

Inleiding

In dit document wordt de architectuur van SARO m.b.t. de Integrale Bedrijfsvoeringsoplossing voor Financiën en HRM beschreven. Deze beschrijving bestaat uit de volgende onderdelen:

1. Algemene architectuurprincipes;
2. Specifieke eisen Integrale Bedrijfsvoeringsoplossing;
3. Technische omschrijving werkplekomgeving;
4. Overzicht met koppelingen;

1. Algemene architectuuruitgangspunten

Principe #1	Gebruik standaardoplossing voor maatwerk voor zelf ontwikkelen
Motivatie	Het gebruik van standaardoplossingen minimaliseert de complexiteit en kosten, bevordert de herbruikbaarheid en de compatibiliteit van systemen. Het minimaliseren van maatwerk aan standaardoplossingen vermindert het risico op fouten, versnelt de implementatie en vereenvoudigt toekomstige upgrades. Het zelf (laten)bouwen van software wordt als alleen als optie beschouwd wanneer een standaardoplossing niet verkrijgbaar is of volledig niet past bij het interne proces. De focus ligt op het gebruik van bewezen oplossingen.
Implicatie	Pas bij de toepassing van een standaardoplossing de werkwijze aan bij de standaarden en de best-practices die aan de oplossing ten grondslag liggen. Volg waar mogelijk de inrichtingsfilosofie van leveranciers.

Principe #2	Er wordt gebruik gemaakt van generieke processen en systemen
Motivatie	Door te werken met generieke processen en systemen wordt maatwerk voorkomen. Hierdoor kan eenvoudiger gebruik worden gemaakt van standaard oplossingen die beschikbaar zijn in de markt en worden kosten bespaard.
Implicatie	Processen worden gebaseerd op generieke procesmodellen, zoals de procesmodellen die worden meegeleverd met pakketapplicaties. Bij het specificeren van functionaliteit wordt een goede balans gezocht tussen standaard inrichting en voldoende procesondersteuning. Processen en systemen worden niet ingericht op uitzonderingen. Specifieke keuzes van de organisatie worden uitgedrukt in (beleids)regels die binnen de generieke processen. Om maatwerk te voorkomen is het soms nodig de processen aan te passen.

Principe #3	Tijd- en plaats-onafhankelijk werken wordt ondersteund
Motivatie	Medewerkers willen in toenemende mate ook zelf de tijd, de plaats en het apparaat waarop zij werken bepalen. Door tegemoet te komen aan dit soort behoeften wordt de medewerkerstevredenheid verhoogd.
Implicatie	De integrale bedrijfsvoeringsoplossing is tijd-, plaats- en apparaat-onafhankelijk beschikbaar.

Principe #4	Gebruik van systemen is herleidbaar naar gebruikers
Motivatie	Om adequaat om te kunnen gaan met fouten, misbruik en fraude in IT systemen is het van cruciaal belang dat het systeem vastlegt wie

	verantwoordelijk is voor specifieke handelingen in het systeem. Dit geldt niet alleen voor reguliere gebruikers, maar vooral ook voor beheerders, die vaak meer rechten hebben en daardoor een groter risico vormen voor misbruik. Het principe niet alleen een mechanisme om individuen ter verantwoording te roepen, het is ook een belangrijk middel voor de interne beheersing en systeemgerichte controle. Door workflows, goedkeuringen en mutaties herleidbaar te maken, creëren we een efficiëntere en meer transparante omgeving waarin we kunnen vertrouwen op een betere naleving van procedures en een grotere bescherming tegen potentiële risico's van misbruik en fraude.
Implicatie	Gebruikers loggen in met een persoonsgebonden account. Gebruikers delen hun account en wachtwoord niet met andere gebruikers. Alle handelingen die gevoelig zijn voor misbruik of fraude worden gelogd in een audit trail. Indien beheerders gebruik maken van een niet-persoonsgebonden account dan voeren zij handelingen uit vanaf een tot hun persoon herleidbaar workstation of netwerktoegang en worden identificerende gegevens (bijv. het IP-nummer en de timestamp) vastgelegd bij hun handelen. Een audit trail is niet te verwijderen of aan te passen door reguliere beheerders.

