Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Beveiliging van meldkamersystemen

Een onderzoek naar het inrichten en borgen van risicomanagement

Inhoudsopgave

Voorwoord

De Inspectie Justitie en Veiligheid en het Agentschap Telecom zijn bezorgd of de meldkamers voor de hulpdiensten politie, brandweer, ambulance en de marechaussee onafgebroken bereikbaar blijven en noodhulp kunnen blijven bieden aan wie dat nodig heeft. Herhaaldelijk is vastgesteld dat dit nog niet goed geregeld is[1].

Dit rapport over het risicomanagement op de informatiebeveiliging van de meldkamersystemen is een aanvulling op eerdere onderzoeken waarin de inspecties aandacht vragen voor de continuïteit van de meldkamers.

Wereldwijd vindt het opzettelijk verstoren en uitschakelen van computersystemen steeds vaker plaats. Wanneer de systemen van de meldkamers verstoord raken, zijn de meldkamers niet goed bereikbaar en loopt de hulpverlening, crisisbeheersing en opsporing gevaar.

Met dit onderzoek laat de Inspectie zien dat het Strategisch meldkamerberaad op dit moment nog onvoldoende in staat is om digitale risico's voor de meldkamersystemen in te schatten en daarop te sturen.

Het toepassen van risicomanagement op de informatiebeveiliging van de meldkamersystemen ontbreekt. Hierdoor kunnen de risico's onvoldoende worden ingeschat om tot een aanvaardbaar niveau te reduceren. Het ontbreken van risicomanagement vormt een ernstig risico voor de continuïteit van de meldkamers als onderdeel van de vitale infrastructuur van Nederland. Dit moet serieus worden opgepakt.

De Inspectie wil met dit rapport de leemtes in de opzet van de beveiliging van de meldkamersystemen inzichtelijk en bespreekbaar maken en bijdragen aan een oplossing.

De Inspectie dankt de medewerkers van de Landelijke meldkamersamenwerking, de meldkamers en van het ministerie van JenV voor hun open houding en medewerking aan dit onderzoek.

H.C.D. Korvinus
Inspecteur-generaal Inspectie Justitie en Veiligheid

[1] *Opvolging aanbevelingen onderzoek continuïteit meldkamers.* Brief van de Inspecteur-generaal Justitie en Veiligheid aan de korpsleiding van de Nationale Politie en aan de voorzitter van het Bestuurlijk Meldkamerberaad, 1 juli 2021.

1. Inleiding

1.1 Aanleiding van het onderzoek

De inspectie Justitie en Veiligheid (hierna te noemen Inspectie) deed in 2021 onderzoek naar het risicomanagement op de informatiebeveiliging van de meldkamers van politie, brandweer, ambulance en de marechaussee. Het toezicht op de meldkamers heeft geprioriteerde aandacht van de Inspectie omdat 'de communicatie met en tussen hulpdiensten middels 112 en C2000' door Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) als vitale processen zijn geïdentificeerd en daarmee deel uitmaken van de vitale infrastructuur van Nederland[2].

Voor wie 112 belt, is de meldkamer het eerste contact met de hulpdiensten van de brandweer, ambulance, politie en de marechaussee. Voor hulpverleners is een meldkamer de plek vanwaar zij informatie ontvangen over een incident en waar zij om ondersteuning vragen. Meldkamers zijn ook cruciaal bij rampenbestrijding en crisisbeheersing en worden ingezet bij het bewaken van de openbare orde en opsporing.

Dit onderzoek vond plaats omdat de Inspectie en het Agentschap Telecom bezorgd zijn of de meldkamers continu bereikbaar blijven en noodhulp kunnen bieden aan wie dat nodig heeft. Het is van levensbelang dat de continuïteit van de dienstverlening van de meldkamers goed geborgd is. Uit onderzoek in 2015 en 2019 bleek dat de meldkamers op dit punt zeer kwetsbaar zijn. In 2021 bleek opnieuw dat de continuïteit van de meldkamers nog niet goed geborgd is[3].

Dit onderzoek naar het risicomanagement op de informatiebeveiliging is een aanvulling op de genoemde onderzoeken naar de continuïteit van de meldkamers. De reden voor deze aanvulling is dat de NCTV aangeeft dat het opzettelijk verstoren en uitschakelen van de systemen van overheden steeds vaker plaatsvindt[4]. Verstoring vormt een grote dreiging voor de meldkamers. Het onderzoek vond plaats in de maanden januari tot en met juli 2021.

