Ministerie van Justitie en Veiligheid

**Nota van Inlichtingen**

# Marktconsultatie
## DV&O Risicoanalyse systeem
IUC/DJI/IENEA/JvH/2022-4

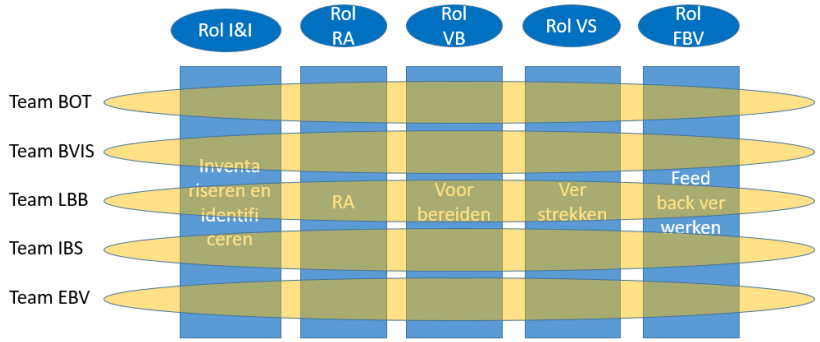
## Nota van Inlichtingen

Het IUC DJI heeft de vragen in het kader van de Nota van Inlichtingen ontvangen.

De inhoud van deze Nota van Inlichtingen maakt deel uit van de marktconsultatie. Deze Nota van Inlichtingen is gepubliceerd op www.tenderned.nl en is daarmee beschikbaar gesteld voor alle belangstellenden van deze marktconsultatie.

## Hoofdstuk 1. Vragen / antwoord

| Nr. | Vragen / antwoord |
|---|---|
| 1. | Vraag:<br>Bij 5.3.2 wordt gesteld "Het kunnen uitvoeren van geautomatiseerde risicoanalyses". Om dit te automatiseren is een overzicht met realistische dreigingen noodzakelijk en om op basis van de inschatting automatisch een beveiligingsadvies te geven is tevens een lijst met mogelijke (standaard) maatregelen nodig.<br>• Zijn de realistische dreigingen ten aanzien van objecten al bepaald?<br>• Is er een standaard programma met maatregelen ten aanzien van objecten vastgesteld?<br>Indien deze niet aanwezig zijn, is het dan de bedoeling dat deze opgesteld worden? |
| | Antwoord:<br>Risico's worden bepaald op basis van risico categorieën. Per dienst zijn de risico categorieën bekend. Elke risicocategorie voor een bepaalde dienst kent een vaste waarde voor de Ernst (per categorie per dienst). Het risico is de combinatie van de Ernst en de Waarschijnlijkheid. De waarschijnlijkheid kan door het systeem bepaald worden op basis van eerdere vergelijkbare analyses voor dezelfde persoon, of mogelijk op basis van een vergelijkbare analyse voor een andere persoon met dezelfde risico categorieën.<br><br>Verder helpt het systeem om bij een risicoanalyse op basis van alle Ernst/Waarschijnlijkheid combinaties, op basis van een matrix, de zwaarstwegende combinatie van Ernst/Waarschijnlijkheid vast te stellen. Deze matrices, die bepalen wat het risico is van een Ernst/waarschijnlijkheid combinatie, bestaan nu in Excel maar worden onderdeel van het gevraagde systeem.<br><br>De beheersmaatregelen die kunnen worden getroffen om een risico te mitigeren liggen vast in een ander systeem, buiten het bereik van deze consultatie. Als u als marktpartij een standaard mogelijkheid heeft voor het ondersteunen van deze maatregelen-matrices, kunt u dat separaat aangeven bij de beantwoording van de vragen. |
| 2. | Vraag:<br>Bij 5.3.3 wordt gesteld "Het kunnen onderhouden van dossiers". Zijn er vaste formats voor dergelijke dossiers en wat voor soort en type informatie kan onderdeel uitmaken van een dergelijk dossier? Is het mogelijk een voorbeeld/fictief dossier op te leveren? |
| | Antwoord:<br>Er is geen vast format. Dossier**s** bevatten documenten (Word, pdf, txt), afbeeldingen en foto's. Mogelijk ook video en audio bestanden**.** Het kunnen metadateren van dossiers en documenten is vereist**.** |
| 3. | Vraag:<br>Bij verschillende punten (o.a. 5.3.3 en 5.3.5) wordt ingegaan op autorisaties, rollen en teams en differentiatie daarin. Duidelijk is dat niet iedereen overal bij moet kunnen. Kan er meer inzicht gegeven worden in welke rollen en differentiaties wenselijk zijn? |
| | Antwoord: |

| Nr. | Vragen / antwoord |
|---|---|
| |  <br>Het systeem kent een aantal niveaus van autorisatie:<br>- Teams, mensen die gezamenlijk aan een product/dienst werken<br>- Rollen, de taken die je binnen het proces mag uitvoeren<br><br>Rollen kunnen direct uitgedeeld worden aan een persoon, bijvoorbeeld:<br>- "Jan is risico-analist (RA). Daarmee is Jan risico-analist voor alle teams.<br>- "Piet is werkvoorbereider (VB) voor team BOT. Daarmee is Piet alleen voorbereider voor team BOT, maar dus niet voor andere teams<br>- Een persoon kan één of meerdere rollen hebben<br>- Een persoon vervult werkzaamheden voor een of meerdere teams<br>- Een persoon kan per team een andere rol hebben<br><br>Daarnaast is er nog een rol "raadpleger". Conform bovenstaande systematiek mag een raadpleger alles inzien, of alleen inzien per team. |
| 4. | Vraag:<br>Bij 5.3.6 wordt gesteld "Het kunnen uitwisselen van risicogegevens (geautomatiseerd)<br>Het systeem moet in staat zijn de in de strafrechtketen afgesproken standaarden met betrekking tot risicogegevens te ondersteunen".<br>Welke standaarden en gedefinieerde structuren zijn van toepassing? |
| | Antwoord:<br>DJI hanteert ebXML volgens de zgn. Jubes standaard (zie JUBES bij Justid).<br>Koppelingen vanuit de applicaties met de federatieve service**s** gebeuren d.m.v. van de protocollen SAML 2.0 en OIDC (OpenIDConnect)<br>Respectievelijk: XML SAML en JSON Web Token (JWT) |

