

Vraagnr.	Vraag	Antwoord
1.	Hoe ziet Veiligheidsregio de scope voor zich? Wordt er alleen gekeken naar de 650 medewerkers + 200 piketmedewerkers? Of moeten alle 2300 mensen toegang krijgen via het IAM-systeem?	Het gaat hier om alle 2300 medewerkers + ongeveer 200 piketmedewerkers van buiten onze organisatie.
2.	Wie zijn jullie partners en moeten zij ook toegang krijgen tot jullie systemen? Zo ja, welke systemen?	Belangrijkste partners zijn gemeenten, provincies, politie en ambulancediensten. Als onderdeel van onze piket organisatie zijn er medewerkers die toegang moeten hebben tot één of meerdere systemen uit de crisisbeheersing. Een voorbeeld hiervan is de toegang tot onze Crisisutrecht website.
3.	Graag ontvangen wij de lijst van de in gebruik zijnde applicatie om een goede fit te maken met onze standaard integraties	Ja dit is mogelijk. Via de berichten modules van Teneder kan dit document opgevraagd worden.
4.	Zal authenticatie zoals SSO of MFA ook onderdeel zijn van de beoogde scope? Of gaat het alleen om provisioning?	Het gaat alleen om provisioning – SSO en MFA lopen via de bestaande systemen. Wel dient het mogelijk te zijn om SSO en MFA per id geautomatiseerd aan- en uit te zetten.
5.	Wat is jullie huidige HRM-oplossing als bronsysteem? Zijn er nog andere bronsystemen waar we rekening mee moeten houden, zoals bijvoorbeeld een CRM-systeem?	AFAS wordt momenteel voor zowel HRM als CRM gebruikt. (zie meegestuurde lijst applicaties)
6.	Gebruiken jullie momenteel een IT-service tool zoals TOPdesk of ServiceNow?	Wij gebruiken hiervoor Axserion. Deze ondersteunt zowel de IT als de facilitaire en de logistieke processen.
7.	Er wordt aangegeven dat er een lijst van doelapplicaties aangeleverd kan worden. Naast deze lijst willen wij ook graag weten welke Identity Provider momenteel wordt gebruikt, bijvoorbeeld Microsoft Active Directory, Microsoft Entra ID (voorheen Azure AD) of Google ID voor Google Workspace (voorheen G-Suite). Daarnaast, welke productiviteitssoftware wordt gebruikt, bijvoorbeeld Microsoft 365, en moet daar een koppeling voor licentietoewijzing gemaakt worden?	Voor de lijst met doelapplicaties zie vraag 3. De gebruikte identity provider waar op aangesloten moet worden is Entra ID. Voor productiviteit wordt Microsoft 365 gebruikt. Ook hiervoor zoeken we een oplossing om licenties toe te kennen obv kenmerken uit de bronsystemen.
8.	Staat u open dat service providers eveneens antwoorden op deze marktconsultatie? Met name dat we dit vanuit een onafhankelijke tooling /adviserende positie beantwoorden ipv gericht te kiezen voor een tool.	Ja, ook service-providers mogen antwoorden op deze marktconsultatie
9.	Is er technisch onderscheid gemaakt tussen de 2300 medewerkers of wordt er geen technisch onderscheid gemaakt en zijn deze allen lid van dezelfde tenant?	Er is geen onderscheid tussen medewerkers. Alle VRU gebruikers en ook vrijwilligers staan in dezelfde tenant. (Piket)medewerkers moet ook toegang verleend kunnen worden obv hun "originele" tenant.
10.	In welke mate is het voor VRU van belang dat de oplossing breder inzetbaar is dan alleen het toekennen van rechten aan individuen?	Dit is van belang om te bepalen of er voor het vervangen van andere functies aparte trajecten moeten worden gestart.

