



> Retouradres Postbus 20301 2500 EH Den Haag

Ministerie van Justitie en Veiligheid
t.a.v. Minister van Weel
Postbus 20301
2500 EH Den Haag

**Inspectie Justitie en
Veiligheid**
Directie Politie, Security en
Crisisbeheersing
Afd. Crisisbeheersing & Cyber

Hoge Nieuwstraat 8
2514 EL Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

Contactpersoon
contact@inspectie-jenv.nl

Onze referentie

Bijlage(n)
1

Datum 15 augustus 2025
Betreft Verslag toezicht wettelijke hackbevoegdheid politie 2024

Geachte heer Van Weel,

Met deze brief rapporteert de Inspectie van Justitie en Veiligheid (hierna: Inspectie JenV) over haar bevindingen uit het toezicht op de hackbevoegdheid over de periode 2024 en het eerste kwartaal van 2025.

De politie en bijzondere opsporingsdiensten zijn sinds 2019 bevoegd om onder strikte voorwaarden heimelijk en op afstand onderzoek te doen in een geautomatiseerd werk (zoals een laptop of smartphone) dat in gebruik is bij een verdachte. Deze bevoegdheid wordt ook wel de "hackbevoegdheid" genoemd. De uitvoering van de hackbevoegdheid door de politie is centraal belegd bij het Digital Intrusion Team (hierna: DIGIT).

De Inspectie JenV houdt toezicht op de uitvoering van de hackbevoegdheid en doet daarover jaarlijks verslag.¹

1. Inleiding

Sinds de inwerkingtreding van de hackbevoegdheid in 2019 is het toezicht van de Inspectie JenV in ontwikkeling. In lijn met de Wet Computercriminaliteit III (hierna: Wet CCIII) en het beoogde doel van de wetgever vult de Inspectie JenV haar toezicht zoveel mogelijk systeemgericht in. Systeemtoezicht is een vorm van toezicht waarbij de toezichthouder gebruik maakt van het systeem van de onder toezicht staande organisatie, dat gericht is op het realiseren van regelnaleving en het systematisch vergroten van de eigen kwaliteit. Systeem is hierbij een breed begrip. De Inspectie JenV verstaat hieronder in ieder geval beleid, processen, methoden, instructies, ondersteunende systemen en interne controle van de politie die zijn ingericht om de naleving van de regels en de kwaliteit te borgen.

In verband met het ontbreken van een robuust kwaliteitssysteem – een basisvoorwaarde voor effectief systeemtoezicht – heeft de Inspectie JenV de eerste jaren na de inwerkingtreding van de Wet CCIII zich hoofdzakelijk gericht op de directe naleving van de wet en daarmee de inzetten van de hackbevoegdheid. Sinds 2023 is de focus van het toezicht verschoven naar de ontwikkeling en implementatie van een kwaliteitssysteem door DIGIT.² Hierbij kijkt de Inspectie JenV dus naar het

¹ Zie voor de bevindingen en conclusies de vijf eerdere verslagen van het toezicht op de hackbevoegdheid van de Inspectie JenV. Deze rapportages zijn te vinden op www.inspectie-jenv.nl/publicaties.

² Zie hiervoor de eerdere verslagen over de hackbevoegdheid van de Inspectie JenV over 2023 en 2024 op de website www.inspectie-jenv.nl

kwaliteitssysteem die DIGIT op dit moment inricht om de naleving van wet- en regelgeving en kwaliteit te borgen.

