheid van en toezicht op de uitgegeven toegangsrechten.
In de huidige opzet kan een toegangslijst in meerdere systeemrollen voorkomen. Hierdoor is er een overlap in functionaliteit tussen de verschillende systeemrollen. De naamgeving van de systeemrollen is niet altijd een goede representatie van de werkzaamheden/taken die er mee kunnen worden uitgevoerd. Daarnaast is er momenteel een veelheid aan rollen en uitzonderingen. Ook is op dit moment geen overzicht welke toegangslijsten niet gelijktijdig aan één arbeidsplaats mogen worden toegekend.
Door het bovenstaande wordt de inzichtelijkheid van de toegekende autorisaties niet bevorderd en daarmee het beheer en het toezicht bemoeilijkt.

Periodiek wordt gecontroleerd of wijzigingen in de systeemrollenmatrix herleidbaar zijn naar een Request for Change. Deze verschillen worden vastgesteld door de huidige inrichting in het informatiesysteem te vergelijken met de situatie aangetroffen tijdens de voorgaande controle. Onverklaarbare verschillen worden voorgelegd aan de beheerorganisatie. Tegelijkertijd wordt de nieuwe situatie vastgesteld als nieuwe definitieve autorisatiematrix. Deze vertegenwoordigt echter niet de SOLL-situatie maar een (deels) verklaarde IST-positie.

Daarnaast vindt een confrontatie plaats tussen de toegekende rollen en de rollen in de functiematrix. De formalisering van deze functiematrix behoeft verdere aanscherping. Tevens maakt deze controle nog geen deel uit van het controleplan.

Tijdens de reguliere jaarrekeningcontrole is vastgesteld dat ruim honderd managers binnen de selfservice-manager (module Peoplesoft) ook reportmanager zijn voor zichzelf zijn. Het risico bestaat dat zij de door hun zelf gestelde mutaties vervolgens ook goedkeuren. Middels data-analyse zal nog vastgesteld in hoeverre dit is gebeurd.

Aanbevelingen:
Wij adviseren om de structuur van inrichting van autorisaties te verbeteren. Aandachtpunten hierbij zijn:

- Het borgen dat er geen overlap tussen toegangslijsten bestaat.
- Een naamgeving die de inhoud van een rol en toegangslijst goed weerspiegelt.
- Geen functiescheidingsdoorbreking binnen toegangslijsten, systeem- en verzamelrollen.
- Het verminderen van het aantal rollen/toegangslijsten en het doorvoeren van een harmoniseringslag voor deze.
- Het aansluiten van de rollen en toegangslijst op de onderkende functies en taken.
- Het opstellen van een overzicht van welke rollen nooit gelijktijdig aan één medewerker mogen worden toegewezen en hierop bij de toewijzing van autorisaties te toetsen.

Tevens adviseren wij om de controle van de IST positie tegen de SOLL positie verder te formaliseren en de verschillen te verklaren. Uit hoofde van doelmatigheid adviseren wij om deze periodieke vergelijking te ondersteunen middels tooling waarbij ook getoetst wordt op onverenigbare, conflicterende rollen/toegangslijsten.