Principe #5	Applicaties werken met Single Sign-On
Motivatie	Om de toegang van gebruikers tot de applicaties te vereenvoudigen wordt gebruik gemaakt van Single Sign-On. In veel gevallen is dat ook niet nodig en kan een initiële authenticatie voldoende zijn voor toegang tot allerlei applicaties. In een aantal gevallen is een extra authenticatie in de vorm van een 2^e factor gewenst, bijvoorbeeld als de gebruiker toegang probeert te krijgen tot meer gevoelige gegevens of functionaliteit.
Implicatie	Gebruikers hebben maar één account. Er zijn centrale authenticatievoorzieningen aanwezig die alle voor applicaties noodzakelijke authenticatiefunctie bieden. Applicaties voeren zelf geen authenticatie uit, maar vertrouwen op tokens die zijn gegenereerd door centrale authenticatievoorzieningen. De tweede factor voorziening wordt ook geleverd door de centrale authenticatievoorziening. Applicaties hebben zelf geen wachtwoordadministratie.

Principe #6	Eénmalige vastlegging, meervoudig gebruik
Motivatie	Gegevens dienen éénmalig vastgelegd te worden in een systeem of een gegevensbron, maar vervolgens op een gecontroleerde en gestandaardiseerde manier worden gebruikt door meerdere verschillende systemen, processen of gebruikers. Het doel van dit principe is om redundante gegevensinvoer te minimaliseren, consistentie te waarborgen en de efficiëntie van gegevensgebruik te maximaliseren.
Implicatie	Systemen moeten voorzien zijn van een REST API waarmee de informatie uitwisseling met andere systemen kan worden gerealiseerd. Het opvragen van gegevens bij de bron heeft de voorkeur boven het kopiëren van gegevens.

Principe #7	De kwaliteit van gegevens wordt zo dicht mogelijk bij de bron gecontroleerd.
-------------	--

Motivatie	De kwaliteit van gegevens is in het erg belangrijk. Door bij invoer alle gegevens grondig te controleren is de kans het kleinst dat hier vervuiling optreedt. Het is de bron zelf die het beste en meest actuele beeld heeft van de gegevens. Als de bron die de gegevens heeft ze ook levert dan worden onnodige tussenliggende lagen voorkomen. Hierdoor wordt de efficiëntie en betrouwbaarheid van de gegevens verhoogt omdat iedere schakel in de keten vertraging oplevert en een mogelijke bron van fouten is.
Implicatie	Gegevens worden uitgebreid gevalideerd voordat ze worden opgeslagen. Gebruikers worden bewust gemaakt van de consequentie van het verkeerd invullen van gegevens. Gegevens hoeven na de uitgebreide validatie niet nogmaals gevalideerd te worden. Er worden elektronische formulieren geboden aan 'klanten' waarmee ze zelf kun gegevens kunnen invoeren/wijzigen. Gegevens worden niet geschoond bij het laden van het datawarehouse. Gegevenskwaliteitsproblemen worden opgelost in het bronsysteem.

Principe #8	Gegevensuitwisselingen die frequent of in grote aantallen plaats vinden worden geautomatiseerd
Motivatie	Als gegevens frequent of in grote aantallen worden uitgewisseld dan rechtvaardigt dat de inspanning van het ontwikkelen van een geautomatiseerde gegevensuitwisseling. Daarnaast zijn handmatige gegevensuitwisselingen foutgevoelig en introduceren ze het risico op inconsistenties.
Implicatie	Er is inzicht in de frequentie en volume van gegevensuitwisselingen. Daar waar frequentie of volume hoog is wordt een integratie tussen applicaties gerealiseerd.