Onderzoeksmethode

In periodieke gesprekken bespreken DIGIT, het Openbaar Ministerie (hierna: OM) en de Inspectie JenV het proces en de (te behalen) mijlpalen die DIGIT, bij het inrichten van het kwaliteitssysteem, realiseert.³ Ook bespreken de drie organisaties tussentijdse bevindingen en risico's in dit overleg. Daarnaast is de Inspectie JenV aanwezig geweest bij een aantal teamsessies die door DIGIT werden georganiseerd om bijvoorbeeld de processen en de risico's in kaart te brengen. Als laatste heeft de Inspectie JenV in 2024 een representatief aantal interviews gehouden met meerdere werknemers van alle verschillende onderdelen van DIGIT.⁴ Deze medewerkers zijn werkzaam in de verschillende onderdelen van DIGIT, te weten medewerkers van het inzetteam, coördinatoren, technisch en tactisch specialisten. De Inspectie JenV heeft geen zaken waarin de hackbevoegdheid is ingezet onderzocht.

Leeswijzer

De Inspectie JenV beschrijft in deze rapportage haar bevindingen van het toezicht. Deze rapportage begint met de belangrijkste conclusies. Hierna volgen de bevindingen van het toezicht. Hiervoor hanteert de Inspectie JenV de onderstaande twee onderdelen, te weten:

1. Algemene beeld over de voortgang en realisatie van het kwaliteitssysteem.
2. Bevindingen over specifieke elementen die belangrijk zijn in een kwaliteitssysteem.

Na de bevindingen volgen per onderdeel specifieke elementen, een tussenconclusie en bijbehorende aanbevelingen. Als laatste wordt een overkoepelende conclusie getrokken en de aanbevelingen nog kort samengevat.

2. Belangrijkste conclusies

De Inspectie JenV concludeert dat DIGIT uitvoering geeft aan haar, in 2023 vastgestelde, procesplan om te komen tot een kwaliteitssysteem. In de rapportage van vorig jaar signaleerde de Inspectie JenV het risico dat door onvoldoende capaciteit, het operationele proces (het hacken zelf) voorrang zou krijgen op het realiseren van het kwaliteitssysteem. Door het aannemen van twee kwaliteitsmedewerkers in 2024 is dit risico door DIGIT gemitigeerd. De Inspectie JenV ziet dat DIGIT met voldoende aandacht, tijd en prioriteit de stappen van het plan uitvoert. Ondanks de opgelopen vertraging gaat de Inspectie JenV ervan uit dat eind 2025 een eerste versie van een werkend kwaliteitssysteem staat. Daarnaast concludeert de Inspectie JenV dat voor een aantal belangrijke onderdelen extra aandacht moet komen om tot een goed functionerend kwaliteitssysteem te komen. Zo is het noodzakelijk om de juridische kennis van (de voornamelijk technische) medewerkers over de regels van de hackbevoegdheid te verhogen en de juridische regels voor deze medewerkers toegankelijker te maken. Dit in het kader van de eerste lijncontrole. Ook het borgen en melden van zelf gesignaleerde

³ Ondanks dat de Inspectie JenV geen toezicht houdt op het OM, is het OM voor dit toezicht wel een belangrijke stakeholder vanwege haar gezagsrol. DIGIT voert haar onderzoekshandelingen uit op bevel van het OM. Ook heeft het OM een controlerende taak op DIGIT. Om te komen tot een effectief kwaliteitssysteem is de bijdrage en de rol van het OM een belangrijk aspect van het proces naar een werkend kwaliteitssysteem.

⁴ Vanwege het vertrouwelijke karakter kan de Inspectie JenV geen uitspraken doen over de grootte van DIGIT.

incidenten en bijna-incidenten is een onderdeel waar de Inspectie JenV nog verbetering wenselijk vindt.

