



Belastingdienst

Review met RAM vergelijkbare systemen

3 maart 2025

In opdracht van CIO Belastingdienst

Vertrouwelijk

Definitief versie 1.0



Opdracht

Naar aanleiding van het rapport Onderzoek Risico Analyse Model (RAM) van KPMG van 7 februari 2025.

In hoeverre heeft de eigenaar van met RAM vergelijkbare systemen inzicht of de systemen voldoen aan de Referentiearchitectuur Integrale Beveiliging en zijn voor onderkende risico's compenserende maatregelen in opzet aanwezig?

In scope zijn de door KPMG genoemde met RAM vergelijkbare systemen die nog in productie zijn:

- Gruff
- Infomatiesjabloon (IFL)
- Invorderings Hulp Programma (IHP)
- Klantbeeld Toezicht Applicatie (KTA)
- Selectie Module OB (SMOB)

(en PRISMA, in deze review buiten scope omdat het een systeem van Douane betreft)

We kijken naar de opzet, d.w.z. zoals het in documentatie beschreven staat, of als er geen documentatie is, dan zoals medewerkers denken dat het is.



Algemeen

Systeem	Soort applicatie	Welke keten	IT Architectuur
Gruff	Regulier	GKT, directie GO voelt zich aangesproken, MKB is aangehaakt	Standaard pakket met Oracle Database. Geen solution architectuur
IFL	LOA	GKT, directie MKB voelt zich aangesproken	Excel
IHP	Kritieke LOA	IenB	MsAccess, SQL-server op Linux.
KTA	Regulier	GKT, directie GO voelt zich aangesproken, MKB is aangehaakt, eventuele andere doelgroepen niet	Cobol, Java en Websphere op IPAS, DB2 database op z/OS
SMOB	LOA	GKT, keten Omzetbelasting voelt zich aangesproken	Inforay op Windows-server, Oracle Database op Linux en Browser based client

- Er is geen sluitende correlatie tussen de systemen en bedrijfsprocessen. Daarom zijn controlelijsten voor een eerdere AVG en BIO compliance uitvraag niet dekkend.
- Er is geen sluitende correlatie tussen de systemen en het verwerkingenregister.
- IFL en SMOB zijn aangemerkt als Lokaal Ontwikkelde Applicaties (LOA's). Daarom is er in de architectuur geen transitie naar een robuuste applicatie uitgewerkt. IHP is aangemerkt als kritieke LOA, echter er is geen transitie naar een robuuste applicatie uitgewerkt.

Privacy



Systeem	Welke gegevens	Bijzondere persoonsgegevens	Welke verwerking	Welk doel
Gruff	KVK en ANBI, BVR, Datafundamenten Loon, Auto en Bank	Nee	Raadplegen op unieke identificatie. Geen profilering of selectie	Verbanden tussen objecten en subjecten uit diverse systemen visueel in kaart brengen voor toezicht . Praktisch niet mogelijk via bronsystemen.
IFL	BVR, OBW, Toeslagen, BRG, Rentebase, FiBase, ABS, VBN, OB, LH. GOA/Dacas/ETM/INL, HSB, vaartuigen.	Nee	Raadplegen op unieke identificatie, geen profilering of selectie	Informatie bundelen over relateerde objecten en subjecten uit diverse systemen voor toezicht . Rechtstreek via bronsystemen is dit zeer bewerkelijk en foutgevoelig.
IHP	INL, COA, ETM, OP, GBV, MAW, BVR, Kentekens, EVP/DRZ, KIS, CSB, Dacas, LWB, IVR. Op attribuutniveau niet inzichtelijk	Nee	Raadplegen op unieke identificatie, wijzigen van invorderingskosten en deze terugleveren aan INL. Geen profilering of selectie	Leveren betaalsituatie, behandelen verzoek/klacht/beroep/bezwaar, verstrekken schuldpositie. Verwerking kan niet met reguliere applicaties omdat het lenB-landschap verouderd is.
KTA	BVR, REN, Kadaster, HSB, RIS, BRG, INL, COA, RBG, GBV, IKB, OOB, PLH, HLP, FAA, ABS, WGA, KRB, INN, VBN, FLG, ANBI/OUA	Nee	Raadplegen op unieke identificatie, geen profilering of selectie	Informatie bundelen over relateerde objecten en subjecten uit diverse systemen voor toezicht . Rechtstreek via bronsystemen is dit zeer bewerkelijk en foutgevoelig.
SMOB	BVR, OB, ICP, Sagitta-invoer	Nee	Raadplegen op unieke identificatie, geen profilering of selectie	Bundelen van binnenlandse en buitenlandse omzetbelastinggegevens voor Toezicht doordat dit niet mogelijk is in verouderde bronsystemen.