Principe #9	Routinematige taken worden geautomatiseerd
Motivatie	Routinematige taken vragen relatief weinig specifieke kennis en kunnen daardoor ook relatief eenvoudig geautomatiseerd worden. Geautomatiseerde taken zijn meer efficiënt in tijd en kosten en minder foutgevoelig.
Implicatie	De kennis die noodzakelijk is om bepaalde taken uit te voeren wordt geanalyseerd, en opgenomen in een IT systeem als het eenvoudig kan worden geformaliseerd. Medewerkers worden zoveel mogelijk ingezet op taken die meer complexe kennis vragen.

2. Specifieke eisen Integrale Bedrijfsvoeringsoplossing

Algemeen	1	De Integrale Bedrijfsvoeringsoplossing wordt geleverd als SaaS (Software as a Service) en wordt gehost door de leverancier.
	2	Patches, updates en upgrades worden door de leverancier geïnstalleerd. De opdrachtgever krijgt de mogelijkheid functionele updates in een acceptatieomgeving te testen. De implementatiedatum van functionele updates wordt vastgesteld in overleg met de opdrachtgever.
	3	Eventueel benodigde clientcomponenten voor het gebruik van het Integrale Bedrijfsvoeringsoplossing dienen via

		beheerde installaties beschikbaar gesteld te worden aan de opdrachtgever.
	4	De stijl van de ESS/MSS omgeving binnen de De Integrale Bedrijfsvoeringsoplossing is aanpasbaar naar de huisstijl van de opdrachtgever. Dit betreft met name de kleurstellingen en logo.
	5	De functionaliteiten voor ESS/MSS moeten ondersteunt worden in elke moderne browser zoals Microsoft Edge, Google Chrome, Mozilla Firefox, Safari op zowel desktop als mobiele besturingssystemen.
	6	Functionaliteit aangeboden via mobiele apps moet altijd ook beschikbaar zijn via de standaard interfaces van de applicatie. Een gebruiker mag niet gedwongen worden de app te installeren.
	7	Apps aangeboden op mobiele platformen moeten minimaal beschikbaar zijn op door de fabrikanten ondersteunde versies van Android en iOS.
Gebruiksvriendelijkheid	8	Aangeboden websites en apps voldoen aan de WCAG richtlijnen voor digitale toegankelijkheid niveau AA. WCAG staat voor Web Content Accessibility Guidelines. https://wcag.nl/kennis/richtlijnen/wcag-2-1-richtlijnen/
	9	Het systeem vormt één herkenbaar geheel; de schermen, kleuren, navigatie en andere basisfuncties zijn eenduidig opgebouwd.
	10	De schermen (invoer, raadpleeg en beheer) zijn overzichtelijk, duidelijk en eenvoudig opgezet, waardoor de meest voorkomende handelingen intuïtief uitgevoerd kunnen worden.
	11	De navigatie en bediening van het systeem is eenduidig. Dat wil zeggen dat deze op elke plaats binnen de Integrale Bedrijfsvoeringsoplossing op dezelfde wijze gedefinieerd en gebruikt zijn.
	12	Het systeem voorziet binnen de gebruikersinterface in een 'help'- functie voor gebruikers.
	13	Het systeem voorziet in sneltoetsen om routinematige handelingen snel toegankelijk te maken.
	14	Het systeem is geschikt voor het gebruik op twee beeldschermen op de werkplek.
Technische aansluitvoorwaarden	15	Opdrachtgever gebruikt Microsoft Entra ID als IdP (Identity Provider). Het platform van de opdrachtnemer treedt op als SP (Service Provider) en dient voor authenticatie te koppelen op basis van OpenID Connect en OAuth 2.0 naar de tenant van de opdrachtgever. Gebruik van deze koppeling voor alle gebruikersauthenticaties is verplicht.
	16	Opdrachtgever gebruikt Conditional Access vanuit Microsoft EntraID om multi-factor authenticatie af te dwingen voor de gebruikers van de applicatie. Het systeem moet deze authenticatievorm ondersteunen.