1.2 Doel van het onderzoek

De Inspectie wilde weten of de meldkamers voldoende weerbaar zijn tegen het opzettelijk verstoren en uitschakelen van de systemen. Hiervoor is onderzocht hoe het risicomanagement op de informatiebeveiliging van de meldkamersystemen is ingericht en wordt toegepast. Eventuele leemtes in de opzet van de beveiliging van de meldkamersystemen worden hiermee inzichtelijk en bespreekbaar.

Bij informatiebeveiliging gaat het in dit onderzoek om het vaststellen van de vereiste beveiliging van de meldkamersystemen. Het doel daarvan is de continuïteit van de hulpverlening te waarborgen door de beschikbaarheid van juiste en tijdige informatie. Deze beveiliging zorgt ervoor dat hulpverleners bij informatie in de meldkamersystemen kunnen komen wanneer men dat wil, dat de informatie klopt

[2] Zie: *Overzicht vitale processen,* www.nctv.nl
[3] *Meldkamers* (Inspectie Justitie en Veiligheid en Agentschap Telecom 2015); *Continuïteit van meldkamers* (Inspectie Justitie en Veiligheid en Agentschap Telecom 2019); *Opvolging aanbevelingen onderzoek continuïteit meldkamers.* Brief van de Inspecteur-generaal Justitie en Veiligheid aan de korpsleiding van de Nationale Politie en aan de voorzitter van het Bestuurlijk Meldkamerberaad*,* 1 juli 2021.
[4] *Cybersecuritybeeld Nederland 2021*, Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020)

en dat de informatie niet bij anderen terecht komt. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen.

Bij risicomanagement op de informatiebeveiliging gaat het erom dat inzichtelijk wordt gemaakt welke risico's er zijn en hoe deze beheerst worden. Dit vindt plaats door het systematisch inventariseren, beoordelen en beheersbaar maken van de risico's die de informatie in de meldkamersystemen bedreigen.

De systemen van de meldkamers worden beveiligd door de Landelijke meldkamersamenwerking (LMS). Dat is een bijzonder organisatieonderdeel[5] van de Nationale Politie. Het Strategisch Meldkamer Beraad (SMB) is op grond van de *Regeling hoofdlijnen beleid en beheer meldkamers* verantwoordelijk voor het strategisch aansturen van de LMS op het beheer van de risico's in de informatiebeveiliging[6]. Het Bestuurlijk Meldkamer Beraad stelt voor de minister van JenV een beleids- en bestedingsplan op, het monitort de werking daarvan en beslist over voorstellen van het Strategisch Meldkamer Beraad die binnen het vastgestelde beleids- en bestedingsplan bestuurlijke borging behoeven[7].

Met de uitkomsten van dit onderzoek wil de Inspectie bijdragen aan het waarborgen van de informatieveiligheid van de meldkamersystemen en daarmee aan de continuïteit van de meldkamers.

1.3 Centrale vraag en onderzoeksvragen

De Inspectie wil een antwoord geven op de volgende centrale vraag:

Hoe is het risicomanagement op de informatiebeveiliging van de meldkamersystemen vormgegeven?

Om tot een antwoord te komen, beantwoordt de Inspectie de volgende onderzoeksvragen:

- *Hoe is het risicomanagement ingericht en geborgd?*
- *Hoe zijn de risico's voor de veiligheid van de informatie geïdentificeerd?*
- *Hoe zijn vervolgens de risico's voor de veiligheid van de informatie geanalyseerd en geëvalueerd?*
- *Hoe zijn de maatregelen voor risicobeperking gekozen, vastgesteld en uitgevoerd?*
- *In welke mate zijn de overblijvende risico's geaccepteerd?*

[5] De LMS dat is een bijzonder onderdeel van de Nationale Politie omdat de sturing gebeurt vanuit multi governance. De veiligheidsregio's, ambulancezorgorganisaties, politie en KMar sturen samen op de prioriteiten en de allocatie van het (multi)budget.

[6] Het SMB is op grond van artt. 2 en 4 lid 1 van de *Regeling hoofdlijnen beleid en beheer meldkamers* verantwoordelijk voor de aansturing van de LMS. Het SMB is daarmee verantwoordelijk voor het beheer van de risico's in de informatiebeveiliging.