Datum
15 augustus 2025

Onze referentie

3. Voortgang realisatie kwaliteitssysteem

In dit eerste onderdeel van de bevindingen gaat de Inspectie JenV in op de voortgang van het realiseren van het kwaliteitssysteem door DIGIT. In de vorige rapportage stelde de Inspectie JenV vast dat DIGIT was gestart met het opstellen van een procesplan voor het realiseren van het kwaliteitssysteem.⁵ Dit procesplan beschrijft zeven fasen die DIGIT doorloopt voor het realiseren van het kwaliteitssysteem;

- 1) Het in kaart brengen van bedrijfsprocessen en technische omgevingen;
- 2) Het in kaart brengen van het wettelijk kader en bijbehorende normen (de wettelijke regels die van toepassing zijn voor het uitvoeren van de hackbevoegdheid, maar ook bijvoorbeeld normen vanuit de informatiebeveiliging);
- 3) Het operationaliseren van het normenkader;
- 4) Het uitvoeren van een risicoanalyse;
- 5) Het ontwerpen van kwaliteitsnormen, maatregelen en controles;
- 6) Het identificeren van bestaande kwaliteitsnormen maatregelen en controles;
- 7) Het opstellen van doelstellingen, taken en activiteiten.

Het eerder vastgestelde procesplan wordt gevolgd en in de praktijk uitgevoerd. In 2024 heeft DIGIT twee fulltime medewerkers aangenomen voor het realiseren van het kwaliteitssysteem. Hierdoor wordt het kwaliteitssysteem uitgewerkt naast de operationele werkzaamheden van DIGIT en is het kwaliteitssysteem niet ondergeschikt geraakt aan het uitvoeren van de hackbevoegdheid. De betreffende medewerkers werken met toewijding en motivatie aan het opzetten van het kwaliteitssysteem. Zij worden hierin ondersteund door het management van DIGIT. In de periode maart 2024 tot februari 2025 heeft DIGIT fase één tot en met drie voor de realisatie van het kwaliteitssysteem doorlopen. Volgens de planning zouden deze stappen in oktober 2024 zijn afgerond.

Beschrijving activiteiten fase 1 tot en met 3

Voor het opstellen van de procesbeschrijvingen (fase 1) heeft DIGIT sessies georganiseerd met medewerkers van de verschillende onderdelen van DIGIT. Daarnaast zijn de (wettelijke) normen in kaart gebracht (fase 2 en fase 3) en is gestart met de risicoanalyse (fase 4). Door middel van een aantal sessies met het team en door de kwaliteitsmedewerkers zijn, op basis van de procesbeschrijvingen, mogelijke risico's geïnventariseerd. Hierbij is door DIGIT breed gekeken naar waar in de processen, welke mogelijke risico's aanwezig zijn op niet-naleving van de normen uit het normenkader.

Door de grote hoeveelheid aan geïnventariseerde mogelijke risico's en nieuwe opgedane kennis over risicomanagement is door DIGIT onlangs besloten om de omslag te maken van het beschrijven van alle mogelijke risico's naar het eerst beschrijven en bepalen van de strategische risico's.

⁵ Rapportage Hackbevoegdheid 2023. In deze rapportage concludeerde de Inspectie JenV dat dit procesplan een goede basis biedt voor het realiseren en implementeren van het kwaliteitssysteem.

Datum
15 augustus 2025

Onze referentie

Informatiebeveiliging

In het procesplan van DIGIT is beschreven dat naast de regels die toezien op de uitvoering van de hackbevoegdheid, ook de regels met betrekking tot informatiebeveiliging van belang zijn voor het kwaliteitssysteem. Het uitvoeren van de processtappen voor dit onderwerp, is in 2024 achtergebleven en heeft nog beperkt uitwerking gekregen.

Bewaren gegevens

In 2024 heeft DIGIT ook het proces in gang gezet om bepaalde werkprocessen die raken aan de naleving van de Wet Politiegegevens (hierna: WPG) aan te passen. DIGIT bewaart alle verzamelde gegevens (het bewijs) nadat deze zijn overgedragen aan het team dat het politieonderzoek uitvoert (het tactisch team). Het bewaren van deze gegevens brengt risico's met zich mee met betrekking tot het naleven van verschillende wet- en regelgeving. De Inspectie JenV heeft in eerdere rapportages geconstateerd dat bij het opslaan en het bewaren van de gegevens niet alle regels worden nageleefd.⁶ DIGIT is in 2024 gestart met het onderzoeken of de gegevens bij DIGIT wettelijk gezien mogen worden verwijderd na de overdracht. De gegevens zouden dan alleen nog exclusief worden bewaard door de betrokken tactische teams. Een dergelijke werkwijze zou risico's ten aanzien van het bewaren en vernietigen kunnen mitigeren.