	17	Een medewerker van opdrachtgever, hoeft zich slechts eenmalig aan te melden bij de Identity Provider (Single Sign-On). De Integrale Bedrijfsvoeringsoplossing mag de medewerker niet nogmaals om inloggegevens te vragen.
	18	Verbindingen tussen de leverancier en systemen van opdrachtgever mogen enkel tot stand gebracht worden via een beveiligde verbinding.
	19	De verbinding naar de Integrale Bedrijfsvoeringsoplossing wordt (beveiligd) opgezet over het reguliere internet.
	20	Voor de beveiliging van https-verbindingen wordt minimaal gebruik gemaakt van een SSL-certificaat van het type SHA-256. De sleutellengte dient 2048-bit te zijn. Leverancier garandeert dat de beveiliging up-to-date gehouden wordt naar de geldende standaarden.
	21	Voor de beveiliging van https-verbindingen wordt minimaal gebruik gemaakt van TLS 1.2. Leverancier garandeert dat de beveiliging up-to-date gehouden wordt naar de geldende standaarden.
	22	API koppelingen moeten voorzien zijn van authenticatie- en autorisatiemechanismen (bijv. OAuth, API keys) om ongeautoriseerde toegang te voorkomen.
	23	API koppelingen moeten voorzien kunnen worden van een extra beveiligingsmaatregel. Denk aan het toestaan van verbindingen op een connector vanaf specifieke IP adressen of authenticatie met certificaten.
	24	API koppelingen zijn beschreven conform de OpenAPI Specification(OAS). De OAS beschrijft de eigenschappen van de data die een API als input accepteert en als output teruggeeft. Met OAS kunnen zowel mensen als machines de dataset attributen van een REST API vinden, bekijken en verwerken zonder toegang tot de achterliggende programmatuur of aanvullende documentatie.
	25	API koppelingen zijn voorzien van logging, controles en validatiemechanismen zijn om de integriteit en consistentie van de uitgewisselde gegevens te waarborgen.
	26	Gegevensdragers die gebruikt worden ten behoeve van de migratie van gegevens dienen voorzien te zijn van encryptie
Informatiebeveiliging	27	De leverancier laat jaarlijks een audit uitvoeren door een externe partij op de dienstverlening geleverd aan de opdrachtgever. Deze audit richt zich met name op het nakomen van de afspraken omtrent beveiliging en privacy en op kwetsbaarheden (pentest). De kosten voor deze audit zijn een integraal onderdeel van de offerte. De leverancier deelt de resultaten en verbeteracties met de opdrachtgever.
	28	De leverancier voorziet de opdrachtgever op aanvraag van de benodigde informatie voor het uitvoeren van een DPIA (Data Protection Impact Assessment)
	29	De volgende acties dienen gelogd te worden en herleidbaar te zijn naar natuurlijke personen: • Het muteren van data;

	• Het exporteren van data: Ook data die de de Integrale Bedrijfsvoeringsoplossing verlaat en daarmee niet meer getraceerd kan worden dient gelogd te worden. Voorbeelden hiervan zijn het al dan niet automatisch versturen van e-mail, het maken van data-dumps en het uitwisselen van data met andere systemen; • Het verwijderen van data; • Het raadplegen van data welke bijzondere persoonsgegevens bevat. • Beheeractiviteiten
30	Een logregels dient minimaal de volgende informatie weer te geven: • de gebeurtenis; • de benodigde informatie die nodig is om de gebeurtenis met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; • het gebruikte apparaat; • het resultaat van de handeling; • een datum en tijdstip van de gebeurtenis.
31	Er is een audittrail beschikbaar met daarin de logging informatie. Deze audittrail is alleen inzichtelijk voor daartoe geautoriseerde personen.
32	Logbestanden kunnen als leesbare tekst geëxporteerd worden in een standaardformaat zoals XML of CSV. Ieder bestand dient te zijn voorzien van informatie die een beschrijving geeft van de data in het bestand.
33	Het is niet toegestaan gevoelige informatie zoals persoonsgegevens, anders dan de gebruikersnaam of het gebruikers ID, op te slaan als gelogde informatie.
34	Logbestanden dienen 1 jaar bewaard te worden. Tevens dient leverancier te garanderen dat log informatie ouder dan 1 jaar verwijderd wordt.
35	Wanneer leverancier gebruik maakt van een shared omgeving, is de data van opdrachtgever niet te benaderen door derden die dezelfde shared omgeving gebruiken. De leverancier neemt hiervoor adequate beveiligingsmaatregelen zoals bijvoorbeeld applicatie- en serverhardening, encryptie (tijdens transport en opslag) en netwerksegmentatie zowel tijdens implementatie als bij onderhoud van de applicatie.
36	De Integrale Bedrijfsvoeringsoplossing biedt de mogelijkheid voor het instellen van meerdere autorisatieniveaus, waardoor inzage, mutatie of export van gegevens voor medewerkers van opdrachtgever beperkt of uitgebreid kan worden afhankelijk van de taak/functie/rol waarvoor zij gemachtigd zijn om specifieke gegevens in te zien of te wijzigen.
37	Opdrachtgever past functiescheiding toe om tegengestelde belangen en fraude te voorkomen. De Integrale Bedrijfsvoeringsoplossing biedt naast de standaard rollen de