Art. 4 lid 5 van de regeling beschrijft hoe het SMB deze aansturing moet uitvoeren:
Het Strategisch Meldkamer Beraad verzamelt de inbreng voor het beleids- en bestedingsplan; draagt zorg voor het opstellen van het beleids- en bestedingsplan en de jaarverantwoording op landelijk niveau; beslist binnen de kaders van het beleids- en bestedingsplan over de uitvoering van beleid en beheer; bewaakt de uitvoering van het beleids- en bestedingsplan; doet voorstellen voor de agenda van het Bestuurlijk Meldkamer Beraad; adviseert het Bestuurlijk Meldkamer Beraad; kan hulpstructuren instellen, die bijdragen aan het realiseren van de vastgestelde kaders voor beleid en beheer.

[7] Bijlage II geeft een beschrijving van de aansturing van de LMS.

1.4 Afbakening

Dit onderzoek beschrijft in hoeverre de informatiebeveiliging van de meldkamersystemen in beheer bij de LMS wordt gebaseerd op risicomanagement, zoals bedoeld in het wettelijk kader dat bestaat uit de *Regeling hoofdlijnen beleid en beheer meldkamers*, het *Voorschrift informatiebeveiliging rijksdienst, de Baseline informatiebeveiliging overheid (BIO)* en de standaarden *ISO/IEC 27001, 27002 en 27005*[8].

De *Regeling hoofdlijnen beleid en beheer meldkamers* beschrijft de verdeling verantwoordelijkheden van de partijen die deelnemen aan de landelijke meldkamersamenwerking, de wijze van sturing op het beheer, en de zorgplicht voor informatieveiligheid.

Het *Voorschrift informatiebeveiliging rijksdienst* en de *BIO* geven de kaders voor de inrichting en de borging van de informatiebeveiliging. De *BIO* is gebaseerd op de standaarden *ISO/IEC 27001, 27002,* en de specifieke uitgangspunten voor het inrichten en borgen van risicomanagement op de informatiebeveiliging vinden hun grondslag in de standaard *ISO/IEC 27005*.

In de standaard *ISO/IEC 27005* zijn alle aspecten van het wettelijk kader voor het inrichten en borgen van risicomanagement op de informatiebeveiliging uitgewerkt. Een deel van deze standaard is daarmee het toetsingskader dat bij dit onderzoek is gehanteerd. Het toetsingskader omvat de uitgangspunten uit de hoofdstukken 7, 8, 9 en 10 van de standaard die specifiek gaan over de opzet en het toepassen van risicomanagement. Deze vormen de kern van het risicomanagement en is de focus van dit onderzoek. De tabel in bijlage I geeft een nadere toelichting op dit toetsingskader. De andere onderdelen van de standaard *ISO/IEC 27005* zoals monitoring, review, communicatie en consultatie, blijven in dit onderzoek buiten beschouwing[9].

Het onderzoek werd uitgevoerd op de dienstverlening die de LMS vanuit haar wettelijke beheertaak verricht rondom de informatiebeveiliging van de meldkamersystemen. Enerzijds toetst de Inspectie op hetgeen feitelijk door de LMS is geïmplementeerd voor het beheer van de risico's in de informatiebeveiliging. Anderzijds biedt het inzicht in de aansturing vanuit het SMB.

Het risicomanagement op systemen die buiten de meldkamersamenwerking vallen, is in dit onderzoek niet meegenomen[10]. Deze systemen worden zelfstandig door de hulpdiensten beheerd volgens een eigen beveiligingsregime.

1.5 Aanpak van het onderzoek

Het beschrijven van het risicomanagement en het vaststellen van mogelijke leemtes in de opzet van de informatiebeveiliging vraagt om een stapsgewijze aanpak. Deze paragraaf zet uiteen welke stappen zijn gezet om tot een antwoord te komen op de centrale vraag: *Hoe is het risicomanagement op de informatiebeveiliging van de meldkamersystemen vormgegeven?*

[8] De internationale standaard ISO/IEC 27005 voor informatietechnologie, beveiligingstechniek en risicomanagement voor Informatiebeveiliging. Zie ook hoofdstuk 2 Kaders en bijlage I voor een toelichting op de genoemde beveiligingsrichtlijnen.
[9] Zie ook bijlage I.
[10] Het gaat hier onder meer om de systemen LCMS dat in gebruik is bij afzonderlijke hulpdiensten, LCPS van ambulancediensten, en WAS en INS van de brandweer.

Stap 1: Informatiebeveiliging van de meldkamervoorzieningen

De eerste stap richtte zich op de informatiebeveiliging vanuit het perspectief van de meldkamers.