Beveiliging



Systeem	BIV	Toegang	Gegevensopslag	Gegevensuitwisseling	Logging en monitoring
Gruff	222	Via loket Alleen Gruff specialist kan bij de gegevens via rol(len) in IMS	Gruff ISS (Oracle Database) in beheer bij DF&A Export: PNG-afbeelding	In: Via Datafundament (heeft niet dezelfde actualiteit als bronsystemen) Uit: Intern via Q-schijf met mappenstructuur. Extern via mail	Historie aanvraag via loket wordt bewaard. ‘Uitzonderlijke directe opdrachten’ lopen niet via loket
IFL	222	Via loket, na goedkeuring aanvraag door goedkeurder en bij >25 subjecten extra check. Alleen CAP gegevens kan bij de gegevens via rol(len) in IMS.	Regulier via CAP gegevens Export: is Excel-bestand met macro's en Active-X blijvend ingeschakeld	In: DF&A levert regulier aan CAP gegevens Uit: Loket mailt resultaat	Historie aanvraag via loket wordt 2 jaar bewaard
IHP	222	~2.000 gebruikers Toegang via rollen in IMS	SQL-server op Linux	In: Geen documentatie ontvangen Uit: export mogelijkheden naar Excel, Word en PDF. Export MUTASV en Data entry bestanden naar INL.	Raadplegen gegevens niet gelogd. Verwerking export INL levert verwerkings- en foutverslag.
KTA	222	~22.000 gebruikers Geen onderscheid in rollen Toegang via IMS Geen check op koppeling met onderhanden werk	DB2 database op z/OS	In: Geen documentatie ontvangen Uit: Voor MKB doorklik naar KRB, voor GO schermexport naar Excel	Raadplegen gegevens wordt gelogd; geen actieve monitoring
SMOB	222	2314 gebruikers (aangegeven is dat het om raadpleegrechten gaat) Toegang via IMS	Inforay op Windows-server, Oracle Database op Linux	In: FTD	Logging op Inforay staat aan, met passieve monitoring



Totstandkoming van dit rapport

Planning

- Referentiearchitectuur Integrale Beveiliging gebruikt als normenkader
- Eventuele mitigerende maatregelen geïnventariseerd
- Interviews met betrokken ketens
- Korte doorlooptijd vanuit de opdrachtgever. Eerste deadline 14-2-2025 9:00 uur
- Documentatie aanleveren in daarvoor aangemaakte pagina in Connect People

Uitvoering

- Aanleveren door de business en verwerking door het onderzoeksteam is onder tijdsdruk tot stand gekomen. Opdrachtgever vond het belangrijk om alle aangeleverde documentatie, toelichtingen en opmerkingen te verwerken.
- Aangeleverde documentatie en opmerkingen verwerkt tot 27-2-2025 17:00 uur
- Er heeft twee maal hoor en wederhoor plaatsgevonden



Bijlagen

Gebruikt normenkader o.b.v. Referentiearchitectuur Integrale Beveiliging

Detailbevindingen Gruff

Detailbevindingen IFL

Detailbevindingen IHP

Detailbevindingen KTA

Detailbevindingen SMOB