		mogelijkheid tot het definiëren van eigen rollen met aangepaste autorisaties.
	38	De Integrale Bedrijfsvoeringsoplossing biedt de mogelijkheid een totaaloverzicht te maken met de ingestelde autorisaties per rol/functie(groep) en afwijkende autorisaties per medewerker. (actueel en op specifieke datum).
	39	De Integrale Bedrijfsvoeringsoplossing blokkeert de toegang voor een specifieke gebruiker tot alle interfaces zodra het gebruikersaccount door de IAM oplossing wordt geblokkeerd.
	40	Email met als afzender het domein van de opdrachtgever, verstuurd vanuit het platform van de leverancier dient te voldoen aan de beveiligingsstandaarden DKIM, DMARC en SPF.
	41	De opdrachtgever kan gebruik maken van een gescheiden test-, acceptatie- en productieomgeving. Wijzigingen in de ene omgeving mogen geen invloed hebben op het functioneren van een andere omgeving.
	42	De opdrachtgever kan gebruik maken van een testomgeving om nieuwe functionaliteit of inrichtingen van de oplossing te testen. De acceptatieomgeving wordt gebruikt om testen uit te voeren voor acceptatie van wijzigingen en nieuwe software releases. De inrichting van de productieomgeving moet eenvoudig gekopieerd kunnen worden naar de test- en de acceptatieomgeving. Wijzigingen aan de kant van opdrachtgever zullen altijd eerst in de acceptatieomgeving doorgevoerd worden, waarna getest kan worden of de Integrale Bedrijfsvoeringsoplossing, inclusief de diverse koppelingen, nog naar behoren werkt.
Stabiliteit en continuïteit	43	De Integrale Bedrijfsvoeringsoplossing beschikt over een adequate back-up voorziening die aansluit bij de gestelde eisen ten aanzien van RPO, RTO en wettelijke bewaartermijnen voor financiële- en personeelsgegevens. Leverancier voert periodiek restore-testen uit om te controleren of de back-ups consistent en herstelbaar zijn. Opdrachtgever kan zelfstandig back-ups terugzetten in de omgeving.
	44	Opdrachtgever is en blijft te allen tijde eigenaar van de data in de Integrale Bedrijfsvoeringsoplossing.
	45	Op verzoek van de opdrachtgever zal de leverancier binnen 40 werkuren alle data op een leesbare manier exporteren naar opdrachtgever, waar nodig vergezeld van documentatie over relevante onderdelen van het datamodel.
Data & Exit-strategie	46	Leverancier dient de data na afloop of bij tussentijdse beëindiging van de overeenkomst via interoperabele (open standaarden) exportformaten op verzoek van opdrachtgever beschikbaar te stellen aan, dan wel mee te werken aan de migratie van de data naar een nieuwe Integrale Bedrijfsvoeringsoplossing. Leverancier garandeert hierbij de

		volledigheid van de data. Na migratie of levering van de data, dient leverancier op verzoek van opdrachtgever de data te verwijderen van haar systemen en deze te vernietigen. Voorgaande geldt uitdrukkelijk ook voor data bestaande uit persoonsgegevens.
	47	De Integrale Bedrijfsvoeringsoplossing beschikt over interoperabele (open standaarden) exportformaten voor alle gegevens die opgeslagen zijn in het systeem.



