Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Betrouwbaarheid diplomaregister

definitief

Colofon

Titel	Betrouwbaarheid diplomaregister
Uitgebracht aan	Rudi Snijders, Hoofddirecteur Uitvoering DUO
Datum	22 oktober 2021
Kenmerk	2021-0000212228

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Managementsamenvatting

Met dit eindrapport willen we inzicht geven in de doeltreffendheid van de getroffen beheersmaatregelen in de keten (DUO) die de betrouwbaarheid van de getoonde onderwijsresultaten in het diplomaregister moeten borgen.
Onderzocht is welke risico's op het gebied van betrouwbaarheid (vertrouwelijkheid en integriteit) zijn te onderkennen, welke beheersmaatregelen DUO heeft getroffen en welke aandachtspunten/verbetermogelijkheden de ADR heeft onderkend.
Hieronder is een beknopte samenvatting opgenomen van de bevindingen.

We hebben, conform de opdrachtbevestiging, onderzoek gedaan naar de betrouwbaarheid van het diplomaregister (keten) en de betrouwbaarheid van de tool EMREX. Omdat EMREX geen onderdeel uitmaakt van de keten diplomaregister en we daardoor andersoortige werkzaamheden hebben uitgevoerd, hebben we de uitkomsten van ons onderzoek in twee separate rapportages weergegeven. De managementsamenvatting van het EMREX-deelrapport hebben we in bijlage 1 van dit eindrapport Betrouwbaarheid diplomaregister opgenomen.

Centrale hoofdboodschap

Het risico van diploma's die onjuist zijn of ten onrechte geregistreerd staan in de registers moet zo veel mogelijk gemitigeerd worden. Om de betrouwbaarheid van de onderwijsresultaten te waarborgen zijn er door DUO vele beheersmaatregelen (BM) getroffen, die apart of in combinatie met andere, risico's mitigeren en bijdragen aan en betere betrouwbaarheid van het diplomaregister.

De getroffen beheersmaatregelen bij de verschillende registers, het Gegevensmagazijn, diplomaregister algemeen en de werking ervan, zijn in paragraaf 4.6 "Recapitulatie getroffen beheersmaatregelen" weergegeven. Daarbij is ook aangegeven welke onderkende risico's ermee worden gemitigeerd, indien correct werkend.

Om de risico's met betrekking tot de betrouwbaarheid van het diplomaregister nog verder te mitigeren kan DUO onderstaande aandachtpunten/verbetermogelijkheden oppakken.

Belangrijkste aandachtspunten/verbetermogelijkheden:

- Autorisatiebeheer registers risicogericht inrichten (algemeen)
- Loginformatie risicogericht monitoren (algemeen)
- Datamanipulaties beperken en monitoren (algemeen)
- Muteren alleen op basis van verzoek onderwijsinstelling (BRON MBO/VO/HO)
- Inregelen toegankelijke loggingsgegevens (BRON MBO/HO)
- Controle Kennis en Leercentrum op handmatige mutaties vanuit systeem (BRON MBO/VO)
- Terugkoppelingsmail verwerkte handmatige mutatie automatiseren (BRON MBO)
- Uitbreiden application controls (BRON HO)
- Koppelen handmatige mutatie aan fysiek verzoek (BRON VO/HO)
- Afdwingen vierogencontrole (BRON MBO/VO//HO,)
- Overgaan op individuele accounts met bijbehorende autorisaties
- Vaststellen uniforme definitie diplomadatum
- GGM-API beveiligen (GGM)

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

Aanleiding onderzoek diplomaregister
DUO ontvangt regelmatig signalen dat er wordt gefraudeerd met diploma's. Websites bieden bijvoorbeeld tegen betaling diploma's aan. Beweerd wordt dat deze "gekochte" diploma's ook in het diplomaregister worden opgenomen. De ontvangen signalen worden door DUO onderzocht en er wordt aangifte van gedaan. Ook worden er ten onrechte diplomagegevens aangeleverd en weer ingetrokken en worden er regelmatig correctieverzoeken ingediend door instellingen.
Omdat documenten uit het diplomaregister gelden als een officieel document en een geldig bewijsstuk zijn, wil DUO ervan uit kunnen gaan dat de gegevens die getoond worden in het diplomaregister betrouwbaar zijn.

DUO wil daarom inzicht hebben in de doeltreffendheid van de getroffen beheersmaatregelen in de keten die de betrouwbaarheid van de getoonde onderwijsresultaten in het diplomaregister moeten borgen.

Aanleiding onderzoek EMREX
De internationale mobiliteit van studenten neemt toe. Er studeren steeds meer studenten in het buitenland en buitenlandse universiteiten hebben vaak studieresultaten van een student nodig om een student in te kunnen schrijven. Met EMREX kunnen studenten hun studiegegevens uitwisselen over landsgrenzen heen voor verschillende doeleinden.

DUO wil inzicht krijgen of er voldoende maatregelen zijn getroffen, ten dienste van de integriteit en vertrouwelijkheid van de onderwijsresultaten die van DUO naar het buitenland verzonden worden met behulp van EMREX.

Opdrachtgever is Rudi Snijders, Hoofddirecteur Uitvoering DUO.

1.2 Doelstelling en onderzoeksvragen

Doelstelling diplomaregister
Inzicht geven in de doeltreffendheid van de getroffen beheersmaatregelen in de keten (DUO) die de betrouwbaarheid van de getoonde onderwijsresultaten in het diplomaregister moeten borgen.

Onderzoeksvragen diplomaregister
1. Hoe verloopt het proces (onderdelen: betrokken ketenpartners, systemen, datastromen) dat ervoor zorgt dat het diplomaregister betrouwbare onderwijsresultaten toont?
2. Welke risico's, op het gebied van betrouwbaarheid (vertrouwelijkheid en integriteit), zijn te onderkennen bij het proces dat ervoor zorgt dat het diplomaregister betrouwbare onderwijsresultaten toont?
3. Welke beheersmaatregelen zijn bij de procesonderdelen van DUO (registers, gegevensmagazijn, diplomaregister) getroffen om de betrouwbaarheid van de getoonde onderwijsresultaten in het diplomaregister te waarborgen?
4. Welke aandachtspunten/verbetermogelijkheden gericht op de betrouwbaarheid (vertrouwelijkheid en integriteit) van de getoonde onderwijsresultaten in het diplomaregister worden door de ADR onderkend?

Doelstelling EMREX

Het doel van dit deelonderzoek is het achterhalen van de maatregelen die reeds zijn getroffen en kunnen worden getroffen, ten dienste van de integriteit en vertrouwelijkheid van de berichten en het berichtenverkeer dat wordt verzorgd door het [redacted] van DUO. Dit [redacted] handelt inkomende onderwijsresultaatverzoeken af die afkomstig zijn uit andere EU-landen.

Onderzoeksvragen EMREX

1. Hoe verloopt een gegevensverzoek van een onderwijsinstelling binnen de EU via EMREX aan DUO?
2. Welke maatregelen zijn er vanuit EMREX en/of DUO getroffen om de vertrouwelijkheid en integriteit van de berichten en het berichtenverkeer te waarborgen?
3. In hoeverre zijn de maatregelen die vanuit EMREX en/of DUO zijn getroffen effectief?
4. Welke aanvullende maatregelen kunnen worden getroffen ter bevordering van de vertrouwelijkheid en/of integriteit van de berichten en/of het berichtenverkeer?

1.3 Afbakening

Object van onderzoek diplomaregister

- Diplomaregister
- Gegevensmagazijn
- Bronregisters:
  - (BRON HO)
  - (BRON VO / VAVO en staatsexamens)
  - (BRON MBO)
  - ISI (Inburgering)
  - (NT2)

Afbakening diplomaregister

Binnen de scope vallen:

- De systemen die onder DUO vallen: het diplomaregister, de bronregisters en het gegevensmagazijn.

Buiten de scope vallen:

- De (systemen van de) onderwijsinstellingen vallen buiten de scope van het onderzoek. Het uitgangspunt is dat de onderwijsinstellingen authentieke diploma's aanleveren. Zij worden gecontroleerd door de Inspectie van het Onderwijs en jaarlijks door een instellingaccountant. Van die controle wordt een Assurancerapport opgesteld.

Object van onderzoek EMREX

- EMREX:

Afbakening EMREX

Binnen de scope vallen:

- De integriteit en vertrouwelijkheid van de berichten en het berichtenverkeer dat wordt verzorgd door het van DUO. Dit handelt inkomende resultaatverzoeken af die afkomstig zijn van andere EU-landen;
- De achterliggende DUO-systemen worden enkel binnen de scope betrokken voor zover deze van invloed zijn op de integriteit en vertrouwelijkheid van de berichten en/of het berichtenverkeer van EMREX.

Buiten de scope vallen:

- Het cliënt-element (verzoeken naar andere EU-landen) is als pilot voor studielink in gebruik, maar zal niet binnen de scope van dit onderzoek vallen. De verzoekzijde (vanuit een ander EU-land) valt daarmee buiten scope;
- De centrale [redacted] (EMREG) valt vooralsnog buiten scope, maar kan op basis van tussentijdse resultaten alsnog worden betrokken.

Afbakening rapportage

In de opdrachtbevestiging is aangegeven dat we onderzoek gaan doen naar de betrouwbaarheid van het diplomaregister (keten) en de betrouwbaarheid van de tool EMREX. Omdat EMREX geen onderdeel uitmaakt van de keten diplomaregister en we daardoor andersoortige werkzaamheden hebben verricht, hebben we de EMREX-bevindingen in een separaat deelrapport opgenomen. De managementsamenvatting van dit deelrapport hebben we in bijlage 1 van dit eindrapport betrouwbaarheid diplomaregister opgenomen.

1.4 Leeswijzer

In hoofdstuk 2 wordt op hoofdlijnen het procesverloop beschreven. Het antwoord op onderzoeksvraag 2, risico's op het gebied van betrouwbaarheid, wordt in hoofdstuk 3 gegeven en het antwoord op onderzoeksvraag 3, de getroffen beheersmaatregelen in hoofdstuk 4. In hoofdstuk 5 worden de aandachtspunten/verbetermogelijkheden genoemd. De verantwoording van het onderzoek is beschreven in hoofdstuk 6.
Als bijlagen zijn de managementsamenvatting van het deelrapport betrouwbaarheid EMREX opgenomen en de managementreactie van DUO op het rapport onderzoek betrouwbaarheid diplomaregister en EMREX.

Begrip	**Gehanteerde definitie/verklaring**
Register	Databases zoals BRON worden bij DUO veelal aangeduid als registers. In dit rapport worden de databases met de gegevens die als input dienen voor het DR aangeduid als registers. Het diplomaregister is hierop een uitzondering, en omvat het geheel aan systemen dat ervoor zorgt dat diploma's kunnen worden weergegeven in MijnDUO. Zie paragraaf 2.1 Keten diplomaregister.
Diploma's	In verband met de leesbaarheid worden in dit rapport diploma's en certificaten aangeduid met het woord 'diploma's'.
Onderwijsresultaten	Dit begrip omvat diploma's, certificaten, cijferlijsten en examenuitslagen.

2 Procesverloop keten diplomaregister

In dit hoofdstuk wordt toelicht hoe en via welke systemen onderwijsresultaten worden doorgegeven om uiteindelijk in het diplomaregister te worden getoond.

Onderzoeksvraag 1 wordt in dit hoofdstuk beantwoord.

Hoe verloopt het proces (onderdelen: betrokken ketenpartners, systemen, datastromen) dat ervoor zorgt dat het diplomaregister betrouwbare onderwijsresultaten toont?

2.1 Keten diplomaregister

Diplomaregister
In het diplomaregister (DR) worden diplomagegevens getoond van de door het ministerie van OCW erkende Nederlandse opleidingen. Het DR dient geen opslagfunctie, maar is uitsluitend een "viewer" van de diploma's in de onderliggende registers. De externe actoren die toegang hebben tot diplomagegevens zijn de onderwijsinstellingen, de ministeries OCW, VWS (CIBG Lerarenportfolio, CIBG Big-register), suwiketen (UWV), MijnOverheid en de diplomahouders zelf. De diplomahouder kan via Mijn DUO zijn/haar eigen gegevens bekijken en een digitaal uittreksel downloaden. Het digitale uittreksel, in de vorm van een door DUO gecertificeerd Pdf-bestand, is een officieel bewijsstuk van het diploma. Wanneer een pdf van een diploma wordt opgevraagd wordt deze aangemaakt door een webservice van DUO (dr-pdf-ws). Het ondertekenen van pdf-bestanden is extern belegd, want DUO verwacht daarmee te kunnen profiteren van diens expertise en hoge mate van beschikbaarheid.

Figuur 1 toont globaal de verschillende onderdelen van het DR. Deze onderdelen worden hierna kort beschreven.