Vraagnr.	Vraag	Antwoord
11.	Zijn er vanuit VRU standaarden waaraan de beveiliging van de oplossing moet voldoen (bijvoorbeeld ISO standaarden etcetera)?	ISO 27001 en indien van toepassing open standaarden op de lijst van het Forum Standaardisatie. (https://www.forumstandaardisatie.nl/open-standaarden)
12.	Mogen wij een lijst ontvangen met in gebruik zijnde applicaties/doelsystemen die gekoppeld dienen te worden aan de nieuwe oplossing?	Zie vraag 3
13.	Wat betreft het kennisniveau dat nodig is voor de oplossing, bestaan de partijen die na implementatie van kennis voorzien dienn te worden, uit interne personen, externe personen of een combinatie van interne/externe personen?	Dit gaat om interne personen (tenzij op moment van implementatie een vacature tijdelijk wordt opgevuld door een externe)
14.	Kan er een informatie worden verschaft over de opzet van het huidige licentiemodel en capabilities die onderdeel uitmaken van de huidige oplossing?	Nee, we denken dat deze informatie in dit stadium niet relevant is.
15.	Binnen de VRU wordt momenteel gewerkt met UMRA van Tools4Ever. Omdat UMRA binnenkort niet meer ondersteund wordt, is de VRU op zoek naar een tool met dezelfde, of liever uitgebreidere functionaliteit. Kunt u aangeven welke functionaliteiten u nu mist in de huidige oplossing?	Uitgebreidere functionaliteit is mogelijk niet de juiste beschrijving. We zijn vooral op zoek naar een tool waar gebruiksvriendelijk en overzichtelijk IAM kan worden toegepast. Binnen UMRA maken we daarnaast gebruik van mogelijkheden als koppelvlak tussen applicaties om zo informatie uit bronsystemen te verzamelen en geschikt te maken voor doelsystemen.
16.	Heeft de VRU een voorkeur voor een on-premises of SaaS oplossing?	De VRU heeft een voorkeur voor een SaaS oplossing.
17.	Kunt u toelichten hoe de huidige oplossing momenteel is ingezet? Bijv. hoeveel applicaties zijn gekoppeld (en op welke manier), welke processen worden ondersteund en wordt er gebruikgemaakt van een rollenmodel?	Zie vraag 3 + vraag 15. Binnen de bronsystemen (m.n. AFAS) zijn reeds rollen gedefinieerd. Deze kunnen gebruikt worden voor toegangsmodellen. Niet alle rollen zijn reeds gedefinieerd. Sommigen zullen dus tijdens de implementatie nog gemaakt moeten worden
18.	Kunt u aangeven uit hoeveel personen het beheerteam IAM bestaat? Is het de doelstelling om de nieuwe tool uiteindelijk zelf te beheren of dit uit te besteden aan de te selecteren leverancier?	Op het moment is er geen apart beheerteam IAM. Beheer wordt gedaan door een functioneel beheerder met ondersteuning van de interne technisch beheerders en van de leverancier. Wij willen bij onze uitvraag onderzoeken welk beheer voor een nieuwe oplossing benodigd is en welke mogelijkheden hiervoor zijn. In de basis is dit dus nog beiden mogelijk.
19.	Wordt UMRA door de VRU zelf beheerd of door de leverancier (Tools4Ever)?	Zie antwoord op vraag 18, 1e en 2e lijns door de VRU, 3e lijns door de leverancier.