3. Technische omschrijving werkplekomgeving

De standaard werkplek voor medewerkers binnen de omgeving van SARO is gebaseerd op een Windows 10 werkplek beheerd vanuit de centrale beheerapplicatie Microsoft Configuration Manager. De werkplekken zijn standaard voorzien van Office 365 applicaties (Word, Excel, Powerpoint), Acrobat Reader en Microsoft Edge browser. Gebruikers hebben geen administrator rechten op de lokale apparatuur. Benodigde installaties van cliënt software voor de werking van de aangeboden oplossing moeten vanuit deze beheerapplicatie aangeboden kunnen worden aan de eindgebruikers.

SARO is voornemens medio 2025 een nieuwe werkplekinrichting in gebruik neemt op basis van de Microsoft moderne werkplek welke beheerd wordt vanuit Intune.

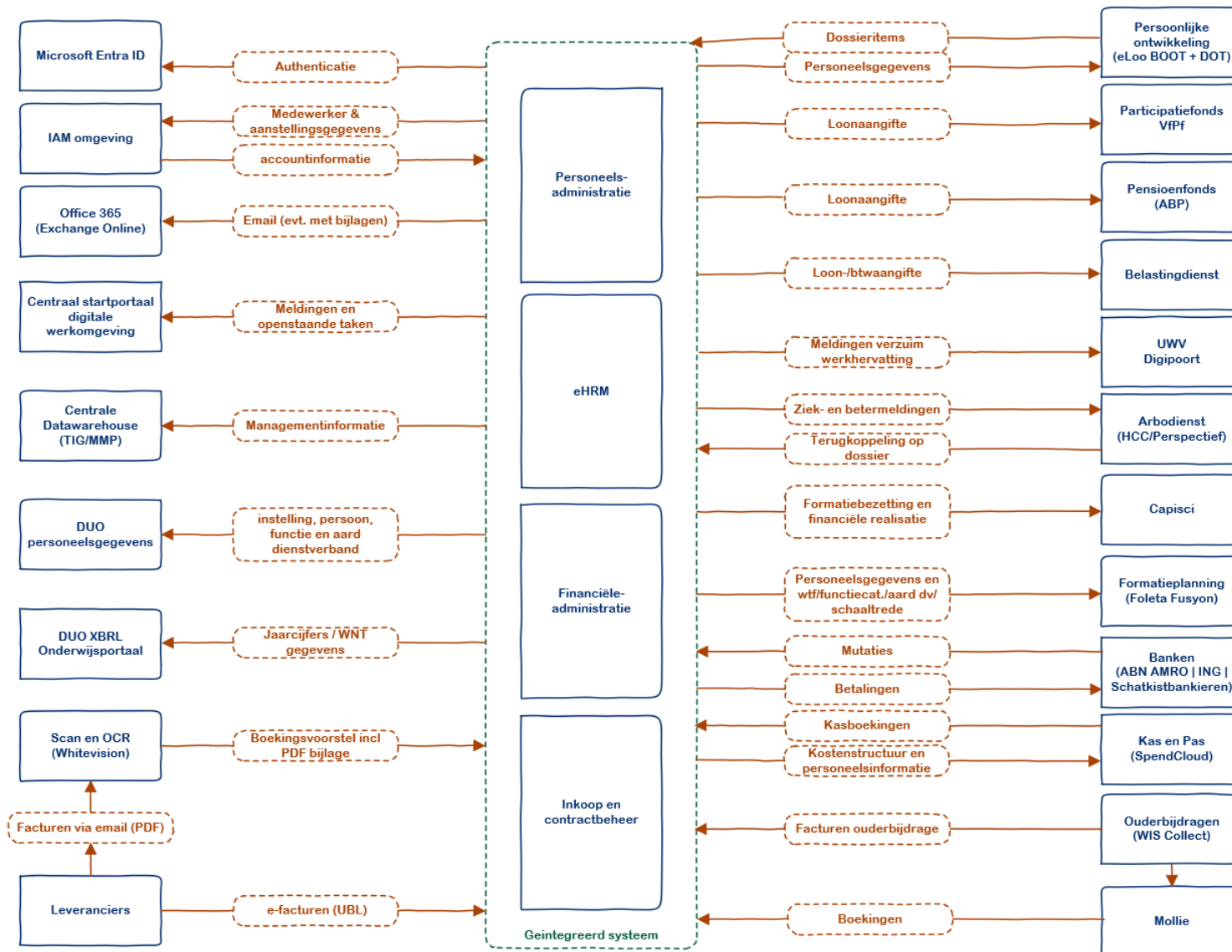
De employee self service interface wordt zowel vanuit SARO werkplekken als vanuit niet beheerde apparatuur benaderd. Deze voorzieningen moeten daarom ondersteunt worden op alle actuele versies van gangbare browsers in de markt: Microsoft Edge, Google Chrome, Mozilla Firefox, Safari op zowel desktop als mobiele besturingssystemen.