Figuur 1 Onderdelen van het diplomaregister

Registers
De gegevens die als input dienen voor het DR zijn opgeslagen in databases (hierna registers genoemd). De gegevens betreffen diploma en/of certificaten uit (HO, VO, MBO), Inburgering/ISI en NT2-Staatsexamen/ en VO-staatexamen . De gegevensstroom naar het DR is eenrichtingsverkeer. De data wordt opgehaald uit de registers om deze aan de klant te kunnen tonen, maar kan middels het DR niet worden bewerkt. In de registers vinden datamutaties plaats op verzoek van onderwijsinstellingen of DUO in het geval van verhangingen (het koppelen van een persoonsregistratie aan een andere persoonsregistratie van dezelfde persoon). Als een diplomahouder/een correctieverzoek indient (juiste gegevens worden daarna opgevraagd bij de onderwijsinstelling) komt deze via de klantenservice van DUO bij de registers terecht. Dit valt onder de verantwoordelijkheid van het team van het betreffende register.

Gegevensmagazijn, gegevensoverdracht, logging en archivering
De data wordt uit de registers gehaald via services van het Gegevensmagazijn (GGM). GGM is een DUO-brede oplossing voor communicatie en gegevensoverdracht tussen verschillende systemen/applicaties en databases. GGM ontsluit gegevens op een generieke manier vanuit de (basis- en gegevens)registraties van DUO voor interne afnemers (DUO-processen) en externe belanghebbenden. De opgehaalde gegevens worden gefilterd op basis van business rules. Deze business rules bepalen per onderwijssoort welke gegevens getoond moeten worden in het DR en worden bijgehouden op de Wikipagina van het diplomaregister. Ze zijn aan verandering onderhevig door nieuwe besluiten en nieuw beleid van de overheid. Het GGM draagt bij aan het standaardiseren en optimaliseren van het proces van gegevensleveringen, zo ook aan het diplomaregister.

Een andere restservice is verantwoordelijk voor het ontsluiten van onderwijsresultaten naar de front-end (de portalen). Dit betreft onder andere het ophalen van gegevens, samenstellen van Front-end-bericht, sorteren, authenticatie gebruiker (particulier, medewerker, zakelijk) en het inzien van logistieke leveringen. Met logistieke leveringen worden opvragingen van onderwijsresultaten uit het DR bedoeld. Verder is er een service die onderwijsresultaten ontsluit via Datapower naar MijnOverheid, CIBG Lerarenportfolio, CIBG Big-register en suwiketen (UWV). Ook via deze partijen kan het DR dus benaderd worden. DUO volgt de Edukoppeling principes/voorschriften. Edukoppeling schrijft voor hoe onderwijsinstellingen, uitvoeringsorganisaties en andere ketenpartijen gegevensuitwisselingen moeten opzetten. Het is een onderwijsspecifieke variant van Digikoppeling. DUO verwacht met Digikoppeling gemakkelijk, eenduidig, veilig en betrouwbaar informatie uit te kunnen wisselen met andere overheidsorganisaties. Edukoppeling maakt deel uit van de referentiearchitectuur voor het onderwijs (ROSA). De voornoemde services en de front-end (portalen e.d.) vallen buiten de scope van dit onderzoek.

De onderdelen Logl en ASC worden gebruikt voor logging en archivering.

Scope onderzoek
Omdat het DR toont wat er in de onderliggende registers is vastgelegd, hebben we de registers en het GGM onderzocht inzake de betrouwbaarheid van de vastgelegde onderwijsresultaten. Daartoe zullen de registers toegelicht worden. Deze registers zijn gezien de aard van de informatieprocessen grofweg in twee categorieën onder te verdelen, namelijk de BRON-registers (paragraaf 2.2) en Inburgering (ISI), NT2-staatsexamens, VO-staatsexamens) (paragraaf 2.3). Het GGM, zorgt voor gegevensoverdracht, wordt verder toegelicht in paragraaf 2.4.

2.2 BRON MBO, BRON VO en BRON HO

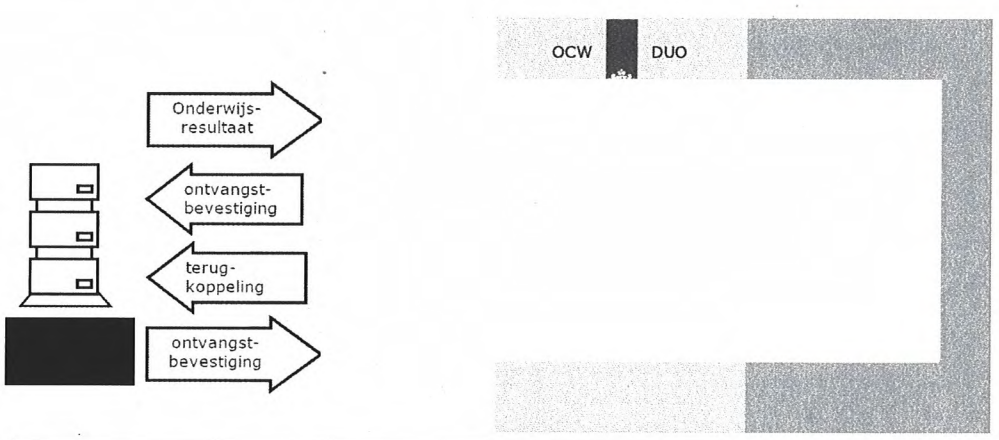
De onderwijsresultaten van studenten/leerlingen in het MBO, VO of HO worden door de onderwijsinstellingen doorgegeven aan DUO. DUO neemt deze gegevens op in het

centrale register [redacted] Deze gegevens worden gebruikt voor diverse processen, zoals het leveren van beleidsinformatie en het tonen van een diploma in het DR.

De standaard verwerking van onderwijsresultaten in de BRON-registers vindt geautomatiseerd plaats. Wanneer de onderwijsinstelling op geen enkele manier (correcties op) de onderwijsresultaten zelf geautomatiseerd kan aanleveren, dient de instelling een "verzoek handmatige mutatie" in.

2.2.1 *Geautomatiseerde verwerking onderwijsresultaten MBO, VO en HO in BRON*

Zoals getoond in onderstaande procesplaat (figuur 2) communiceert DUO met ketenpartners middels de infrastructurele component
Deze component controleert of de aanroep technisch rechtmatig (volgens de afgesproken syntaxis) is en of de aanroep door een geauthentiseerde en geautoriseerde partij is verzonden. Indien deze controle niet akkoord wordt bevonden, wordt het bericht afgekeurd en is de afkeur zichtbaar voor de instelling in het Dashboard van Studielink. Voldoet het bericht wel, dan wordt per e-mail een ontvangstbevestiging gestuurd naar de instelling. De aangeleverde diplomagegevens worden vervolgens verwerkt in de applicatie (MBO, VO en HO). Deze uitwisseling vindt plaats zonder menselijke tussenkomst.



Figuur 2: procesplaat automatische verwerking onderwijsresultaten

In figuur 2 staat "BRON HO", maar het proces om diploma's aan te leveren door MBO- en VO-instellingen verloopt op dezelfde wijze. Bij BRON HO en MBO wordt de eigen leerling/studentadministratie vastgelegd in , bij BRON VO in

2.2.2 *Handmatige verwerking onderwijsresultaten MBO, VO en HO in BRON*

Als een vertegenwoordiger van de onderwijsinstelling op geen enkele manier zelf (correcties op) de onderwijsresultaten geautomatiseerd kan aanleveren, dient de vertegenwoordiger een "verzoek handmatige mutatie" in via Mijn DUO. Voor het opvoeren of wijzigen van onderwijsresultaten moet de onderwijsinstelling een bewijsstuk meesturen. DUO verwerkt dan handmatig de (correctie op) onderwijsresultaten in de applicatie (MBO, VO en HO).
De beheerder van een instelling kan zichzelf en gebruikers (medewerkers) rollen en kenmerken toewijzen voor taken en diensten op Mijn DUO.

Wanneer de onderwijsresultaten niet op de reguliere wijze (geautomatiseerd of via een HM door DUO) verwerkt kunnen worden, kan een rechtstreekse ingreep op de database (datamanipulatie) worden gedaan.

2.3 Inburgering, NT2- en VO-staatsexamens

2.3.1 *Verwerking aangeleverde onderwijsresultaten Inburgering in ISI*

Om de Wet inburgering goed uit te kunnen voeren, heeft DUO een registratiesysteem gebouwd, het Informatiesysteem Inburgering (ISI). In ISI worden alle diploma´s van Inburgeringsplichtigen opgeslagen. In ISI wordt op basis van business rules bepaald of iemand recht heeft op een diploma. De inburgeringsexamenonderdelen zijn luisteren, lezen, spreken en schrijven. De resultaten van de examens luisteren en lezen worden automatisch geregistreerd in ISI. Bij spreken en schrijven vindt een handmatige beoordeling plaats voordat de resultaten worden geregistreerd.
Via het portaal MijnInburgering kan de klant zijn gegevens inzien en examens opvragen.

2.3.2 *Verwerking aangeleverde onderwijsresultaten NT2- en VO-staatsexamens in*

NT2-staatsexamen
DUO organiseert het staatsexamen Nederlands als tweede taal (NT2). Dit examen is bedoeld voor mensen die het Nederlands niet als moedertaal hebben, maar het Nederlands op het gewenste niveau willen beheersen voor werk of studie. In het DR zijn NT2-diploma´s en -certificaten te raadplegen. Certificaten worden behaald bij voldoendes voor de losse examenonderdelen (lezen, luisteren, spreken en schrijven). Na het behalen van alle certificaten kunnen deze worden omgezet in een diploma.

VO-staatsexamen
Het staatsexamen Voortgezet Onderwijs (VO) is bedoeld voor mensen die niet (meer) deelnemen aan het "gewone" voortgezet onderwijs. In het DR zijn VO-staatsexamen diploma´s en certificaten te raadplegen. Certificaten worden behaald bij voldoendes voor de verschillende vakken. Na het behalen van de benodigde certificaten kunnen deze worden omgezet in een diploma.

Proces verwerken staatsexamens in (NT2 tot juli 2021 en VO)
Resultaten van de examens worden opgenomen in stuurt resultaten met een voldoende naar print de certificaten, waarna deze via DataWareHouse in de database terechtkomen. In wordt de verzameling gemaakt van hetgeen getoond moet worden in het diplomaregister. Vervolgens wordt er middels de database GGM een kopie gemaakt van . Het doel van deze kopie is om de data leesbaar te maken voor GGM. Middels GGM worden de certificaten en diploma's opgehaald uit GGM en getoond in het DR.

Wanneer data niet op de reguliere wijze verwerkt kan worden, kan een rechtstreekse ingreep op de database plaatsvinden (datamanipulatie).

Vernieuwing systemen voor NT2
De processen en systemen rondom het staatsexamen NT2 zijn vernieuwd. In het voormalige proces werden de gedateerde en technisch complexe applicaties en gebruikt, waarbij een groot aantal handmatige acties nodig was. Het systeem moest efficiënter en minder foutgevoelig worden ingericht. Vanaf juli 2021 wordt door de introductie van het systeem [redacted]) een groot deel van de processtappen geautomatiseerd. VO-staatsexamen is in de vernieuwing nog niet meegenomen, omdat de regelgeving complexer en veranderlijker is.

De nieuwe systemen en processen zijn weergegeven in figuur 3.

Figuur 3: verwerking resultaten staatsexamens systeemsituatie oud en nieuw

2.4 Gegevensmagazijn

Architectuur GGM

Het Gegevensmagazijn bestaat uit tal van onderdelen die elk verantwoordelijk zijn voor het ontsluiten van registers (databases) richting verschillende afnemers (applicaties uit verschillende domeinen). Een GGM-onderdeel wordt opgeleverd als een Java WAR-file, de applicatie bevat SQL-statements en eenvoudige logica. Functioneel is het een API die wordt opgeleverd. Dit maakt gegevensoverdracht mogelijk tussen applicaties (clients) en databases. Gegevens kunnen realtime worden opgevraagd uit authentieke registers of een kopie hiervan.

Het GGM binnen de keten diplomaregister bestaat grofweg uit twee onderdelen: een clientapplicatie) en een API ( ), zie figuur 4. De client kan de API aanroepen om gegevens op te vragen uit de databases (registers). De client wordt beheerd door het DR-team en de API door het GGM-team. Er wordt enkel data gelezen, via GGM kan geen data toegevoegd, gewijzigd of verwijderd worden.

Figuur 4: GGM-onderdelen binnen de keten diplomaregister

3 Belangrijkste risico's

In dit hoofdstuk worden de belangrijkste risico's op het gebied van betrouwbaarheid toegelicht die bij de registratie van onderwijsresultaten in de registers tot het tonen van de onderwijsresultaten in het diplomaregister te onderkennen zijn.