Tussenconclusie

De Inspectie JenV concludeert dat het uitwerken van de kwaliteitssysteem voldoende tijd en prioriteit krijgt. De stappen worden met voldoende aandacht en inzet doorlopen. Kijkend naar de planning uit het procesplan concludeert de Inspectie JenV dat de planning met betrekking tot de implementatie van het kwaliteitssysteem een vertraging van ongeveer vier maanden heeft opgelopen. De Inspectie JenV hecht veel waarde aan een solide basis en opzet. De vertraging die is ontstaan acht zij begrijpelijk gelet op de hoeveelheid werk dat moet worden verzet. De eerste planning was, achteraf gezien, te ambitieus.

Aanbeveling voortgang realisatie kwaliteitssysteem

De Inspectie JenV adviseert DIGIT en de eindverantwoordelijke voor het kwaliteitssysteem dan ook om een aanpassing te maken op de eerder opgestelde planning. Daarbij dient de politie ook oog te hebben voor de situatie dat hierdoor mogelijk een langere periode beperkte (interne) controle plaatsvindt en geen extern toezicht op zaakniveau en de informatiebeveiliging. Door de eindverantwoordelijke dient een keuze te worden gemaakt of tussentijdse maatregelen noodzakelijk zijn.

4. Specifieke elementen van het kwaliteitssysteem

In dit tweede onderdeel van de bevindingen staat de Inspectie JenV stil bij een aantal specifieke elementen van het kwaliteitssysteem en systeemtoezicht. Dit zijn tevens de onderwerpen waarover medewerkers van DIGIT door de Inspectie JenV zijn geïnterviewd. De rode draad hierin is het zogenoemde *Three lines of Defense model*.⁷ Dit model verdeelt de verantwoordelijkheden voor het beheren van risico's, regelgeving en interne controle over drie niveaus. Het *Three lines of Defense model* gaat uit van lijnverantwoordelijkheid verdeeld in drie lijnen van controles. De

⁶ Hierbij doelt de Inspectie JenV op de eerdere bevindingen ten aanzien van het vernietigen van informatie van verschoningsgerechtigden. Zie het verslag toezicht wettelijke hackbevoegdheid politie 2022, pagina 18 en 52.

⁷ The Institute of Internal Auditors - Het Three Lines Model van het IIA, zie www.iaa.nl.

eerstelijnscontrole komt vanuit de werkvloer, waarbinnen verantwoordelijkheid wordt gedragen voor het beheer van de processen en operaties. De tweedelijnscontrole beschrijft een lijn die in vormen van risicomanagement regelgeving en kwaliteitssystemen ondersteuning biedt aan de eerstelijnscontrole. Ten slotte biedt de derde lijn uit het model een controle bestaande uit onafhankelijke controlerende organisatieonderdelen die toezien op het functioneren van zowel de eerste als tweede lijn, zoals een interne auditafdeling of een compliance afdeling. Daarnaast zijn onderdelen als een open cultuur, de lerende organisaties en transparantie naar de toezichthouder het fundament van een kwaliteitssysteem en systeemtoezicht. Ook naar deze onderdelen heeft de Inspectie JenV in 2024 gekeken.