De netwerkomgeving bestaat uit twee gescheiden netwerken voor het primair en voortgezet onderwijs. De Microsoft tenants zijn ook twee gescheiden tenants. Medio 2025 worden deze tenants samengevoegd.

Architectuur

4. Overzicht koppelingen

In deze paragraaf zijn alle benodigde koppelingen van en naar de Integrale Bedrijfsvoeringsoplossing beschreven.



Domein	Verbonden applicatie	Toelichting
Algemeen	Microsoft EntraID	OpenID Connect and OAuth koppeling t.b.v. authenticatie van de gebruikers met als doel SSO te realiseren.
Algemeen	IAM omgeving	De IAM omgeving is gebaseerd op Microsoft Identity Manager. De applicatie haalt via REST/JSON protocol de gegevens van de medewerkers en aanstellingen op en gebruikt deze gegevens voor het aanmaken van o.a. het netwerkaccount. De IAM omgeving schrijft na het aanmaken van de gebruiker in de systemen de gegevens en status van het aangemaakte netwerkaccount terug naar de Integrale Bedrijfsvoeringsoplossing zodat de gebruiker via SSO kan inloggen op de Integrale Bedrijfsvoeringsoplossing.
Algemeen	Email	SARO maakt gebruik van Office365 voor het versturen en ontvangen van email. De Integrale Bedrijfsvoeringsoplossing moet kunnen koppelen met deze omgeving om email met gevoelige gegevens beveiligd te ontvangen en te versturen.
Algemeen	Centraal startportaal	SARO is voornemens een startportaal in te richten voor de medewerkers. De oplossing dient gebruiksvriendelijke interfaces te bieden om informatie betreffende openstaande acties en signalen in de Integrale Bedrijfsvoeringsoplossing te ontsluiten richting een portaal.
Algemeen	Whitevision	Voor het scannen en herkennen van documenten wordt de software van Whitevision gebruikt. Specifieke gebruikte toepassingen zijn het verwerken van facturen en het scannen van documenten met als bestemming personeelsdossiers. De aangeboden Integrale Bedrijfsvoeringsoplossing faciliteert de benodigde koppelingen om de voor dit proces benodigde basisgegevens uit te wisselen met Whitevision en de boekingen vast te leggen in de Integrale Bedrijfsvoeringsoplossing.
Financieel	Begroting- en rapportagetool (nu: Capisci)	De applicatie Capisci wordt gebruikt ter ondersteuning van de financiële planning & control cyclus. De koppeling omvat het uitwisselen van gegevens m.b.t. budgetten en het ophalen van de formatiebezetting en financiële informatie en brondocumenten. De koppeling maakt het mogelijk om de in de tool vastgestelde budgetten terug te brengen in het de Integrale Bedrijfsvoeringsoplossing.
Financieel	Foleta Fusyon	De applicatie Foleta Fusyon wordt gebruikt voor het opstellen van de formatieplanning door alle scholen van opdrachtgever. De koppeling maakt het mogelijk om de huidige personeels-, aanstellings- en formatiegegevens (incl. kostenplaats en kostendrager) op te halen uit de salarisadministratie als basis voor dit proces. De Integrale Bedrijfsvoeringsoplossing moet de mogelijkheid bieden om te koppelen met twee gescheiden instances van deze applicatie (PO+VO)
Financieel	WIS Collect	Voor het innen van o.a. ouderbijdragen wordt gebruik gemaakt van de applicatie WIS Collect. De Integrale Bedrijfsvoeringsoplossing biedt de interface voor de WIS Collect applicatie om de benodigde informatie automatisch te verwerken in de financiële administratie. In de huidige situatie