Onderzoeksvraag 2 wordt in dit hoofdstuk beantwoord.

Welke risico's, op het gebied van betrouwbaarheid, zijn te onderkennen bij het proces dat ervoor zorgt dat het diplomaregister betrouwbare onderwijsresultaten toont?

Algemeen
In dit hoofdstuk worden vanuit een hoog abstractieniveau drie risico's onderkend ten aanzien van de betrouwbaarheid van de gegevens in het diplomaregister (DR). De gegevens worden betrouwbaar geacht wanneer de onderwijsresultaten juist zijn, afkomstig van een (onderwijs)instelling en gebaseerd op een geleverde prestatie met positief resultaat van een leerling/student.

De risico's zijn opgesteld op basis van input van de opdrachtverstrekker, een brainstormsessie binnen het onderzoeksteam en gekoppeld aan de doelstelling van het diplomaregister. De doelstelling van het DR is dat de getoonde gegevens betrouwbaar moeten zijn. Dat houdt in dat de gegevens inhoudelijk juist moeten zijn en dat een diploma terecht is aangemaakt.

3.1 Risico van het ten onrechte tonen van een diploma

Het eerste risico is het ten onrechte tonen van diploma's doordat deze ten onrechte geregistreerd staan in de registers. De eigenaar van het diploma kan een digitaal uittreksel downloaden in de vorm van een pdf-bestand. Dit pdf-bestand is een officieel bewijsstuk van het diploma, welke dus in deze situatie ten onrechte in omloop wordt gebracht.

Binnen dit risico kan onderscheid worden gemaakt in de verantwoordelijke entiteit. Enerzijds heeft de onderwijsinstelling de verantwoordelijkheid om alleen rechtmatige diploma's aan te leveren. Gezien de afbakening van dit onderzoek wordt hier niet verder op in gegaan. Anderzijds heeft DUO de verantwoordelijkheid om niet op eigen initiatief (onrechtmatig) diploma's handmatig in de registers vast te leggen. Door DUO vastgelegde onderwijsresultaten zijn onrechtmatig wanneer er geen verzoek vanuit de onderwijsinstelling aan ten grondslag ligt.

Een onderwijsinstelling kan een verzoek indienen om een reeds in een register vastgelegd diploma te verwijderen/in te trekken. Instellingen kunnen diploma's laten intrekken om verschillende redenen:

1. fout met betrekking tot persoonsgegevens; bijvoorbeeld wanneer twee studenten dezelfde naam hebben en het diploma of certificaat wordt erkend voor de verkeerde persoon;
2. op verzoek van een student die wel een diploma heeft behaald, maar nog hogere cijfers probeert te halen;
3. op verzoek van een student die nog een andere studie wil gaan beginnen en daarvoor zijn/haar resterend recht op studiefinanciering wil gebruiken;
4. dat de onderwijsinstelling of diplomahouder erachter is gekomen dat er ten onrechte, in geval van fraude, een diploma is uitgegeven.

Het 1e en 4e verzoek moeten direct opgepakt worden door een DUO-medewerker, anders bestaat het risico dat de betreffende student ten onrechte een diploma getoond krijgt via Mijn DUO en kan downloaden met alle gevolgen van dien. Het 2e en 3e verzoek zijn minder urgent, omdat de diploma's in die situaties wel authentiek zijn.

3.2 Risico van een inhoudelijk onjuiste diploma

Het tweede risico is het tonen van diploma's met inhoudelijke onjuistheden, zoals een onjuiste naam of datum. Wederom kan er onderscheid worden gemaakt ten aanzien van de verantwoordelijke entiteit. Enerzijds heeft de onderwijsinstelling de verantwoordelijkheid om juiste diploma(gegevens) aan te leveren. Gezien de afbakening van dit onderzoek wordt hier niet verder op in gegaan. Anderzijds heeft DUO de verantwoordelijkheid om de aangeleverde diploma's onveranderd vast te leggen in de registers. Het kan echter voorkomen dat DUO-medewerkers mutaties moeten verrichten op de geregistreerde diploma's, omdat daar onjuistheden in blijken te staan. Hierbij moet DUO systematisch uitsluiten dat handmatige mutaties en datamanipulaties plaatsvinden zonder dat daar een verzoek van de onderwijsinstelling aan ten grondslag ligt. Anders riskeert DUO dat medewerkers onrechtmatige inhoudelijke mutaties kunnen doorvoeren. Daarnaast dienen er maatregelen getroffen te worden om een onjuiste verwerking van een door de onderwijsinstelling aangevraagde mutatie te voorkomen.

Datamanipulaties direct op productiedata vormen een groter risico ten aanzien van data-integriteit dan handmatige mutaties via een interface, zoals het medewerkersportaal. Data-integriteit kan op twee manieren worden geschonden door datamanipulaties:

1. Middels ongeautoriseerde datamanipulaties, waarbij datamanipulaties zonder toestemming worden uitgevoerd door iemand met (te) hoge rechten op een productiedatabase.
2. Middels geautoriseerde datamanipulaties, waarbij geautoriseerde personen zoals beheerders onbedoeld fouten maken en onjuistheden doorvoeren.

3.3 Risico van ten onrechte lezen van onderwijsresultaten

Het derde risico is dat ongeautoriseerde toegang tot gegevens onvoldoende wordt voorkomen. Dit is het geval wanneer medewerkers ten onrechte onderwijsresultaten (kunnen) lezen. Er dienen daarom maatregelen getroffen te worden ter bescherming van de vertrouwelijkheid van gegevens, objecten en bronnen. Dergelijke maatregelen dienen te borgen dat niemand anders dan de beoogde ontvanger/gebruiker/eigenaar berichten of gegevens ontvangt of kan lezen.

Het laatstgenoemde risico heeft geen invloed op de betrouwbaarheid van het DR, maar wel op de vertrouwelijkheid van de gegevens. Dit risico is opgenomen, omdat in de onderzoeksvragen 2, 3 en 4 de term betrouwbaarheid (vertrouwelijkheid en integriteit) is opgenomen. Het ten onrechte lezen van onderwijsresultaten valt onder vertrouwelijkheid.

4 Getroffen beheersmaatregelen

In dit hoofdstuk wordt beschreven welke beheersmaatregelen bij de registers, het gegevensmagazijn en het diplomaregister zijn getroffen om ervoor te zorgen dat de getoonde onderwijsresultaten in het diplomaregister betrouwbaar zijn.

Onderzoeksvraag 3 wordt in dit hoofdstuk beantwoord.

Welke beheersmaatregelen zijn bij de procesonderdelen van DUO (registers, gegevensmagazijn, diplomaregister) getroffen om de betrouwbaarheid van de getoonde onderwijsresultaten in het diplomaregister te waarborgen?

Algemeen
Om de risico's beschreven in hoofdstuk 3 te mitigeren heeft DUO diverse beheersmaatregelen getroffen. DUO-brede beheersmaatregelen en specifieke registerbeheersmaatregelen worden hierna separaat besproken.
In de recapitulatie, zie paragraaf 4.6, wordt per getroffen beheersmaatregel aangegeven op welk risico de beheersmaatregel een mitigerende werking heeft.

Van de getroffen beheersmaatregelen bij de registers BRON MBO, VO, HO en de DUO-brede beheersmaatregelen, is opzet, bestaan en werking vastgesteld. Van de overig getroffen beheersmaatregelen alleen de opzet.

4.1 DUO-brede beheersmaatregelen

Fysieke toegangscontrole
De toegang tot het gebouw vindt plaats via een persoonlijke Rijkspas. Wanneer de medewerker de Rijkspas is vergeten of kwijtgeraakt, kan een collega de medewerker identificeren en ophalen bij de balie. De medewerker krijgt dan een bezoekerspas voor een dag. Bij uitdiensttreding wordt de Rijkspas ingenomen.

Logische toegangscontrole
De toegang tot de geautomatiseerde systemen vindt plaats via een persoonlijke gebruikersnaam en wachtwoord. Dit wachtwoord moet driemaandelijks gewijzigd worden. Er vindt two factor authentication plaats indien er vanuit huis wordt gewerkt, omdat er dan aanvullend gebruik gemaakt moet worden van een token. Bij uitdiensttreding wordt de token ingenomen.

Autorisaties beheerschermen
Autorisatiebeheer is een belangrijk aspect van informatiebeveiliging, omdat DUO-processen voor een aanzienlijk deel worden ondersteund door geautomatiseerde informatiesystemen. De gegevens die daarbij worden verwerkt dienen te worden beschermd tegen onbevoegd gebruik of inzage. Leidinggevenden stellen vast welke autorisaties een medewerker behoort te krijgen aan de hand van de taken die de betreffende medewerker vervult. ICT-beveiliging zorgt er vervolgens voor dat deze autorisaties worden ingeregeld in de informatiesystemen. Bij uitdiensttreding worden diens autorisaties geblokkeerd. Bij de registers zijn de leesrechten ruim verleend, de muteerrechten in de meeste gevallen niet. Dit wordt verder toegelicht bij de betreffende registers in paragrafen 4.3 en 4.4.

Autorisaties databaseniveau (uitkomst ADR wettelijke controle OCW Bekostiging 2020)
De ADR en Algemene Rekenkamer hebben vastgesteld dat DUO sinds 2017 kampt met een onvolkomenheid op het gebied van autorisatiebeheer. Autorisaties werden te ruim verstrekt, met name aan IT-personeel. Dit heeft geleid tot een groot aantal systemen waarin medewerkers meer rechten hadden dan noodzakelijk. Er waren bijvoorbeeld systemen waarbij het aantal beheeraccounts vele malen groter was dan het aantal beheerders. Daarnaast werden uitdiensttredingen niet altijd tijdig verwerkt, ook in , het platform van de . Deze onvolkomenheid heeft geleid tot toegenomen awareness en aandacht vanuit het management, maar het probleem bleek in 2020 nog niet verholpen.

Desondanks heeft DUO de afgelopen jaren grote stappen gezet. Via het traject 'Autorisatiebeheer In Control' (AIC) blijft DUO werken aan het op orde krijgen van autorisatiebeheer. Het traject is veelomvattend, gezien het grote aantal systemen en de hoeveelheid werk dat dit met zich meebrengt. De mate waarin DUO het autorisatiebeheer onder controle heeft, verschilt per systeem. Binnen dit onderzoek hebben we gekeken naar de autorisaties met betrekking tot handmatige mutaties binnen de in de scope benoemde registers.
We hebben niet naar autorisaties met betrekking tot datamanipulaties (direct op de gekeken, aangezien dit in 2020 nog is onderzocht tijdens de jaarlijkse GITC-controle.

Logging
DUO heeft beleid opgesteld ten opzichte van het gebruik van en inrichten van logging van gebeurtenissen en systemen binnen de DUO ICT-omgeving. Logging is in deze het vastleggen van relevante acties en gebeurtenissen op een systeem of in een omgeving/keten, zodat een betrouwbaar overzicht kan worden gegenereerd van alle gebeurtenissen die daar hebben plaatsgevonden. Logging is bedoeld voor verschillende doeleinden zoals performance, incident afhandeling, compliance en security.

Alle systemen en applicaties die vertrouwelijke informatie bevatten, netwerk connecties accepteren of waar toegangsbeleid (authenticatie en autorisatie) wordt toegepast, dienen gebeurtenissen te registreren en op te slaan in een (audit)log.
De bewaartermijn van een log of andere informatie zoals Audit context (ID) is afhankelijk van de rechtsgeldigheid van de desbetreffende data.

Werkinstructies en procesbeschrijvingen
Voor het handmatig verwerken van mutaties en datamanipulaties zijn werkinstructies opgesteld. Deze werkinstructies beschrijven hoe een mutatie beoordeeld en/of verwerkt moet worden in de betreffende systemen. Deze beschrijvingen moeten waarborgen dat mutaties juist en uniform worden verwerkt. Voor wijzigingsbeheer zijn procesbeschrijvingen opgesteld.

Beheersmaatregelen datamanipulaties
Datamanipulaties zijn een riskante en daarom ongewenste ingreep. Ze moeten daarom waar mogelijk worden vermeden. Om ongeautoriseerde datamanipulaties en fouten bij geautoriseerde datamanipulaties te minimaliseren zijn een aantal beheersmaatregelen getroffen. DUO heeft een proces vastgesteld voor het gecontroleerd uitvoeren van datamanipulaties. Dit proces is in 2020 getoetst tijdens de GITC-controle in het kader van de wettelijke taak van de ADR. De beheersmaatregelen waarvan de opzet en het bestaan zijn aangetoond zijn hieronder toegelicht:

- Registratie: De registratie van datamanipulaties vindt plaats in Topdesk. Dit betreft toelichting, situatie voor en na de datamanipulatie en het script;
- Autorisatie door bevoegde: De product owner of manager geeft schriftelijk akkoord voorafgaand aan de datamanipulatie;

- Vierogencontrole: Een uitgevoerde service request wordt gecontroleerd door een andere collega dan de uitvoerder van de service request;
- Logging: De uitgevoerde datamanipulaties worden gelogd en zijn te herleiden naar de persoon die ze heeft uitgevoerd.