4.1. Open cultuur

Een open cultuur is belangrijk voor de eerstelijnscontrole. Door een open cultuur, waarin het mogelijk is om kritisch te zijn op het eigen proces, kunnen fouten worden voorkomen en tijdig wordenesignaleerd. De houding en het gedrag van de leidinggevende en (specifiek voor DIGIT) het OM zijn richtinggevend voor welke cultuur er heerst binnen DIGIT. Uit de interviews is door medewerkers aangegeven dat zij een open en informele organisatie ervaren. Op de werkvloer wordt nauw samengewerkt. Er wordt weinig afstand tot de eigen leidinggevende en het OM ervaren door het team. Medewerkers geven aan geen drempels te voelen als het gaat om het benoemen en bespreken van fouten en andere incidenten. Ook wordt volgens de medewerkers door zowel de leidinggevende en het OM benadrukt dat als fouten worden gemaakt, transparantie hierover belangrijk is.

Tussenconclusie

De Inspectie JenV concludeert dat de huidige cultuur voldoende basis biedt om het kwaliteitssysteem straks te laten werken. Met de wijzigingen in de organisatie van één landelijke eenheid naar twee eenheden en eventuele wijzigingen in het team (denk hierbij aan mogelijke uitbreiding of wisseling van medewerkers) is het van belang (en tevens de uitdaging voor DIGIT) om deze cultuur te behouden.

Aanbevelingen

Borg de huidige cultuur en draag zorg dat deze wordt behouden indien wijzigingen in het team plaatsvinden en het team wordt overgeplaatst naar de nieuwe eenheid.

4.2. Kennis regels hackbevoegdheid

Medewerkers van DIGIT zijn gemotiveerde professionals die over veel (technische) kennis en kunde binnen hun vakgebied beschikken. Voor een goed functionerende eerstelijnscontrole is het cruciaal dat medewerkers weten wat de kaders zijn waarbinnen zij werken. In de kwalificaties van opsporingsambtenaren staat vermeld dat leden van het technisch team dienen deel te nemen aan de cursus Bijzondere Opsporingsbevoegdheden en CCIII van de Politieacademie of van een vergelijkbare aanbieder.⁸ Dit om te borgen dat medewerkers beschikken over de juridische kennis die noodzakelijk is voor het uitvoeren van hun werkzaamheden.

DIGIT heeft in samenspraak met het OM enige jaren geleden de werkwijze gehanteerd dat het OM juridische sessies over CCIII bij DIGIT organiseert voor

⁸ Regeling van de Minister van Justitie en Veiligheid van 15 februari 2019, kenmerk 2429311.

medewerkers. Deze sessies worden gegeven wanneer een nieuwe lichter medewerkers start, en kunnen ook worden bijgewoond door medewerkers die al langer bij DIGIT werkzaam zijn. Uit de interviews die zijn gevoerd en op basis van het bijwonen van verschillende sessies is op te maken dat medewerkers de juridische kaders nog niet volledig beheersen. Dit komt mogelijk omdat niet elke medewerker bij DIGIT de cursus over CCIII van het OM heeft gevolgd. Ook ontbreken handvatten als bijvoorbeeld een handboek waarin de regels begrijpelijk worden uitgelegd. Wel weten medewerkers dat zij bij het OM of coördinatoren terecht kunnen voor vragen over het juridisch kader. De Inspectie JenV begrijpt dat de politie bezig is met een wijziging ten aanzien van de opleiding van medewerkers. De opleidingen en examinering voor DIGIT, waaronder de opleiding CCIII, worden ondergebracht bij de Politieacademie.

Tussenconclusie

De Inspectie JenV concludeert dat de juridische kennis van de medewerkers nu nog onvoldoende is om straks de eerstelijnscontrole goed uit te kunnen voeren. De Inspectie JenV vraagt zich af of alleen het volgen van deze éénmalige sessies voldoende is ook gelet op het feit dat handvatten als een handboek ontbreken. De medewerkers van DIGIT zijn immers veelal technische professionals, hierdoor zit hun expertise voornamelijk op technisch vlak en minder op het juridische vlak.