		is dit alleen gekoppeld voor de VO scholen, in de toekomstige situatie is een koppeling voor alle scholen vereist. WIS Collect is per school ingericht omdat de administratieve afhandeling van de ouderbijdragen ook vanuit de scholen plaatsvindt.
Financieel	Mollie	De payment provider Mollie wordt gebruikt voor het afhandelen van online betalingen. De financiële module van de Integrale Bedrijfsvoeringsoplossing ondersteunt het automatisch inlezen van de specificatie van de uitbetalingen om de openstaande posten af te letteren.
Financieel	Visma Spend Cloud Kas en Pas	De applicatie Visma Spend Cloud, module Kas en Pas wordt gebruikt voor het uitgeven en beheren van betaalpassen voor de scholen. De Integrale Bedrijfsvoeringsoplossing faciliteert een koppeling naar deze applicatie voor het uitwisselen van de benodigde stamgegevens. Ook wordt een connector ondersteund voor het verwerken van de gegevens uit SpendCloud naar de grootboekadministratie.
HRM	DUO	De Integrale Bedrijfsvoeringsoplossing ondersteunt de verplichte elektronische gegevensuitwisseling tussen SARO en DUO t.b.v. het maandelijks aanleveren van personeelsgegevens.
HRM	UBL Facturen	De Integrale Bedrijfsvoeringsoplossing moet de functionaliteit bieden om e-Facturen in het UBL formaat in te kunnen lezen.
HRM	eLoo BOOT en DOT	Koppeling voor het ophalen van de personeelsgegevens en het bekwaamheidsdossier in het personeelsdossier aan te vullen met bestanden uit de Ontwikkelmodule (BOOT) en Observatiemodule (DOT)
HRM	UWV Digipoort	De Integrale Bedrijfsvoeringsoplossing ondersteunt de door UWV Digipoort aangeboden koppelingen voor digitale gegevensuitwisseling met UWV.
HRM	Arbodienst	De Integrale Bedrijfsvoeringsoplossing ondersteunt de koppeling voor verzuimmeldingen door te sturen naar de ARBO dienstverlener. Ook biedt de applicatie de interface om vanuit de eigen applicatie van de ARBO dienstverlener de terugkoppeling in het dossier te plaatsen.
HRM Financieel	BI Omgeving (nu: MMP en Power BI)	Alle data opgeslagen in de Integrale Bedrijfsvoeringsoplossing moet door middel van een API component ontsloten kunnen worden naar externe BI oplossingen. De BI oplossing die momenteel gebruikt worden zijn MMP van TIG en Power BI van Microsoft.
PSA	VfPf	De Integrale Bedrijfsvoeringsoplossing voorziet in een koppeling t.b.v. loonaangifte bij het Participatiefonds. Deze koppeling moet zo ingericht zijn dat alleen de medewerkers van het PO domein in de aangifte opgenomen worden.
PSA	ABP	De Integrale Bedrijfsvoeringsoplossing voorziet in een koppeling t.b.v. loonaangifte bij het t.b.v. Pensioenfonds
PSA Financieel	Belastingdienst	De Integrale Bedrijfsvoeringsoplossing voorziet in een koppeling met de Belastingdienst Digipoort t.b.v: - PSA: Loonaangifte - Financieel: btw-aangifte.