Onderstaande beheersmaatregelen *ontbreken (deels) of kennen beperkingen*:

- Monitoring: Monitoring op datamanipulaties ontbreekt waardoor ongeautoriseerde datamanipulaties niet kunnen worden opgemerkt;
- Functiescheiding: In de werkinstructie wordt functiescheiding tussen opstellen en uitvoering van datamanipulaties niet genoemd. Uit gesprekken met DUO en de GITC-controle 2020 is gebleken dat de meeste Devopsteams zelf geen datamanipulaties uitvoeren, maar dit laten doen door een apart team, het . Hiermee is functiescheiding tussen opstellen en uitvoeren dus geborgd. Dit geldt echter niet voor alle teams; BRON VO voert bijvoorbeeld zelf datamanipulaties uit.

Wijzigingsbeheer (uitkomst ADR wettelijke controle OCW Bekostiging 2020)

De Devopsteams van DUO volgen het DUO-brede Changemanagementbeleid en de DUO Way Of Working. Het wijzigingsbeheerproces wordt elk jaar door de ADR onderzocht tijdens de GITC-controles in het kader van de jaarrekeningcontrole. In 2020 zijn de volgende maatregelen in opzet en bestaan vastgesteld:

- Registratie: Wijzigingen worden vastgelegd in Topdesk en Jira;
- Impactbepaling: DUO ziet een goede impactbepaling als randvoorwaarde voor het gecontroleerd kunnen doorvoeren van een wijziging. Een impactbepaling wordt uitgevoerd om in kaart te brengen welke andere objecten en diensten mogelijk worden geraakt door een wijziging;
- Accordering door bevoegde: Changes zijn geaccordeerd door de Product Owner en/of CAB alvorens deze naar productie gaan. Hierbij wordt rekening gehouden met de impact, testresultaten en kritische productiemomenten.

Onderstaande beheersmaatregelen ontbreken (deels) of kennen beperkingen:

- Functiescheiding: In de beleidsstukken van DUO wordt functiescheiding tussen ontwikkelen van software en deployen naar productie niet genoemd. Ook is functiescheiding niet gebruikelijk binnen DevOps-team, waarbij development en operations samengebracht worden in een multidisciplinair team. In 2020 is daarom vastgesteld dat functiescheiding niet consequent is ingericht. Maatregelen als code-reviews en onafhankelijk testen zijn daarom extra belangrijk in deze context;
- Testen: In 2020 is echter ook vastgesteld dat wijzigingen niet altijd aantoonbaar getest en goedgekeurd worden op basis van testresultaten.

Momenteel wordt door de ADR een vraaggestuurd onderzoek uitgevoerd gericht op het beheer van het changemanagementproces binnen de afdeling Infrastructuur en Exploitatie (I&E) en de diverse Business Development Operations (BDO) teams. Uit dit onderzoek zullen aandachtspunten en verbetermogelijkheden volgen. Om die redenen is wijzigingsbeheer tijdens het DR-onderzoek niet nader onderzocht en worden er geen verbeterpunt aangegeven.

Hacktesten en securitytesten

Het beleid van DUO rondom hacktesten en securitytesting is vastgelegd in het Voorschrift (geautomatiseerd) security testen. Middels hacktesten wordt inzicht verkregen in de risico's en kwetsbaarheden van het onderzochte systeem. Ook worden verbeteringen gedefinieerd om de geïdentificeerde risico's en kwetsbaarheden te bestrijden. Met behulp van een risico-calculator wordt een risicoanalyse worden uitgevoerd. Het resultaat daarvan bepaalt of er een hacktest dient te worden uitgevoerd. Bevindingen uit een hacktest krijgen een classificatie om de ernst aan te duiden. De classificatie bepaalt de opvolging.

De volgende uitgangspunten zijn opgenomen in het beleid van DUO:

- Eigenaarschap en aanspreekpunten: Van elke dienst is bekend wie de Product Owner is. Van elke locatie is bekend wie de eigenaar en aanspreekpunt is;
- Beveiligingsincidenten: Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten en een proces om eenvoudig en snel beveiligings-incidenten en zwakke plekken in de beveiliging te melden;
- Functiescheiding: De securitytesten worden uitgevoerd door onafhankelijke, gekwalificeerde personen of instanties. Een onafhankelijk team van DUO, het ethical hacking team, voert de hacktesten uit.

Een dedicated team (S3, Software Security Support) ondersteunt de Devopsteams bij het ontwikkelen van veilige software en faciliteert geautomatiseerd testen. Voor dat laatste kunnen verschillende tools gebruikt worden. Devopsteams kunnen in aanmerking komen voor een hacktestvrijstelling en zo een verlicht hacktestregime volgen. Teams die aan een bepaalde set voorwaarden voldoen (o.b.v. automatische securitytesten) hoeven dan nog maar jaarlijks een hacktest te doen. De aanvraag om hiervoor in aanmerking te komen wordt beoordeeld door de Security Competence Group op basis van een beoordelingsmodel. Het diplomaregisterteam heeft deze vrijstelling ook. De hacktesters registreren en onderhouden hun bevindingen in Mantis. Dit systeem is niet toegankelijk voor andere medewerkers dan de hacktesters zelf.

4.2 Beheersmaatregelen diplomaregister

Het diplomaregister (DR) kent een aantal onderdelen en processen die als beheersmaatregelen aangemerkt kunnen worden, omdat deze bijdragen aan het bewaken van de betrouwbaarheid (integriteit en vertrouwelijkheid) van diplomagegevens.

Authenticatie en autorisatie voor toegang tot portalen
Gebruikers moeten inloggen voordat ze toegang krijgen tot het DR. Diplomahouders loggen bijvoorbeeld in met Digi-D voordat gegevens kunnen worden geraadpleegd. Toegang tot de front-end valt buiten de scope van dit onderzoek.

Document-signing
Wanneer een diplomahouder een diploma downloadt vanuit het DR, wordt dit diploma in pdf-format op geautomatiseerde wijze digitaal ondertekend op basis van een DUO-certificaat en verstrekt. Middels deze dienst worden diploma's gelegaliseerd. Het pdf-document is een officieel document en een geldig bewijsstuk.
Het ondertekenen van pdf-bestanden is sinds 1 maart 2020 extern belegd bij een Trusted Service Provider. Door deze activiteit extern te beleggen profiteert DUO van diens expertise en hoge mate van beschikbaarheid. De externe partij is verantwoordelijk voor het voldoen aan de eisen van de accreditatie "Trusted Service Provider" die nodig is om deze dienst aan te bieden. Logius controleert jaarlijks of de leverancier aan de logische eisen voldoet. Bij een positief resultaat wordt een certificaat afgegeven. In de SLA met de externe partij kan worden opgenomen dat DUO de accreditatie en het bijbehorende certificaat jaarlijks kan opvragen. DUO controleert zelf of de functionele eisen uit het programma van eisen (pve) nageleefd worden.

Logging en monitoring
Opvragingen uit het DR (logistieke leveringen) door iemand anders dan de diplomahouder worden gelogd. Hierdoor kunnen diplomahouders bekijken welke organisaties hun diplomagegevens hebben ingezien. De service Logl wordt gebruikt voor het vastleggen en opvragen van deze informatie en is in beheer van het DR-team. Daarnaast wordt elk pdf-document (bijvoorbeeld diploma) dat gedownload is,

gearchiveerd in ASC. Zo is door DUO na te gaan hoe vaak en door wie een onderwijsresultaat is gedownload. DUO monitort voornoemde gegevens.

4.3 Beheersmaatregelen BRON HO, BRON MBO en BRON VO

Relevante systemen:

Geautomatiseerd verwerken onderwijsresultaten

Zoals toegelicht bij onderzoeksvraag 1 worden de diploma's aangeleverd door de instellingen en zonder menselijke tussenkomst in de BRON-registers opgevoerd. Alleen door DUO erkende instellingen kunnen een diploma opvoeren via beveiligde webservices tussen de portalen van de instellingen en DUO.

Programma van eisen
Het programma van eisen (pve) is een handleiding voor onderwijsinstellingen en beschrijft de geautomatiseerde uitwisseling tussen de bekostigde HO/MO/VO-instellingen, Studielink/MijnDUO en de DUO. In het pve wordt bijvoorbeeld aangegeven hoe (wijzigingen op) onderwijsresultaten geautomatiseerd kunnen worden doorgegeven. Op deze manier worden onderwijsresultaten uniform en op de juiste wijze aangeleverd.

Application controls
Zodra de instelling een diploma heeft aangeleverd via de webservices wordt deze eerst gecontroleerd middels diverse application controls in [redacted] voordat de registratie in de BRON-registers plaatsvindt. De application controls controleren of de ingezonden diploma's voldoen aan een aantal randvoorwaarden, zoals of het aantal diploma's het aantal ingeschreven studenten binnen de betreffende opleiding/instelling niet overschrijdt. Elk van de BRON-registers heeft een set aan application controls, maar het ene register heeft een uitgebreidere set dan het andere. Dit zal verder toegelicht worden onder de uitwerking van onderzoeksvraag 4.

Ontvangstbevestiging automatisch te verwerken onderwijsresultaten
De instelling geeft onderwijsresultaten door aan DUO via het Zakelijk Portaal (Mijn DUO). Er wordt via de mail een ontvangstbevestiging, met de vermelding goedgekeurd of afgekeurd na syntaxis-controle, naar de onderwijsinstelling gestuurd.

Terugkoppeling automatisch verwerkte onderwijsresultaten
Na ontvangst van het bericht voert DUO diverse controles uit. Het resultaat hiervan wordt terug gemeld aan de aanleverende partij. Indien het bericht is goedgekeurd wordt het opgenomen in het register, indien het bericht is afgekeurd wordt een afkeurbericht teruggekoppeld met één reden van afkeur.

Handmatig verwerken mutaties onderwijsresultaten

De aanleiding voor een handmatige mutatie kan zijn:
- Een omhanging die niet geautomatiseerd in het [redacted]-register is verwerkt. Vanuit het systeem wordt een e-mailbericht verstuurd naar de afdeling IPO ter verwerking;
- Een correctieverzoek vanuit het DR van een student. De mutatie wordt kortgesloten met de instelling. De instelling past de onderwijsresultaten aan in hun eigen administratiesysteem en levert deze daarna aan DUO aan via Mijn DUO;
- Een correctieverzoek vanuit de instelling via Mijn DUO.

De meeste mutaties in diploma's worden in BRON uitgevoerd naar aanleiding van een verzoek van de instelling. Er is binnen BRON-VO systematisch uitgesloten dat een handmatige mutatie kan worden uitgevoerd zonder een verzoek vanuit de instelling. Hierdoor wordt voorkomen dat een DUO-medewerker onrechtmatig handmatige mutaties verricht. Binnen BRON-MBO en BRON-HO is dit niet systematisch uitgesloten en kunnen er dus, tegen de regels in, wel gegevens opgevoerd worden zonder verzoek van de instelling.

Ontvangstbevestiging (geautomatiseerd) verzoek handmatige mutatie
De instelling geeft mutatieverzoeken door aan DUO via het Zakelijk Portaal (Mijn DUO). Zodra het verzoek is verzonden, wordt er door DUO automatisch een bevestigingsmail gestuurd naar de instelling met vermelding van een automatisch toegekend referentienummer. Ook wordt deze bevestigingsmail gestuurd naar het algemene mailadres van de afdeling binnen DUO die belast is met de werkzaamheden omtrent het betreffende BRON-register. Om het verzoek te bekijken raadpleegt de medewerker het overzichtsscherm van mutatieverzoeken op het Medewerkersportaal. Alle binnengekomen mutatieverzoeken (open en gesloten) worden bewaard in het Medewerkersportaal Dit proces borgt de volledigheid van de aanvragen aangezien deze alleen in behandeling worden genomen als ze via dit proces zijn ingediend. In het overzichtsscherm kun je zoeken op brinnummer, datum, referentienummer en de status van het verzoek: afgehandeld, in behandeling of afgewezen.