Aanbevelingen

De Inspectie JenV beveelt aan om in de nog uit te werken maatregelen (fase 5 van het procesplan) aandacht te hebben voor (aanvullende) maatregelen ter verbetering van de kennis en het verbeteren van de borging van de kennis. De Inspectie JenV dringt aan om na te denken over handvatten voor (de veelal technische) medewerkers om de juridische teksten toegankelijker te maken.

4.3. Kennis kwaliteitssysteem

De medewerkers van DIGIT zijn in teamoverleggen geïnformeerd over het kwaliteitssysteem en de voortgang. Medewerkers die de hackbevoegdheid uitvoeren worden betrokken bij de realisatie van het kwaliteitssysteem, maar het ontbreekt bij de meeste medewerkers aan overzicht over het gehele traject en het einddoel. De kennis van medewerkers over het kwaliteitssysteem reikt tot waar in het proces DIGIT op dat moment staat.

Tussenconclusie

De Inspectie JenV constateert dat de noodzaak en het doel van het kwaliteitssysteem vooral duidelijk is bij een kleine groep binnen DIGIT, waaronder de kwaliteitsmedewerkers. De kennis over het kwaliteitssysteem onder medewerkers is nog onvoldoende om het kwaliteitssysteem straks goed te laten functioneren. Het ontbreken van voldoende kennis over de regels (zie hierboven) maakt het ook lastig voor medewerkers om de input te leveren die noodzakelijk is voor het ontwerpen van het kwaliteitssysteem.

Aanbevelingen

De Inspectie JenV beveelt dan ook aan om de kennis van medewerkers over het doel en opzet van het kwaliteitssysteem op korte termijn te verbeteren. Ook hier geldt dat voor fase 5 van het procesplan aandacht besteed dient te worden aan het

borgen van deze kennis en het zodanig te vertalen dat dit toepasbaar wordt voor alle medewerkers. Het kwaliteitssysteem is immers een continu proces en dynamisch geheel waar alle medewerkers een rol hebben en waarbij het van belang is dat medewerkers weten wat van hen wordt verwacht.

4.4. Lerende organisatie

DIGIT opereert in een complexe en technische omgeving. Incidenten zijn dan ook niet uit te sluiten. Het is belangrijk dat een organisatie incidenten tijdig kan herkennen. Ook is van belang hoe een organisatie omgaat met deze incidenten en of, en zo ja, wat er van deze incidenten wordt geleerd.

Momenteel signaleert DIGIT incidenten voornamelijk door de oplettendheid van de medewerkers. In de eerdere rapporten van de Inspectie JenV is beschreven dat DIGIT minimaal gebruik heeft gemaakt van logging om incidenten op te sporen.⁹ Het kwaliteitssysteem moet gaan zorgen voor het beter signaleren en vastleggen van incidenten. Zoals eerder in deze brief beschreven is de cultuur binnen DIGIT wel zodanig dat medewerkers geen drempels ervaren om incidenten te melden bij de teamleider en/of het OM. Voor de registratie van incidenten is echter geen centrale plek ingericht. Incidenten worden op verschillende plaatsen binnen de organisatie vastgelegd en dit wordt gedaan voor de betreffende zaak. Dit maakt het lastig om te reflecteren, van incidenten te leren en om de geleerde kennis door te geven aan nieuwe medewerkers zodat dezelfde incidenten kunnen worden voorkomen.