Vraagnr.	Vraag	Antwoord
20.	Heeft de VRU naast IAM nog aangrenzende wensen voor de aankomende jaren? Denk hierbij: aan implementatie van PAM, Access Management, secrets management, etc.	Wij hebben de ambitie op het gebied van PIM, PAM, FIM, maar zijn nog niet concreet gepland.
21.	De VRU wil deze marktverkenning gebruiken om inzicht te verkrijgen in het benodigde budget. Inschrijver implementeert verschillende technologieën met verschillende bijbehorende kosten. Heeft de VRU reeds een budget in gedachten en is zij voornemens dit te delen?	Wij zijn niet voornemens dit in deze fase te delen.
22.	De functionaliteiten van UMRA worden binnenkort niet meer ondersteund. Kan de VRU meer inzicht geven in de tijdslijnen wanneer de implementatie van de IAM-tool moet starten en wanneer deze live moet gaan?	De intentie is begin Q4 2025 de implementatie te hebben afgerond voor de functionaliteiten die nu gebruik maken van UMRA.
23.	Hoe schat VRU de volwassenheid van haar eigen organisatie in?	Onze teams functioneel en technisch beheer hebben voldoende inhoudelijke en proceskennis in huis om dit project te ondersteunen om dit te implementeren.
24.	De gedeelde vragenlijst gaat erg in op de technische kant van een implementatie en minder op de organisatorische/ procesmatige kant. Inschrijver is een implementatiepartner die oplossingen van meerdere technologieleveranciers implementeert. Welke technologie uiteindelijk het best past hangt van verschillende factoren af, denk hierbij aan: budget, te ondersteunen use cases, beheerlast, etc. In deze fase hebben wij nog onvoldoende informatie om een beslissing te maken welke technologie het beste bij de VRU past. Is het daarom toegestaan om de vragenlijst te beantwoorden met meerdere technologieën in onze gedachten?	Ja dit is toegestaan.
25.	heeft u voorbeelden van beperken in uw huidige oplossing?	Zie vraag 15
26.	In de marktverkenning wordt gesproken over "Identity and Access Management" (IAM). Tegenwoordig wordt IAM gezien als een paraplu begrip voor onder andere "Identity Governance and administration" (IGA), "Privileged Access Management" (PAM) en "Access Management" (AM). Bedoelt u met IAM in deze context alleen IGA of ook PAM en AM?	De VRU is geïnteresseerd in al deze mogelijkheden op elk van deze gebieden. Zodat we voor de aanbesteding hierin een weloverwogen keuze in kunnen maken.
27.	Bedoelt u met vraag 7a, de duur van de initiële installatie (met de out-of-the-box)?	Ja. De eerste uitrol van de applicatie zelf.
28.	Kunt u vraag 7c nader toelichten. Bedoelt u hier bijvoorbeeld mee het inrichten van de In-, Door en Uitstroom processen en het Rollenmodel (RBAC)?	Ja, wij bedoelen inderdaad het inrichten van de In-, Door en Uitstroom processen en het Rollenmodel (RBAC).

Vraagnr.	Vraag	Antwoord
29.	Heeft u niet nog andere wensen zoals aanvraag processen (incl. goedkeuringswerkstromen), attestatie processen (Access review), controle processen (o.a. soll-ist) , rapportages, delegatie, logging, audit trail, SOD, Opvoeren externe medewerkers etc.	Graag willen we weten welke mogelijkheden de oplossing standaard bevat.
30.	Is het mogelijk om de lijst met in gebruik zijnde applicaties bij VRU de delen met de inschrijvers?	Zie vraag 3
31.	kunt vraag 12a toelichten?	Als u van mening bent dat de oplossing verbeterd kan worden met de toevoeging van extra oplossingen willen we die graag in beeld krijgen.
32.	Hoeveel gebruikers heeft VRU momenteel in de organisatie? Hoeveel hiervan zijn interne medewerkers, vrijwilligers, tijdelijke medewerkers, en externe partijen?	2300 mensen, inclusief 1.650 vrijwilligers. Daarnaast zijn er ongeveer 200 piketmedewerkers vanuit andere organisaties met (beperkte) toegang tot onze omgeving. Op het (hoofd)kantoor en de meldkamer werken ca. 650 medewerkers. (zie ook uitvraag marktverkenning 1.1)
33.	Welke specifieke groepen gebruikers (bijv. operationele teams, kantoorpersoneel, externen) hebben unieke toegangseisen?	Het zal nodig zijn een veelvoud aan profielen te maken op basis van o.a. afdeling, functie en/of rol. Daarnaast moeten deze ook gestapeld kunnen worden.
34.	Hoeveel applicaties maakt VRU momenteel gebruik van, en welke daarvan moeten direct geïntegreerd worden in de IAM-oplossing? Kunnen we een prioriteitenlijst ontvangen?	Zie vraag 3 De prioriteitenlijst bespreken we in een latere fase.
35.	Hoe beheert VRU momenteel de toegang voor externe partijen, zoals leveranciers, consultants en vrijwilligers? Zijn er specifieke uitdagingen bij het beheren van deze toegangen?	Externe partijen krijgen toegang op basis van de mogelijkheden van een specifieke applicatie
36.	Welke samenwerkingsplatformen (bijv. Microsoft Teams, SharePoint) worden gebruikt en hebben deze specifieke IAM-behoefte?	Zie vraag 3. Voor wat betreft specifieke behoeften zal er een combinatie van centrale en lokale toekenning van rechten zijn.
37.	Zijn er specifieke eisen voor het tijdelijk of dynamisch beheren van toegang voor externen? Bijv. tijdsgebonden toegang of toegang gebaseerd op specifieke projecten.	Ja, aan externen moeten meerdere profielen gekoppeld kunnen worden. De profielen bepalen de rechten. Ook is het wenselijk dat zowel in een profiel alsook bij een individu tijdsgebonden toegang ingesteld kan worden.
38.	Hoe belangrijk is het voor VRU dat externe gebruikers toegang kunnen aanvragen en beheren via self-service functies?	Dit is niet belangrijk, toegang loopt via kenmerken uit de verschillende bronsystemen die bepalen of aan een externe een specifiek profiel wordt toegekend. Externen hoeven dus niet zelf toegang te vragen via self-service functies.
39.	Verwacht VRU een toename in het aantal gebruikers of applicaties in de komende jaren? Zijn er plannen voor nieuwe samenwerkingen met externe partijen?	Nog niet bekend.