Vierogencontrole
Mutatieverzoeken moeten binnen vijf werkdagen zijn behandeld. Als het verzoek aan alle voorwaarden voldoet, wordt de gevraagde wijziging door de DUO-medewerker in de database OR verwerkt. Zodra het verzoek afgehandeld is moet deze volgens de werkinstructies gecontroleerd worden door een collega. Op alle verwerkte handmatige mutaties vindt collegiale controle plaats (100%). Een uitzondering is de controle op mutatielijsten, hierop vindt steekproefsgewijs controle plaats op 10% van de verwerkte mutaties. Bij een foutief verwerkte mutatie wordt de fout hersteld door de medewerker die de oorspronkelijke mutatie heeft uitgevoerd. Er is per BRON-register een handjevol medewerkers die muteerrechten hebben en dus de handmatige mutaties mogen verwerken en collegiaal mogen controleren.

Bij BRON-MBO en BRON-HO wordt vierogencontrole niet afgedwongen. In theorie zouden er handmatige mutaties kunnen worden doorgevoerd zonder dat er een collegiale controle heeft plaatsgevonden. De toepassing van vierogencontrole bij BRON-MBO en BRON-HO is zichtbaar op de banderol (MBO) of papieren dossier (HO).

Terugkoppeling (handmatig) verwerkte handmatige mutatie
Na de verwerking van een mutatieverzoek wordt handmatig een mail opgesteld en gestuurd naar de instelling ter kennisgeving dat het verzoek is verwerkt of afgewezen. De mail bevat het referentienummer van het mutatieverzoek alsmede een korte toelichting, zonder de vermelding van persoon herleidbare gegevens. Naar aanleiding van deze mail kan de instelling controleren of de verwerking goed is uitgevoerd.

Kwaliteitscontrole door KLC
Een medewerker van de afdeling Kennis en Leercentrum (KLC) controleert de kwaliteit van 10% van de verwerkte handmatige mutaties bij BRON VO en BRON MBO. Deze controle vindt plaats vanuit collegiaal gecontroleerde handmatige mutaties die op de afdeling liggen, niet vanuit verwerkingen in de BRON-registers.

Logging verwerkte handmatige mutatie
Bij BRON VO is de voortgang van een verwerking van een handmatige mutatie digitaal zichtbaar. Bij mutaties wordt automatisch de userID gelogd, waardoor afgeleid kan worden bij welke persoon de mutatie in behandeling is. Bij BRON MBO en BRON HO schijnt de verwerking van handmatige mutaties ook gelogd te worden, maar het

opvragen hiervan bleek tijdens dit onderzoek lastig te gaan. Het is daarom onduidelijk in welke mate logging plaatsvindt.

Archivering (indirecte beheersmaatregel)
De gecontroleerde en verwerkte mutaties worden door een BRON-medewerker per kwartaal gebundeld, voorzien van een banderol en naar het archief verstuurd (BRON HO en BRON MBO). Op de banderol staat de naam van de afdeling, de betreffende periode en de persoonsnummers van de medewerkers. De banderollen gaan per kalenderjaar in een doos, welke tevens in het archief wordt opgeslagen.

Overzichtsbestand verwerkte handmatige mutaties (indirecte beheersmaatregel)
Door senior medewerkers van de BRON-registers wordt regelmatig het automatisch gegenereerd overzichtsbestand beoordeeld waarin alle handmatig verwerkte mutaties zijn opgenomen. Indien nodig kan naar een specifieke mutatie worden gezocht. De medewerkers kunnen hier niets aan toevoegen of weghalen.

Registratieoverzicht (indirecte beheersmaatregel)
DUO kan op verzoek van onderwijsinstellingen een registratieoverzicht genereren van de vastgelegde onderwijsresultaten. Op basis daarvan kan de instelling controleren of de gegevens in het BRON-register overeenkomen met de eigen administratie.

4.4 Beheersmaatregelen registers Inburgering, NT2- en VO-staatsexamens

4.4.1 Inburgering

Relevant systeem: ISI

Automatische registratie examenresultaten
Examens worden afgenomen in Minerva (SaaS-systeem). De examenonderdelen zijn luisteren, lezen, spreken, schrijven en Kennis van de Nederlandse Maatschappij (KNM). De resultaten van de examens luisteren, lezen en KNM worden automatisch geregistreerd in SAP.

Automatisch toewijzen beoordelaars bij handmatige beoordeling examens
Het beoordelen van de open vragen van de examenonderdelen schrijven en spreken wordt gedaan in Minerva. De beoordeling wordt gedaan door gecertificeerde beoordelaars van DUO. Minerva wijst zelf al bij de exameninschrijving beoordelaars toe.

Vierogencontrole/zesogencontrole
Alle afgelegde examens worden beoordeeld door minimaal twee beoordelaars. De beoordelaars kunnen niet zien wie de andere beoordelaar is of wat diens beoordeling is geweest. Wanneer het verschil tussen de beoordelingen te groot is (bij de ene geslaagd en bij de ander gezakt), dan wordt automatisch een derde beoordelaar toegewezen door Minerva (arbitrage). Wie de derde beoordeling uitvoert is zichtbaar vastgelegd voor de backoffice (planning).

Automatische vastlegging examenresultaat en vaststelling diplomarecht
Het examenresultaat dat uit de beoordeling volgt wordt vanuit Minerva geautomatiseerd vastgelegd in ISI en bij de kandidaat. In ISI wordt op basis van business rules bepaald of de examenresultaten recht geven op een diploma. Wanneer een diploma is behaald, wordt deze na een week wachttijd afgedrukt en opgestuurd naar de kandidaat. Afgezien van het printen en opsturen, waarvoor werkinstructies aanwezig zijn, vindt dit proces geautomatiseerd plaats.

Op MijnInburgering kan de klant zijn gegevens inzien en examens opvragen.

In de nieuwe situatie wordt gebruik gemaakt van een batch-proces waarbij gegevens periodiek uit ISI worden gehaald door Datawarehouse (DWH) en opgeslagen worden in . DR haalt vervolgens via GGM de benodigde gegevens uit ODS wanneer daarom wordt verzocht (→ GGM → DR).

4.4.2 *NT2-en VO-staatsexamens*

Relevante systemen:

Situatie tot juli 2021 – registratie in systeem [redacted] en [redacted]

Functiescheiding
CITO en ICE beoordelen de afgelegde examens. Wekelijks mailen zij de resultaten ter registratie naar DUO in de vorm van een resultatenbestand.

Application controls
Voordat een NT2-resultaat wordt geregistreerd, worden er eerst een aantal controles uitgevoerd in , zoals:

- Voldoet het bericht technisch;
- Heeft de kandidaat een bruikbaar gebruikers-ID (staat deze in de BAP);
- Resultaat (programma en examenonderdeel) komt voor in de waardenlijst;
- Heeft deze kandidaat eenzelfde certificaat of diploma al? Indien dit het geval blijkt, wordt er automatisch een melding gestuurd naar Examendiensten;
- De uitslagdatum van het resultaat ligt niet in de toekomst.

Automatisch inlezen resultaten in
De in het aangeleverde resultatenbestand genoemde kandidaten worden geïdentificeerd aan de hand van een examennummer. Een DUO-medewerker past het resultatenbestand aan indien de resultaten achteraf gekoppeld moeten worden aan de juiste examennummers. Het resultatenbestand wordt vervolgens automatisch ingelezen in Indien een kandidaat buiten het computerexamensysteem om o

Nadat de uitslagbrieven zijn aangemaakt wordt in het Kwaliteit Inspectie Printen (KIP)-proces opgestart. Het KIP-proces zet de gegevens vanuit klaar voor het standalone systeem stuurt alleen resultaten naar wanneer deze voldoende zijn.

print de certificaten nadat een medewerker op de printknop drukt, waarna deze via Datawarehouse (DWH) in de database terechtkomen. Ook kan een DUO-medewerker in een kandidaat opzoeken, een diploma aanmaken voor deze kandidaat en dit diploma printen. In wordt de verzameling gemaakt van hetgeen getoond wordt in het DR. Middels de database GGM L wordt een exacte kopie gemaakt van , zodat de data in een bepaalde format komen die GGM kan uitlezen. GGM dient als het doorgeefluik waarmee het DR de certificaten kan ophalen uit GGM .

Controleoverzichten
Inhoudelijk moet de data van de positieve resultaten in overeenkomen. In werkelijkheid komt het voor dat er verschillen in bijv. diplomadatum zijn tussen de databases. De oorzaak hiervan zit in het gebrek aan een eenduidige definitie van een diplomadatum. In wordt de diplomadatum handmatig ingevoerd. In de werkinstructie staat dat de diplomadatum de datum is waarop het laatst behaalde certificaat is behaald. Daarbij worden weleens fouten gemaakt. Juridisch gezien is de diplomadatum echter de datum waarop het laatste examen heeft plaatsgevonden. Intern wordt hetgeen in als de waarheid beschouwd, maar hetgeen in staat wordt aan de buitenwereld getoond. In

de nieuwe situatie van zal bij de conversie de datum, zoals geregistreerd in uitgangspunt vormen voor hetgeen in het diplomaregister getoond wordt.

Er is een overzicht opgesteld met verschillen tussen de twee databases Deze verschillen worden uitgezocht en opgelost voordat de conversie naar gaat plaatsvinden.

Controle juistheid recht op diploma m.b.v. een query
Wanneer een NT2-kandidaat vier certificaten (lezen, luisteren, spreken, schrijven) heeft behaald dient hij/zij een verzoek in bij de afdeling Examendiensten (ED) van DUO om certificaten om te zetten in een diploma. Een medewerker van ED controleert of de kandidaat inderdaad voldoende certificaten heeft. Als hulpmiddel hierbij kunnen DUO-medewerkers sinds januari 2021 gebruik maken van een query op , waarbij ze een overzicht kunnen genereren van mensen die recht hebben op een diploma. Wanneer onvoldoende certificaten zijn behaald of de aanvraag niet onvolledig en/of onjuist is wordt geen diploma afgegeven en wordt een brief gestuurd naar de kandidaat.

Wanneer de aanvraag rechtmatig, juist en volledig is controleert ED in :

- of de datum van het laatst behaalde certificaat overeenkomt met de datum uitgifte op het laatst behaalde certificaat;
- of de adresgegevens in de brief overeenkomen met die in ;
- of alle persoonsgegevens van de kandidaat conform GBA-V (gemeentelijke basisregistratie) zijn.

ED verwerkt de gegevens rondom het nieuwe diploma in . Hierbij worden onder andere de uitgiftedatum (datum van laatst behaalde certificaat) en het examenjaar ingevuld. [redacted] maakt het diploma en de brief voor de kandidaat aan, ED print deze.

Kandidaten kunnen soms hun diploma's niet inzien in het DR. Dit gebeurt vaker bij de VO-staatsexamens dan NT2-examens. De oorzaak kan in de meeste gevallen niet worden achterhaald. In sommige gevallen ligt de oorzaak bij het filteren van data in . In deze filtering kan soms een diploma wegvallen. Een medewerker moet dan de resultaten opnieuw aanbieden. Het resultaat is pas na enkele dagen zichtbaar.

Collegiale controle bij onduidelijk
In theorie worden de geprinte brief, diploma en certificaten bijeengevoegd en gecontroleerd door een collega. Er vindt controle plaats op de persoonsgegevens, datum uitgifte, recht op diploma, programma en adresgegevens. Hierbij vult de collega een controleformulier in, welke wordt vastgelegd op een gezamenlijke netwerkschijf van ED. maakt het diploma en de brief voor de kandidaat aan, ED print deze. Vervolgens wordt de brief met het diploma verzonden naar de kandidaat.

Van collegiale controle wordt gebruik gemaakt, maar het is onduidelijk in hoeverre dit plaatsvindt. Dit heeft ook te maken met het autorisatiebeheer. Er is bij namelijk één inlognaam die elke medewerker mag gebruiken om diploma's uit te geven. Ten gevolge hiervan kan er niet gecontroleerd worden óf en door wie een diploma opgevoerd en gecontroleerd wordt. Daardoor is het in theorie mogelijk om onrechtmatig diploma's aan te maken.

Situatie vanaf juli 2021 – registratie in systeem

Onderstaande situatie geldt alleen voor NT2-staatsexamens. Voor de VO-staatsexamens blijft de oude situatie gelden.

Beheersmaatregelen automatisch verwerken resultaten

Automatisch aanleveren en inlezen resultaten
Resultaten worden automatisch aangeleverd via Zakelijk Portaal via Secure File Transfer Protocol (SFTP). Een DUO-medewerker hoeft deze niet meer handmatig te muteren en in te lezen in . De uitslagen en bijbehorende gegevens worden vanuit Zakelijk Portaal automatisch ingelezen in de bijbehorende databases.

Beperkte mutatierechten
In de nieuwe situatie hebben medewerkers inzage- en printrechten en een beperkt aantal medewerkers mutatierechten. Aangepaste examens worden namelijk nog wel per mail aangeleverd en handmatig door DUO-medewerkers ingevoerd in . Dit komt in de praktijk maar heel weinig voor.