Een belangrijk element van systeemtoezicht is dat incidenten worden gemeld bij de toezichthouder of periodiek inzichtelijk worden gemaakt. Ook bijna-incidenten zijn van belang om te melden bij de toezichthouder. Het direct melden van incidenten aan de toezichthouder geeft vertrouwen en biedt transparantie. Op basis hiervan kan de dialoog worden gevoerd over wat de oorzaak is geweest van het incident, wat hiervan is geleerd en of en zo ja, hoe het proces is verbeterd. Deze stappen worden gezet door DIGIT. Zo is in 2024 door DIGIT tijdig aan de Inspectie JenV gemeld dat zij zijn binnengedrongen op een ander geautomatiseerd werk dan waarvoor het bevel was afgegeven. Door de wijze van voorbereiding van de inzet heeft DIGIT de fout snel kunnen ontdekken, kunnen handelen en maatregelen kunnen nemen. Ook is de oorzaak onderzocht en is dit besproken binnen het team. Het melden van incidenten (zoals welke incidenten, termijn van melden) aan de Inspectie JenV is nog geen onderdeel van beleid bij de politie.

Tussenconclusie

Voor een goed functionerend kwaliteitssysteem dient door DIGIT nog nader te worden gewerkt aan het signaleren van incidenten en het vastleggen van eerder gemaakte incidenten, van de geleerde lessen en de genomen maatregelen. Hierbij gaat het niet om het vastleggen met als doel 'het vastleggen', maar om te realiseren dat deze informatie inzichtelijk en makkelijk vindbaar is voor alle medewerkers, waardoor wordt bijgedragen aan een lerende organisatie. Daarnaast meldt DIGIT incidenten aan de Inspectie JenV, maar dient dit nog wel formeel een plaats te krijgen in het beleid en werkprocessen.

⁹ Verslag toezicht wettelijke hackbevoegdheid politie 2022 bladzijde 13.

Aanbevelingen

De Inspectie JenV beveelt dan ook aan om in de, nog uit te werken, maatregelen (fase 5 van het procesplan) aandacht te hebben voor maatregelen ter verbetering van het signaleren, vastleggen van incidenten, het leren hiervan en het verbeteren van de processen. Ook beveelt de Inspectie JenV aan dat het melden van incidenten en bijna-incidenten aan de Inspectie JenV onderdeel wordt van de nog op te stellen maatregelen.

5. Hoofdconclusie

DIGIT geeft uitvoering aan het, in 2023 vastgestelde, procesplan om te komen tot een kwaliteitssysteem. In de rapportage van vorig jaar signaleerde de Inspectie JenV het risico dat door onvoldoende capaciteit het operationele proces (het hacken zelf) voorrang zou krijgen op het realiseren van het kwaliteitssysteem. Door het aannemen van twee kwaliteitsmedewerkers in 2024 is dit risico door DIGIT gemitigeerd. De Inspectie JenV ziet dat met voldoende aandacht, tijd en prioriteit de stappen van het plan worden uitgevoerd. DIGIT heeft ongeveer vier maanden vertraging opgelopen ten aanzien van de planning. Ook het uitvoeren van de processtappen die toezien op het onderwerp 'informatiebeveiliging' zijn nog achtergebleven. Het ontwikkelen van het kwaliteitssysteem is inmiddels een volwaardig onderdeel geworden van de taakuitvoering van DIGIT. De Inspectie JenV heeft gekeken naar een aantal belangrijke onderdelen van het kwaliteitssysteem, waaronder de afdelingscultuur, kennis van medewerkers en de lijnverantwoordelijkheid. De Inspectie JenV concludeert dat bij DIGIT sprake is van een open cultuur met korte lijnen en de huidige cultuur een goede basis vormt voor het kwaliteitssysteem. Op een aantal onderdelen van het kwaliteitssysteem signaleert de Inspectie JenV risico's voor het goed functioneren van het kwaliteitssysteem.

Ondanks de opgelopen vertraging en de gesignaleerde risico's gaat de Inspectie JenV ervan uit dat eind 2025 een eerste versie van een werkend kwaliteitssysteem staat.