Vraagnr.	Vraag	Antwoord
40.	Heeft VRU specifieke eisen aan de beveiliging van accounts en toegangen voor externe partijen? Bijv. verplichte MFA of periodieke hercertificering?	We vragen externe partijen ISO 27001 gecertificeerd te zijn. Naast de maatregelen in de ISO27001 dient er voor toegang tot VRU systemen altijd gebruik gemaakt te worden van MFA en indien nodig aangevuld met conditionele toegang. Voor toegang tot applicaties wordt daarnaast in de regel ook SSO toegepast (bij Cloud apps altijd). De VRU is in controle over de koppeling tussen de VRU en leverancier (denk bijv. aan just-in-time principe). Naast MFA dienen de verbindingen ook versleuteld te zijn volgens laatste beveiligingsstandaarden. Voor een gebruiker die toegang heeft tot VRU bedrijfsmiddelen en systemen zijn de minimale wachtwoordvereiste als volgt: • Minimaal 12 vrij te kiezen karakters. • Niet eerder gebruikt. • Niet in gebruik op andere systemen of omgevingen. • Niet makkelijk te raden door gebruik van bijvoorbeeld namen, telefoonnummers, geboortedatum etc. • Vrij van opeenvolgende of identieke, alfabetische of numerieke karakters. • Elke 365 dagen gewijzigd worden, of bij (vermoeden van) compromittering. MFA verplicht met beperkte uitzonderingen (b.v. testdoeleinden).
41.	Zijn de applicaties die VRU gebruikt voornamelijk on-premise, cloud-gebaseerd of een hybride model? Zijn er plannen om de IT-landschap te moderniseren?	Op dit moment hybride – doelstelling is om richting SaaS-applicaties te gaan.
42.	Zijn er specifieke compliance-eisen waaraan VRU moet voldoen bij het beheer van externen en hun toegangen, zoals ISO 27001 of AVG?	We vragen aan externe partijen om ISO 27001 gecertificeerd te zijn en te voldoen aan de AVG.
43.	Hoe belangrijk is het voor VRU om gedetailleerde auditlogs te hebben voor de toegang en activiteiten van externe gebruikers?	Logging en monitoring dient te worden toegepast, zodat de VRU weet wanneer de leverancier gebruik maakt van externe toegang en de activiteiten die worden uitgevoerd door externe gebruikers.

Vraagnr.	Vraag	Antwoord
44.	Heeft VRU gedefinieerde rollen en toegangsmodellen voor externen, of moeten deze worden opgesteld tijdens de implementatie?	Binnen de bronsystemen (m.n. AFAS) zijn reeds rollen gedefinieerd. Deze kunnen gebruikt worden voor toegangsmodellen. Niet alle rollen zijn reeds gedefinieerd. Sommigen zullen dus tijdens de implementatie nog gemaakt moeten worden.
45.	Hoe belangrijk is het dat incidenten, zoals onrechtmatige toegangspogingen, direct gemonitord worden voor zowel interne als externe gebruikers?	Gewenst, maar geen vereiste, geef aan wat de mogelijkheden zijn van uw applicatie.
46.	Heeft VRU een centraal HR-systeem waarmee automatisch lifecyclebeheer kan worden uitgevoerd, inclusief het onboarden en offboarden van externen?	Ja dit gaat via AFAS

Rectificatie: In de marktconsultatie stond het verkeerde telefoonnummer in van de contactpersoon. Het juiste telefoonnummer is 06-30849374