Inhoudelijke controles
Wanneer een kandidaat een voldoende heeft gehaald op een examenonderdeel, wordt hiervoor een certificaat toegekend. Dit certificaat wordt door een ED-medewerker gecontroleerd. Dit zijn inhoudelijke controles, er kan bijvoorbeeld geen certificaat behaald zijn bij een onvoldoende. Deze controle vindt plaats via de beheerschermen van het Medewerkersportaal.

Functionele controles
Voordat een NT2-resultaat wordt geregistreerd, worden er eerst een aantal controles uitgevoerd, zoals: voldoet het bericht technisch, heeft de kandidaat een bruikbaar gebruikers-ID (komt deze voor in de BAP), komt het resultaat voor in de waardenlijst, etc. Dit zijn afkeurcontroles, als deze afgaan, wordt het bericht afgekeurd, niet opgeslagen en teruggekoppeld. Wordt het bericht goedgekeurd, dan wordt het bericht/certificaat vervolgens vastgelegd in de database .

Automatische terugkoppeling verwerking
Er gaat automatisch een bericht naar ED dat het bericht/certificaat is goedgekeurd.

Beslisboom (application controls) m.b.t. toekennen diploma
In de nieuwe situatie bepaalt het systeem zelf welke personen recht hebben op een diploma op basis van een geprogrammeerde regels, een soort beslisboom. Hierbij voert automatisch een vijftal application controls uit. Wanneer een kandidaat recht heeft op een diploma op basis van deze beslisboom wordt dit automatisch vastgelegd in . Van daaruit kan het weergegeven worden via GGM in het DR.

Beheersmaatregelen handmatig verwerken resultaten

Functiescheiding
In de nieuwe situatie kan een Medewerker ED/NT2 een officieel verzoek voor een handmatige mutatie (VHM) indienen voor . De IPO-Medewerker (Informatie Punt Onderwijs) neemt het verzoek in behandeling en kan de mutatie verwerken. Hier wordt dus functiescheiding toegepast tussen aanvraag en behandeling. Een aanpassing kan binnen alleen plaatsvinden als een VHM in behandeling is.

Schrijfrechten
Een IPO-medewerker kan alleen een mutatie uitvoeren indien deze schrijfrechten heeft, als onderdeel van de rol op zijn account. Dit wordt buiten de applicatie geregeld, door fysiek de url's te blokkeren waar iemand geen toegang tot heeft. Slechts een beperkt aantal IPO-medewerkers mogen handmatige mutaties/aangepaste uitslagen verwerken. De beheerschermen zijn momenteel nog in ontwikkeling.

Vierogencontrole
Binnengekomen verzoeken van handmatige mutaties moeten binnen vijf werkdagen zijn behandeld. Een dergelijk mutatieverzoek moet verschillende gegevens omvatten: Wie het verzoek indient, gegevens van de instelling, wat er aangepast moet worden, de reden voor de mutatie etc. Mutatieverzoeken worden vastgelegd in het systeem met een vermelding van de status van dat verzoek. Als het mutatieverzoek aan alle voorwaarden voldoet, wordt de gevraagde wijziging door een IPO-medewerker in verwerkt. Hierbij vindt vierogencontrole plaats, maar dit wordt niet afgedwongen door het systeem. Wanneer iemand een vals certificaat of diploma zou willen vastleggen kan dat dus zonder dat er een vierogencontrole plaats vindt.

Verschillen situatie oud en nieuw

In de nieuwe situatie met het nieuwe systeem zijn er een aantal positieve verschillen te onderkennen ten opzichte van de oude systemen

1. Ten eerste wordt de IT-infrastructuur minder complex middels een conversie van naar en naar . DUO onderzoekt momenteel om, in plaats van ,) de bron voor te laten zijn. Op die wijze zou de infrastructuur nog minder complex en minder foutgevoelig worden. Ten aanzien van VO-staatsexamens vindt deze conversie overigens (nog) niet plaats, omdat de bijbehorende keten daarvoor nog te complex is.

2. Een tweede verschil betreft de autorisaties van medewerkers. Dit aspect is afgestemd met de afdeling Compliancy. In de nieuwe situatie hebben medewerkers inzage- en printrechten, en slechts een beperkt aantal medewerkers mogen mutaties/uitslagen verwerken. Resultaten worden aangeleverd via het Zakelijk Portaal (m.b.v. een token op naam) in plaats van via e-mail. Deze worden dus niet meer handmatig in overgenomen door een medewerker van DUO. Uitzondering hierop is dat aangepaste examens per mail aangeleverd zullen blijven worden. Deze worden dus wel handmatig opgevoerd door een DUO-medewerker. Dit zijn er heel weinig.

3. Een derde verschil betreft het toekennen van een diploma. In de nieuwe situatie bepaalt het systeem zelf welke personen recht hebben op een diploma op basis van een geprogrammeerde regels, soort beslisboom. Hierbij voert automatisch een vijftal application controls uit.

4.5 Beheersmaatregelen Gegevensmagazijn

Gegevensmagazijn als beheersmaatregel
Het Gegevensmagazijn is in zekere zin zelf een beheersmaatregel, omdat hiermee de DR-applicatie geen rechtstreekse toegang wordt verleend tot de databases. De toegang verloopt via de GGM-API, waardoor de toegang wordt beperkt tot de noodzakelijke gegevens.

Authenticatie en autorisatie
Zoals in hoofdstuk 2 is toegelicht kan het DR gezien worden als "viewer" van de diploma's in onderliggende registers. De GGM-API is de link tussen deze viewer en de data in de registers. Deze service is verantwoordelijk voor het ophalen van de juiste gegevens uit de juiste databaseschema's. Wanneer hierbij fouten worden gemaakt bestaat het risico dat gegevens onjuist worden weergegeven. De GGM-API kan echter enkel informatie in de databases lezen, en niet wijzigen of verwijderen. Wanneer onbevoegden de GGM-API zouden aanroepen kan dit een vertrouwelijkheidsrisico vormen. Er vindt echter geen authenticatie en autorisatie van de bevragende applicatie plaats dus hiermee kan niet worden voorkomen dat GGM door onbevoegden binnen DUO kan worden aanroepen.

Logging en monitoring
DUO houdt bij door wie (welke applicaties/services) GGM wordt aangeroepen en welke data is opgevraagd (welke URIs). Met deze informatie worden rapportages gegenereerd, welke worden gemonitord door de product owners van het GGM en de betreffende applicaties. Hierdoor kunnen afwijkingen worden gedetecteerd.

Beschermen vertrouwelijke gegevens
Bij het ontwikkelen van services en applicaties wordt rekening gehouden met de bescherming van vertrouwelijke gegevens zoals BSN's.

4.6 Recapitulatie getroffen beheersmaatregelen

Het risico van diploma's die onjuist zijn of ten onrechte geregistreerd staan in de registers moet zo veel mogelijk gemitigeerd worden. Om de betrouwbaarheid van de onderwijsresultaten te waarborgen zijn er door DUO vele beheersmaatregelen (BM) getroffen, die apart of in combinatie met andere, risico's mitigeren en bijdragen aan een betere betrouwbaarheid van het DR.

De volgende beheersmaatregelen zijn getroffen:

Maatregelen DUO-breed
1. Fysieke toegangscontrole
2. Logische toegangscontrole
3. Beperkte autorisaties beheerschermen
4. (Beperkte) autorisaties databaseniveau
5. Logging van relevante acties en gebeurtenissen
6. Werkinstructies en procesbeschrijvingen
7. Datamanipulaties: registratie, autorisatie, vierogencontrole, logging
8. Datamanipulatie: monitoring
9. Wijzigingsbeheer
10. Hacktesten en securitytesten

Maatregelen registers
11. Programma van eisen (handleiding)
12. Application controls / functionele controles op de aangeleverde onderwijsresultaten
13. Inhoudelijke controles op de aangeleverde onderwijsresultaten
14. Ontvangstbevestiging (geautomatiseerd) automatisch of handmatig te verwerken onderwijsresultaten
15. Terugkoppeling (automatisch) verwerkte of afgekeurde geautomatiseerde onderwijsresultaten
16. Terugkoppeling (handmatig) verwerkte of afgekeurde handmatige mutatie
17. Vierogencontrole
18. Afgedwongen vierogencontrole
19. Archivering verwerkte handmatige mutaties (indirecte BM)
20. Kwaliteitscontrole door afdeling kennis- en leercentrum (KLC)
21. Overzichtsbestand verwerkte handmatige mutaties (indirecte BM)
22. Registratieoverzicht met vastgelegde gegevens voor onderwijsinstellingen (indirecte BM)
23. Automatisch aanleveren en registratie onderwijsresultaten
24. Automatisch toewijzen beoordelaar bij handmatige beoordeling examens
25. Automatisch vastleggen examenresultaat en bepalen behalen diploma aan de hand van een beslisboom
26. Functiescheiding
27. Controleoverzicht verschillen databases)
28. Bepalen recht diploma met behulp van query
29. Beperking schrijfrechten

Maatregelen GGM en DR algemeen

30. Authenticatie en autorisatie
31. Document-signing
32. Logging en monitoring van opvragingen
33. Gegevensmagazijn als beheersmaatregel
34. Bescherming vertrouwelijke gegevens

Onderkende risico's:

1. Ten onrechte tonen van een diploma (bijv. valse diploma)
2. Inhoudelijk onjuiste diploma
3. Ten onrechte lezen van onderwijsresultaten

Elk van de beheersmaatregelen dragen bij (indien correct werkend) aan het mitigeren van de bovenstaande drie onderkende risico's. In onderstaande twee tabellen wordt aangegeven welke beheersmaatregel welk risico kan verkleinen. Een vinkje in de kolom betekent niet bij voorbaat dat risico's zijn afgedekt, enkel dat er een beheersmaatregel aanwezig is die de risico's kan verkleinen.

Ter illustratie: de derde beheersmaatregel draagt bij niet bij aan het mitigeren van de risico's. Voor de overige registers is dit wel het geval.

Van de getroffen beheersmaatregelen bij de registers BRON MBO, VO, HO en de DUO-brede beheersmaatregelen, is opzet, bestaan en werking vastgesteld. Van de getroffen beheersmaatregelen bij overige registers, GGM en DR is alleen de opzet vastgesteld.

Getroffen beheersmaatregelen per register gekoppeld aan de 3 onderkende risico's:

BM	BRON MBO	BRON VO	BRON HO	ISI			Risico gemitigeerd
1	√	√	√	√	√	√	R1, 2 en 3
2	√	√	√	√	√	√	R1, 2 en 3
3	√	√	√	√	x	√	R1, 2 en 3
4	√	√	√	√	√	√	R1, 2 en 3
5	√	√	√	√	√	√	R1, 2
6	√	√	√	√	√	√	R1, 2
7	√	√	√	√	√	√	R1, 2
8	x	x	x	x	x	x	R1, 2
9	√	√	√	√	√	√	R1, 2
10	√	√	√	√	√	√	R1, 2 en 3
11	√	√	√	-	-	-	R1, 2
12	√	√	√	*	√	√	R1, 2
13	√	√	√	*	√	√	R1, 2
14	√	√	√	*	*	*	R1, 2
15	√	√	√	*	*	*	R1, 2
16	√	√	√	*	*	*	R1, 2
17	√	√	√	√	√	√	R1, 2
18	x	x	x	√	x	x	R1, 2
19	√	√	√	*	*	*	R1, 2
20	√	√	x	-	-	-	R1, 2
21	√	√	√	-	√	-	R1, 2
22	√	√	√	-	-	-	R1, 2
23	√	√	√	√	√	√	R1, 2
24	-	-	-	√	-	-	R1, 2
25	-	-	-	√	-	√	R1, 2
26	√	√		√	√		R1, 2
27	-	-	-	-	√	-	R1, 2
28	-	-	-	-	√	-	R1, 2
29	√	√	√	*	*	√	R1, 2

Getroffen beheersmaatregelen bij GGM en DR algemeen gekoppeld aan de 3 onderkende risico's:

BM	GGM	DR	Risico gemitigeerd
1	V	V	R1, 2 en 3
2	V	V	R1, 2 en 3
3	V	V	R1, 2 en 3
4	V	V	R1, 2 en 3
5	V	V	R1, 2
6	V	V	R1, 2
7	V	V	R1, 2
8	X	X	R1, 2
9	V	V	R1, 2
10	V	V	R1, 2 en 3
30	X	V	R1, 2 en 3
31	-	V	R1, 2
32	V	V	R3
33	V	-	R1, 2
34	V	-	R3

V aanwezig
X niet aanwezig
- niet van toepassing
* niet vastgesteld
R1 mitigeren risico 1
R2 mitigeren risico 2
R3 mitigeren risico 3

5 Aandachtspunten/verbetermogelijkheden

In dit hoofdstuk wordt beschreven welke aandachtspunten/verbetermogelijkheden worden onderkend.