| Nr. | Vragen / antwoord |
|---|---|
| 5. | Vraag:<br>Bij 9. wordt gesteld "Kunt u aangeven welke standaarden op het gebied van informatiebeveiliging u heeft toegepast bij de ontwikkeling van uw oplossing?". Zijn er specifieke voorkeuren, eisen of specifieke maatregelen op het gebied van informatiebeveiliging die wenselijk of vereist zijn? |
| | Antwoord:<br><br>DJI conformeert zich aan de Baseline Informatiebeveiliging Overheid. De minimale eisen van een informatiesysteem m.b.t. beveiliging zijn:<br>1.) Passwordbeveiliging voldoet aantoonbaar aan de security eisen<br>2.) Een entiteit (natuurlijk persoon of systeemfunctie) krijgt slechts eenmalig een uniek user-id toegewezen. Elk user-id is herleidbaar tot slechts één entiteit. Het mag niet voorkomen dat een natuurlijk persoon meer dan één account heeft.<br>3.) De uitvoering van alle authenticatie en autorisatie functies wordt gelogd.<br>4.) Het kopiëren van bestanden van een naar de applicatie (en onderliggende databases) wordt vastgelegd t.b.v. audit.<br>5.) Er is vastgelegd dat voor toegang tot productiegegevens bij verstoringen voorafgaande toestemming door de systeemeigenaar vereist is.<br>6.) Het gebruik van het back-up (en restore) mechanisme wordt t.b.v. auditing gelogd in de log van het ICT infrastructuur component.<br>7.) Elk gegevenstransport met externe partijen wordt gelogd t.b.v. auditing.<br>8.) De applicatie maakt het mogelijk om handelingen in de applicatie te herleiden tot een specifiek gebruiker. |
| 6. | Vraag:<br>Welk systeem gebruikt de DV&O momenteel en wat zijn de tekortkomingen? |
| | Antwoord:<br>DV&O gebruikt het systeem INGRID. Dit betreft een MS Access applicatie. De huidige tekortkomingen zijn o.a.:<br>- Herleidbaarheid van gegevens, situatie van beschikbare gegevens in de tijd (welke risico categorieën waren bekend ten tijde van analyse x)<br>- Opslag van documenten en andere bijlagen<br>- Alleen analyses voor personen mogelijk, niet voor objecten<br>- Geen mogelijkheid om verbanden te registreren tussen analyse<br>- Geen ondersteuning bij het uitvoeren van netwerkanalyses |
| 7. | Vraag:<br>Wordt er een formele methodiek voor risicoanalyse toegepast, zo ja welke? |
| | Antwoord: DV&O hanteert een zelf vormgegeven methodiek voor het classificeren van risico's. De methodiek is geënt op ISO-31000. De methode wordt ondersteund door het gebruik van risico-matrices per product/dienst, zie ook antwoord op vraag 1. |

| Nr. | Vragen / antwoord |
|---|---|
| 8. | Vraag:<br>Worden er ook analyses in teamverband gemaakt? (dus meerdere analisten c.q. stakeholders werken aan dezelfde analyse) |
| | Antwoord:<br>Nee, wel is het zo dat het werk van een analist overgenomen moet kunnen worden door een ander. Bij de meeste analyses zijn ook infodesk medewerkers betrokken voor het aanleveren en complementeren van informatie, dus het aantal mensen dat bijdraagt aan een analyse is altijd wel meer dan één. |
| 9. | Vraag:<br>Is het ook de bedoeling dat analisten vanaf verschillende locaties aan dezelfde analyse werken? |
| | Antwoord: Zie vraag 8, het werk in het systeem zou niet locatie gebonden moeten zijn. DV&O medewerkers werken op circa 18 locaties én vanuit thuis. De medewerkers maken gebruik van de DJI-werkplek. |
| 10. | Vraag:<br>"5.3.3" Dossiers: moet het hier ook mogelijk zijn om data te rubriceren en/of source classification (reliability, accuracy) "5.3.2" spreekt van "volledig geautomatiseerde risicoanalyses", het is niet precies duidelijk wat daarmee bedoelt wordt, kunt een aantal voorbeelden geven? |
| | Antwoord:<br>- Ja, source classification (reliability, accuracy) is gewenst; het is wenselijk de bron van informatie en de waarde hiervan te kunnen vastleggen.<br>- Rubricering is niet direct nodig, indirect is dit geregeld met het autorisatiemechanisme. Termijnen van schonen gaan per dossier (persoon, locatie of vracht) en niet per dossier stuk. |
| 11. | Vraag:<br>"5.3.6" spreekt over "in de strafrechtketen afgesproken standaarden". Welke standaarden zijn dit? |
| | Antwoord:<br>Zie antwoord vraag 4 |
| 12. | Vraag:<br>Kunt u bestaande Use Cases beschrijvingen m.b.t. de risicoanalyses delen? |
| | Antwoord:<br><br>Deze zullen we pas verstrekken of toelichten op het moment van gesprek of demo. Dit gezien de gevoeligheid van de materie. |

*****