6. Opsomming en samenvatting aanbevelingen

De Inspectie JenV adviseert DIGIT en de eindverantwoordelijke voor het kwaliteitssysteem om:

- Gelet op de vertraging en het achterblijven van de activiteiten op het onderwerp 'informatievoorziening' om een aanpassing te maken op de eerder opgestelde planning. Daarbij dient de politie ook oog te hebben voor de situatie dat hierdoor mogelijk een langere periode beperkte (interne) controle plaatsvindt en geen extern toezicht op zaakniveau en de informatiebeveiliging. Door de eindverantwoordelijke dient een keuze te worden gemaakt of tussentijdse maatregelen noodzakelijk zijn;
- Zorg te dragen dat de huidige cultuur wordt behouden indien wijzigingen in het team plaatsvinden en het team wordt overgeplaatst naar de andere eenheid.

De Inspectie JenV beveelt DIGIT aan om, in de nog uit te werken maatregelen, (fase 5 van het procesplan) aandacht te hebben voor (aanvullende) maatregelen ter verbetering van:

- de kennis en het borgen van de juridische kennis van medewerkers. De Inspectie JenV dringt aan om na te denken over handvatten voor (de veelal technische) medewerkers om de juridische teksten toegankelijker te maken;
- de kennis van medewerkers over het doel en opzet van het kwaliteitssysteem als mede het borgen van deze kennis en zodanig vertalen van de theorie dat deze toepasbaar wordt voor alle medewerkers. Hierbij dient de afdeling ook oog te hebben voor het verbeteren van deze kennis op de korte termijn;
- het signaleren van incidenten en het vastleggen, het leren van incidenten en het verbeteren van de processen;
- het melden van incidenten en bijna-incidenten aan de Inspectie JenV.

Afsluitend

Vanaf 1 januari 2026 gaat DIGIT over naar een andere eenheid. Vanaf 2024 is de landelijke eenheid opgeheven en opgegaan in twee nieuwe eenheden, namelijk de eenheid Landelijke Opsporing en Interventies (hierna: LO) en de eenheid Landelijke Expertise en Operaties. DIGIT wordt ondergebracht in de eenheid LO. De Inspectie JenV gaat ervan uit dat de goede stappen die nu worden en zijn gezet, worden vervolgd en niet verloren gaan met de overplaatsing. De Inspectie JenV vraagt hier dan ook nadrukkelijk de aandacht voor. Daarnaast wijst de Inspectie JenV het lijnmanagement en de korpsleiding op de eerder opgestelde intentieverklaring en het belang van het omzetten van deze intentie op papier naar een uitwerking in de praktijk.¹⁰ Dit is des te belangrijker gelet op de wijziging die plaats gaat vinden in de aansturing van DIGIT. Dit zal vanzelfsprekend een onderwerp van aandacht zijn voor het toezicht van de Inspectie JenV.

Voor het vervolg van de implementatie van het kwaliteitssysteem is het jaar 2025 cruciaal. In 2025 worden de benodigde maatregelen beschreven op basis van de geïnventariseerde risico's en gaat DIGIT over tot het daadwerkelijk implementeren van de maatregelen en hiermee van het kwaliteitssysteem. De Inspectie JenV blijft de realisatie van het systeem nauwlettend volgen. Als laatste benadrukt de Inspectie JenV, net als in de rapportage van 2023, dat uit de (verdere) uitvoeringsfase van het procesplan en de uiteindelijke uitvoering van het kwaliteitssysteem moet blijken of de beoogde kwaliteitsslagen en intenties gerealiseerd worden.

Hoogachtend,

De inspecteur-generaal Inspectie Justitie en Veiligheid,
Namens deze,

P.C.J. Neuteboom
Hoofdinspecteur-directeur Politie, Security en Crisisbeheersing

¹⁰ Eind 2023 heeft de korpsleiding in het kader van deze lijnverantwoordelijkheid een intentieverklaring opgesteld en geaccordeerd. De intentieverklaring bevestigt de lijnverantwoordelijkheid, draagvlak en bereidheid van de politie om het kwaliteitssysteem te realiseren. Zie hiervoor de rapportage 2023 over de hackbevoegdheid van de Inspectie JenV.