Onderzoeksvraag 4 wordt in dit hoofdstuk beantwoord.

Welke aandachtspunten/verbetermogelijkheden gericht op de betrouwbaarheid (vertrouwelijkheid en integriteit) van de getoonde onderwijsresultaten in het diplomaregister worden door de ADR onderkend?

Om antwoord op deze onderzoeksvraag te kunnen geven worden aandachtspunten en verbetermogelijkheden toegelicht voor elk register onderliggend aan het diplomaregister (DR). In tegenstelling tot de voorgaande onderzoeksvraag wordt elk register hier separaat besproken.

5.1 Algemeen

Autorisatiebeheer registers risicogericht inrichten
Autorisatiebeheer is en blijft een bekend aandachtspunt voor DUO. Dat geldt DUO-breed en heeft ook impact op de betrouwbaarheid van het DR. Met name te ruime beheerrechten op de databases vormen een risico voor de integriteit van de gegevens in de registers. Dergelijke risicovolle autorisaties vergen de hoogste prioriteit. Naast het integriteitsrisico is autorisatiebeheer ook van belang om de vertrouwelijkheid van data te waarborgen. De AVG dwingt organisaties om goed na te denken over het verwerken en beschermen van persoonsgegevens. In het kader van de AVG hebben organisaties onder andere de plicht om intern vertrouwelijk om te gaan met gevoelige (persoons)gegevens en de uitwisseling daarvan. Daartoe dient een autorisatiebeheerproces te worden vormgegeven waarin de uitgifte van mutatie- en leesrechten niet op een *nice-to-know* maar *need-to-know* wijze plaatsvindt.

De afgelopen jaren is het bewustzijn van het belang van autorisatiebeheer binnen DUO toegenomen. Er wordt hard gewerkt aan het verbetertraject Autorisatiebeheer In Control (AIC). Ook wanneer de bevinding op autorisatiebeheer straks kan worden afgeschaald is het van belang aandacht te blijven houden voor de PDCA-cyclus (Plan Do Check Act) van autorisatiebeheer. Dit is een continu proces.

Aandachtspunten ten aanzien van mutatierechten binnen de DUO-registers worden, indien door de ADR onderkend, verderop in dit rapport per register aangeduid. Ten aanzien van leesrechten binnen DUO geldt voor alle registers onderliggend aan het DR dat deze ruim uitgegeven worden. Daardoor is het risico op niet-legitieme inzage van gegevens aanwezig.

- Richt autorisaties (zowel lees- als mutatierechten) in volgens need-to-know en least-privilege principes, en niet volgens een nice-to-know principe. Geef prioriteit aan de meest risicovolle systemen en processen;
- Onderschat interne risico's door menselijk handelen niet, zoals het risico op datalekken door medewerkers (bedoeld of onbedoeld);
- Laat de aandacht voor autorisatiebeheer niet verslappen na afloop van het AIC-traject.

Loginformatie risicogericht monitoren
Binnen DUO wordt veel gebruik gemaakt van logging, dit is een positieve ontwikkeling. Wanneer loginformatie echter niet proactief gemonitord wordt, wordt deze niet optimaal benut. De mate waarin binnen DUO actief wordt gemonitord verschilt per domein en proces.

Een verbetermogelijkheid is om loginformatie niet enkel correctief, maar ook preventief, detectief en repressief in te zetten. Monitor risicogericht, gebruik per proces een risicoanalyse als uitgangspunt voor het inrichten van logging en monitoring. Ook hierbij is het van belang interne risico's door eigen medewerkers (bedoeld of onbedoeld) niet te onderschatten.

Datamanipulaties beperken en monitoren
Directe ingrepen op de database zijn riskant en ongewenst. DUO onderkent dit gegeven, maar in de praktijk worden datamanipulaties nog altijd veelvuldig uitgevoerd, bijvoorbeeld bij gebrek aan functionaliteit in beheerschermen. Databasetransacties worden veelal gelogd maar niet gemonitord.

- Stuur actief aan op het beperken van directe ingrepen op de databases. Geef prioriteit aan oplossing (zoals het bouwen van extra functionaliteit in beheerschermen) waarmee datamanipulaties in de toekomst kunnen worden voorkomen;
- Overweeg risicogerichte monitoring van datamanipulaties;
- Zorg voor een duidelijke werkinstructie met beheersmaatregelen om risico's van datamanipulaties te beperken. Neem functiescheiding (tussen opstellen script en uitvoeren) en collegiale review hierin mee.

5.2 BRON MBO

Muteren alleen op basis van verzoek onderwijsinstelling
Ten eerste wordt er, net zoals bij BRON HO en BRON VO, niet systematisch uitgesloten dat een DUO-medewerker een handmatige mutatie verricht zonder dat daar een verzoek vanuit de onderwijsinstelling aan ten grondslag ligt. Ook voor BRON-MBO moet er omwille van de betrouwbaarheid van de diploma's dus ingeregeld worden dat er alleen gemuteerd kan worden op verzoek van de instelling.

Afdwingen vierogencontrole
Ten tweede zijn er, net als bij BRON HO, aandachtspunten ten aanzien van collegiale controle. Ook voor BRON MBO geldt dat vierogencontrole in de regel wordt toegepast, maar niet wordt afgedwongen in de geautomatiseerde systemen. Om er zeker van te zijn dat collegiale controle werkelijk wordt toegepast moet systematisch worden afgedwongen.

Inregelen toegankelijke loggingsgegevens
Ten derde is ook bij BRON MBO onduidelijk gebleven in welke mate digitale logging plaatsvindt. Om eventuele fouten te kunnen digitaal te kunnen achterhalen en (terug) te koppelen aan een individu wordt digitale logging onderkend als zijnde een verbetermogelijkheid.

Controle KLC op handmatige mutaties vanuit systeem
Ten vierde kwam in het onderzoek naar voren dat verwerkte handmatige mutaties van onderwijsresultaten steekproefsgewijs gecontroleerd worden door KLC op de kwaliteit van verwerking. Deze steekproef vindt plaats op de verwerkte mutaties die op de afdeling liggen. Het zou beter zijn om verwerkte handmatige mutaties uit het geautomatiseerde systeem te controleren, om de kans te vergroten dat mutaties zonder verzoek van een onderwijsinstelling gesignaleerd worden.

Terugkoppelingsmail verwerkte handmatige mutatie automatiseren
Tot slot wordt de bevestiging van een verwerkte mutatie handmatig opgesteld en verstuurd naar de betreffende onderwijsinstelling. Hier loopt DUO een risico dat er geen bevestiging wordt gestuurd naar de onderwijsinstelling bij een mutatie zonder verzoek. In theorie zou het daardoor mogelijk zijn om een nepdiploma op te voeren, zonder dat een onderwijsinstelling daarover geïnformeerd wordt.

5.3 BRON VO

De diploma's zoals aangeleverd vanuit de onderwijsinstellingen worden geacht juist en betrouwbaar te zijn. De onderwijsinstellingen zijn dus zelf verantwoordelijk voor de inhoud van de diploma's. Het is daarom belangrijk om systematisch af te dwingen dat er uitsluitend op verzoek van een onderwijsinstelling handmatige mutaties verricht kunnen worden. Anders kunnen er ongeautoriseerde mutaties plaatsvinden, met alle mogelijke gevolgen van dien.

Koppelen handmatige mutatie aan fysiek verzoek
Volgens de BRON VO-medewerkers is het mutatiescherm niet gekoppeld aan het verzoekenscherm. Hierdoor is het mogelijk om handmatige mutaties te verrichten zonder dat daar een verzoek vanuit de onderwijsinstelling aan ten grondslag ligt. Om de betrouwbaarheid van diploma's in het BRON VO-register te borgen is een verbetersuggestie om een koppeling tussen het mutatie- en verzoekenscherm te creëren.

5.4 BRON HO

Uitbreiden application controls
Ten eerste zijn er verbetermogelijkheden ten aanzien van de input controls. Hoewel er application controls zijn ingericht om de ontvangen diploma's te toetsen aan een aantal randvoorwaarden, is de set minder uitgebreid dan die van BRON VO. Er wordt bij BRON HO bijvoorbeeld niet gecontroleerd of de persoon wel ingeschreven stond bij de betreffende opleiding. Het opgeven van een studentnummer is daarbij ook niet verplicht. Daarnaast ontbreken er zekere "logica-controles" zoals leeftijd.

Afdwingen vierogencontrole
Ten tweede zijn er aandachtspunten ten aanzien van collegiale controle. Hoewel vierogencontrole naar voren komt in procedures en werkinstructies, is dit niet afgedwongen in de geautomatiseerde systemen. Op dit moment worden afgehandelde handmatige mutaties geprint in het bakje "te controleren" gelegd. In theorie zou één medewerker de mutatie daarom volledig zelfstandig kunnen verrichten. Om de toepassing van collegiale controle te borgen is het belangrijk dat dit systematisch wordt afgedwongen. Dit kan gedaan worden door de toepassing van application controls die verifiëren dat de userID van de mutator anders is dan de userID van de controleur. Ook moet er worden ingeregeld dat de mutatie niet definitief wordt doorgevoerd zonder dat de controleur deze geaccordeerd heeft.

Koppelen handmatige mutatie aan fysiek verzoek
Ten derde wordt er, net als bij BRON VO, niet systematisch uitgesloten dat een DUO-medewerker een handmatige mutatie verricht zonder dat daar een verzoek vanuit de onderwijsinstelling aan ten grondslag ligt. Ook voor BRON HO is het creëren van een koppeling tussen het mutatie- en verzoekenscherm daarom een verbetersuggestie.

Inregelen toegankelijke loggingsgegevens
Ten vierde is in het onderzoek onduidelijk gebleven in welke mate logging plaatsvindt bij de verwerking van handmatige mutaties. Logging vormt een belangrijke basis voor repressieve controle binnen de interne procesbeheersing. Door logging kan er immers gecontroleerd worden welke medewerker een mutatie heeft verricht, waardoor

eventuele fouten kunnen worden (terug)gekoppeld aan een individu. In het onderzoek kwam wel naar voren.

Controle op verwerking HM op basis van document onderwijsinstelling
Tot slot kwam in het onderzoek naar voren dat er in gelogd wordt of een mutatie is doorgevoerd door de betreffende onderwijsinstelling of door een BRON HO medewerker. In dit laatste geval zou er dus een mutatieverzoek vanuit de onderwijsinstelling aanwezig moeten zijn. Dit wordt echter niet gecontroleerd door de BRON HO medewerkers. Vanuit functioneel beheer (FB) wordt soms gekeken naar het aantal verwijderde deelnames en resultaten, maar niet of daar een verzoek vanuit een instelling aan ten grondslag ligt. Nadat de ADR dit had aangekaart bij FB, hebben ze direct een beheersmaatregel getroffen in de vorm van een query met verwerkte handmatige mutaties over een bepaalde afgelopen periode. Met de output van de query kunnen medewerkers van de Helpdesk wekelijks vaststellen of aan de handmatige mutatie een brondocument van de instelling ten grondslag ligt.

5.5 Inburgering (ISI)

Bij Inburgering zijn de meeste processen geautomatiseerd. Bij de handmatige procestap van het beoordelen van de examenonderdelen lezen en schrijven zijn zeer goede beheersmaatregelen getroffen. We hebben daarom geen aandachtspunten/verbetermogelijkheden voor dit proces.

5.6 NT2- en VO-staatsexamens ( )

Aangezien voor de registratie van NT2-staatsexamens met ingang van juli 2021 gebruik wordt gemaakt van een nieuw en verbeterd systeem is dit voor ons het uitgangspunt voor wat betreft het onderkennen van aandachtspunten en verbetermogelijkheden. Dit systeem is nog niet in gebruik voor de VO-staatsexamens. Hierbij gaan we uit van het oude systeem .

NT2-staatsexamen ( )

Afdwingen vierogencontrole
Net als bij BRON HO en BRON MBO wordt vierogencontrole niet systematisch afgedwongen binnen In de procedures en werkinstructies komt de instructie tot collegiale controle wel naar voren, maar dat is niet voldoende om verzekerd te zijn van de werkelijke toepassing daarvan. Om collegiale controle systematisch af te dwingen kunnen application controls ingeregeld worden die verifiëren dat de userID van de mutator anders is dan de userID van de controleur. Ook moet er worden ingeregeld dat de mutatie niet definitief wordt doorgevoerd zonder dat de controleur deze geaccordeerd heeft.

VO-staatsexamen)

Overgaan op individuele accounts met bijbehorende autorisaties
In het onderzoek kwam naar voren dat DUO-medewerkers gebruik maken van één gezamenlijke inlognaam en wachtwoord. Hierdoor is er geen inzicht in welke medewerker een diploma heeft opgevoerd of gecontroleerd. Ook kan door dit gezamenlijke account niet gemonitord worden in hoeverre collegiale controle wordt toegepast. Het is daarom van belang om de medewerkers uitsluitend individuele accounts te geven. In deze individuele accounts moet het autorisatiebeheer dusdanig worden vormgegeven dat slechts een beperkt aantal medewerkers rechten krijgt om diploma's uit te geven.

Vaststellen uniforme definitie diplomadatum
Daarnaast is het van belang om een uniforme definitie vast te stellen ten aanzien van de te hanteren diplomadatum, zodat de data in en L overeenkomen en de juiste datum wordt getoond in het DR. Wanneer ook de registratie van de VO-staatexamens overgaat op zal de datum van het laatste examen uitgangspunt vormen voor hetgeen in het DR wordt getoond. Dit is in lijn met wet- en regelgeving.

5.7 Gegevensmagazijn

GGM-API beveiligen
GGM is een belangrijke schakel in de DR-keten en kan gezien worden als Single Point Of Failure. API's kunnen worden beveiligd door middel van authenticatie en autorisatie van applicaties die de API bevragen, bijvoorbeeld met behulp van API-keys of JWTs (JSON Web Tokens). Dit wordt momenteel niet gedaan. Door de identiteit van de afnemer van de API vast te stellen en vervolgens te bepalen of deze de API mag gebruiken kan de toegang tot de API (en dus de achterliggende database) worden bewaakt.

5.8 Recapitulatie aandachtspunten/verbetermogelijkheden

De volgende aandachtspunten/verbetermogelijkheden worden onderkend:
- Autorisatiebeheer registers risicogericht inrichten (algemeen)
- Loginformatie risicogericht monitoren (algemeen)
- Datamanipulaties beperken en monitoren (algemeen)
- Muteren alleen op basis van verzoek onderwijsinstelling (BRON MBO/VO/HO)
- Inregelen toegankelijke loggingsgegevens (BRON MBO/HO)
- Controle KLC op handmatige mutaties vanuit systeem (BRON MBO/VO)
- Terugkoppelingsmail verwerkte handmatige mutatie automatiseren (BRON MBO)
- Uitbreiden application controls (BRON HO)
- Koppelen handmatige mutatie aan fysiek verzoek (BRON VO/HO)
- Afdwingen vierogencontrole (BRON MBO/VO//HO,)
- Overgaan op individuele accounts met bijbehorende autorisaties ( )
- Vaststellen uniforme definitie diplomadatum ( )
- GGM-API beveiligen (GGM)

6 Verantwoording onderzoek

In de opdrachtbevestiging is aangegeven dat we onderzoek gaan doen naar de betrouwbaarheid van het diplomaregister (keten) en de betrouwbaarheid van de tool EMREX. Omdat EMREX geen onderdeel uitmaakt van de keten diplomaregister en we daardoor andersoortige werkzaamheden hebben verricht, hebben we de EMREX-bevindingen in een separaat deelrapport opgenomen.
In dit eindrapport wordt verantwoording afgelegd over het onderzoek naar de betrouwbaarheid van het diplomaregister. De verantwoording over het onderzoek naar de betrouwbaarheid van de EMREX-tool is afgelegd in het EMREX-deelrapport.
De managementsamenvatting van het EMREX-deelrapport hebben we in bijlage 1 van dit eindrapport opgenomen.

6.1 Werkzaamheden en afbakening

Werkzaamheden
Om de onderzoeksvragen te kunnen beantwoorden, hebben we de volgende werkzaamheden uitgevoerd:

1. Op basis van de aangeleverde informatie hebben we aanvullend met relevante functionarissen interviews gehouden. De te interviewen personen zijn onder andere door de opdrachtverstrekker aangegeven en mede op basis van de aangeleverde documentatie bepaald. Van de interviews hebben wij verslagen opgesteld en teruggekoppeld voor hoor en wederhoor.
2. Waar van toepassing hebben wij kennisgenomen van documenten ter ondersteuning van de in de interviews verstrekte informatie.
3. Bij het onderzoek naar de registers BRON VO, BRON MBO, BRON HO en bij "autorisaties databaseniveau" en bij "wijzigingsbeheer" is gebruik gemaakt van de uitkomsten van de wettelijke controle OCW Bekostiging uitgevoerd door de ADR in 2020/2021.
4. De bij punt 2 en 3 verzamelde informatie is gebruikt voor de analyse, beantwoording van de onderzoeksvragen, de doelstelling en eventuele aandachtspunten/verbetermogelijkheden.
5. Het conceptrapport met de resultaten van het onderzoek is eerst met de contactpersoon en de gedelegeerd opdrachtgever besproken, voordat het definitieve rapport is uitgebracht aan de opdrachtgever.

Daarmee hebben we de overeengekomen werkzaamheden conform de opdrachtbevestiging uitgevoerd. De onderzoeksvragen en afbakening zoals vermeld in paragraaf 1.2 respectievelijk paragraaf 1.3 zijn aangehouden.

Wijziging ten opzichte van opdrachtbevestiging
In de opdrachtbevestiging is aangegeven dat de deelrapportage van het onderzoek naar de betrouwbaarheid van EMREX als bijlage in de eindrapportage van het onderzoek Betrouwbaarheid diplomaregister zou worden opgenomen. Gedurende het onderzoek is besloten en afgestemd met de opdrachtverstrekker dat niet het gehele deelrapport als bijlage zal worden opgenomen, maar alleen de managementsamenvatting. Dit vanuit het oogpunt van informatiebeveiliging. Derden kunnen makkelijker misbruik maken van het systeem als bepaalde kwetsbaarheden openbaar worden gemaakt.

Het EMREX-deelrapport is afgestemd met en verstrekt aan de (gedelegeerd) opdrachtgever.

6.2 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.

6.3 Verspreiding rapport

De opdrachtgever, Rudi Snijders, Hoofddirecteur Uitvoering DUO, 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.

7 Ondertekening

Groningen, 22 oktober 2021

Auditdienst Rijk

9 Bijlage 2 Managementreactie DUO op rapportage onderzoek betrouwbaarheid diplomaregister en EMREX

De managementreactie van DUO is opgenomen op pagina 43, 44 en 45.

Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

DEFINITIEF
ADR

Directie
R&E

Afdeling
Internationale Diensten

Contactpersoon

Datum
05-10-2021

memo

Managementreactie Onderzoeksrapport Betrouwbaarheid Diplomaregister en Onderzoek Betrouwbaarheid EMREX.

Geachte heer/mevrouw,

Het Diplomaregister (DR) is in 2012 gerealiseerd met een drietal heel concrete doelen: 1. Het voorzien in een voorziening in gevallen van verlies of diefstal van diploma's, 2. Het vereenvoudigen van administratieve lasten en 3. Het bestrijden van fraude met diploma's.

Na een aanvankelijk bewust voorzichtige promotie van het DR kan nu worden geconcludeerd dat het DR inmiddels zeer breed bekend is bij de onderwijsinstellingen, ministeries en bestuursorganen en de Nederlandse burger. Het DR toont inmiddels meer dan 10 miljoen diplomagegevens en naar verwachting worden er in 2021 meer dan 1,5 miljoen Pdf's gedownload uit het DR door de burger als digitaal bewijs van behaalde diploma's. In de meeste gevallen gebruikt de burger dit om bij sollicitaties of opleidingen aan te tonen dat hij het vereiste diploma heeft behaald. Ook werkgeversvragen meer en meer om harde bewijzen in het kader van pre-employmentscreening c.q. sollicitatieprocedures. Hiermee wordt fraude met diploma's, een wereldwijd probleem, adequaat bestreden.
Alles valt en staat bij de betrouwbaarheid van de gegevens die in de DUO-registers zijn opgeslagen en via het DR aan de burger en aan wettelijk bevoegde instanties worden getoond (?) .q. verstrekt.

Het DR heeft zich verder ontwikkeld en wordt ook gebruikt voor de uitwisseling van Diplomagegevens met het buitenland met het oog op het digitaliseren van het inschrijvingsproces van buitenlandse studenten in Nederland en Nederlandse studenten die in het buitenland (in het bijzonder Vlaanderen) gaan studeren. De oprichting van het zogenaamde Groningen Declaration Network is hier een van de meest concrete uitingsvormen van. Bovendien is in samenwerking met andere Europese partners (Diplomaregisters) een uitwisselingsstandaard (ELMO) en een samenwerkingsorgaan (EMREX) gerealiseerd.

In de loop van de jaren is DUO geconfronteerd met meerdere situaties van diplomafraude. Daarbij kan het gaan om zogenaamde Diploma Mills (frauduleuze organisaties die zich uitgeven als onderwijsinstelling en fake diploma's verstrekken) of diploma-aanbieders die via internet nagemaakte diploma's van bestaande opleidingsinstellingen te koop aanbieden. In het ergste geval wordt daarbij ook nog de belofte gedaan dat het gekochte diploma ook staat geregistreerd in het DR van DUO.

In geval van diplomafraude doet DUO altijd aangifte bij het Openbaar Ministerie en enkele keren heeft dit ook tot vervolging en veroordeling geleid.
Bovendien hebben deze fraudegevallen diverse malen geleid tot interne onderzoeken naar de betrouwbaarheid van het DR.

Om absoluut zeker te zijn van de betrouwbaarheid van het DR en elke vorm van twijfel uit te sluiten, heeft DUO aan de ADR de opdracht verstrekt zowel het DR als EMREX nauwkeurig onder de loep te nemen.

Het door de ADR uitgevoerde onderzoek naar het DR geeft een uitstekende weergave van de werking van het DR, de onderliggende registers en de werkprocessen die binnen DUO worden uitgevoerd.
DUO is de ADR bijzonder dankbaar voor het gedegen onderzoek, de conclusies en de geformuleerde verbeterpunten.

Het is geruststellend om te constateren dat de betrouwbaarheid van het Diplomaregister gegarandeerd is en dat het uitgesloten is dat kwaadwilligen gegevens die via het DR worden getoond kunnen toevoegen c.q. manipuleren.

Het rapport bevat tevens een aantal aanbevelingen. Deze aanbevelingen zijn erop gericht de interne processen en procedures met betrekking tot de onderliggende systemen verder aan te scherpen.
Deze bevinden zich vooral op het vlak van het verstrekken van autorisaties waarmee medewerkers diplomagegevens ten onrechte kunnen inzien. Dit is weliswaar onwenselijk, maar vormt geen bedreiging voor de betrouwbaarheid van het DR zelf. Autorisatiebeheer is een belangrijk aandachtspunt voor DUO en diverse verbetermaatregelen op dit vlak zijn reeds genomen. Alle bevindingen zijn inmiddels voorgelegd aan het compliance platform van de directie Registers & Examens (R&E) en waar nodig zullen nog verbetermaatregelen in de interne procedures en werkprocessen worden geformuleerd en uitgevoerd.

In het verlengde van het onderzoek naar de betrouwbaarheid van het DR is op verzoek van de Businessmanager Internationale Diensten (ID) ook een onderzoek uitgevoerd naar EMREX. EMREX, ontwikkeld in opdracht van de EC, heeft als doel het inschrijvingsproces van internationale studenten van het ene land naar het andere land te vergemakkelijken en sneller, betrouwbaarder en veiliger te maken.
De ADR-bevindingen ten aanzien van EMREX zijn vooral gericht op de governance van EMREX en minder op de werking van het systeem zelf. De aanbevelingen op het bestuurlijke vlak zijn inmiddels besproken in het EMREX Steering Committee (bestuur EMREX) en er is met instemming kennis van genomen.
Zowel in het bestuur als bij de beheerder van het systeem (Noorwegen) worden maatregelen genomen die tegemoet komen aan de gedane aanbevelingen. De Dienst Uitvoering Onderwijs (DUO) is hierbij slechts gebruiker van het systeem en daarmee afhankelijk van de andere EMREX partners.

EMREX wordt bij DUO gebruikt om het inschrijvingsproces van Nederlandse internationale studenten te vergemakkelijken. Met behulp van EMREX worden de benodigde gegevens van de student op eigen initiatief automatisch verzonden

naar de partij die de inschrijving van de student bij de betrokken instelling verzorgt.
In de situatie van DUO heeft dit dan vooral betrekking op Nederlandse studenten die in Vlaanderen gaan studeren. De student geeft in elke situatie zelf toestemming deze gegevens te verstrekken. Inmiddels zijn alle ho-instellingen in Vlaanderen waar Nederlandse studenten staan ingeschreven op EMREX aangesloten.
De constateringen in het EMREX-rapport die betrekking hebben op hoe DUO EMREX gebruikt, zijn omgezet in concrete verbetervoorstellen en op de planning van het DR-team opgenomen.

Met vriendelijke groet,

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00