In gesprekken met de directeur/CIO van de LMS[11], de functionaris voor informatiebeveiliging en andere medewerkers namen de inspecteurs kennis van de visie van het SMB en de LMS op informatiebeveiliging. Ook het verloop van het traject voor de inrichting van de informatiebeveiliging en de totstandkoming van het samenwerkingsverband van meldkamers kwam daarbij aan de orde. Daarnaast werd besproken welke partijen een rol spelen in de informatiebeveiliging en hoe de verantwoordelijkheden zijn belegd. Ook sprak de Inspectie met medewerkers van het directoraat-generaal Politie en Veiligheidsregio's over informatiebeveiliging en over het programma voor kwalitatieve verbeteringen in het meldkamerdomein. Dat is omdat het ministerie van JenV kaders stelt voor het beheer van enkele meldkamersystemen[12]. Ten slotte spraken de onderzoekers met medewerkers van de meldkamers die zitting hebben in gremia voor onderlinge samenwerking op het gebied van informatiebeheer en -beveiliging.

Stap 2: Inrichting en borging van het risicomanagement

In de tweede stap onderzocht de Inspectie welke beheermaatregelen zijn genomen om de meldkamersystemen weerbaar te maken tegen het opzettelijk verstoren en uitschakelen. De Inspectie wilde hiervoor van de LMS weten hoe het risicomanagement op de informatiebeveiliging van de meldkamersystemen is ingericht en geborgd, zoals bedoeld in het toetsingskader *ISO/IEC 27005*.

De feitelijke inrichting en borging van het risicomanagement stelde de Inspectie vast aan de hand van documenten die zij opvroeg bij de LMS, de Nationale Politie, de meldkamers en bij het directoraat-generaal Politie en veiligheidsregio's van het ministerie van JenV. De uitkomsten zijn aansluitend besproken in de interviews.

In deze gesprekken kwam tevens aan de orde: hoe de risico's voor de veiligheid van de informatie zijn geïdentificeerd; en hoe vervolgens de risico's voor de veiligheid van de informatie zijn geanalyseerd en geëvalueerd. Daarnaast wilde de Inspectie van de LMS weten hoe de beheermaatregelen voor risicobeperking zijn gekozen, vastgesteld en uitgevoerd; en in welke mate de overblijvende risico's zijn geaccepteerd.

Stap 3: Het groepsgesprek

De bevindingen uit de voorgaande stappen besprak de Inspectie in een bijeenkomst met de directeur/lid van het SMB, en met medewerkers van de LMS en een hoofd van een meldkamer om te peilen in hoeverre de bevindingen in algemene zin werden herkend. De Inspectie benoemde in het gesprek geconstateerde leemtes in de inrichting en borging van het risicomanagement en vroeg de LMS om hierop te reageren.

[11] De directeur is naast Chief information officer (CIO) van de LMS, heeft zitting in het SMB en is ook de voorzitter van het Overleg Hoofden Meldkamers.
[12] Het ministerie JenV is eigenaar van de systemen C2000, GMS, NL-Alert en WAS.

De uitkomsten van de drie stappen zijn in deze rapportage verwerkt.

1.6 Leeswijzer

Hoofdstuk 2 beschrijft de uitkomsten van het onderzoek naar het vormgeven van risicomanagement op de informatiebeveiliging van de meldkamersystemen. Aan het begin van iedere paragraaf wordt beschreven wat vanuit het wettelijk kader van het SMB wordt verwacht. Deze verwachtingen zijn uitgewerkt in het toetsingskader in bijlage I.

Paragraaf 2.1 beschrijft de situatie die de Inspectie tijdens het onderzoek aantrof, en de beveiligingsafspraken die de LMS in de Werkgroep Informatiebeveiliging Meldkamers ontwikkelt. Paragraaf 2.2 beschrijft hoe het risicomanagement tijdens het onderzoek is ingericht en geborgd. Het gaat hier om het vastleggen van de reikwijdte, de context en de criteria voor het beheren van risico's. Paragraaf 2.3 gaat over risicobeoordeling. Het geeft weer hoe de risico's voor de veiligheid van de informatie zijn geïdentificeerd, geanalyseerd en geëvalueerd. Paragraaf 2.4 en 2.5 beschrijven hoe de maatregelen voor risicobeperking zijn gekozen en vastgesteld en in welke mate het SMB de overblijvende risico's accepteert.

Hoofdstuk 3 vat de voornaamste uitkomsten van het onderzoek samen en geeft de Inspectie haar oordeel over de wijze waarop het risicomanagement op de informatiebeveiliging van de meldkamersystemen is vormgegeven, gevolgd door aanbevelingen.

2. Bevindingen en conclusies

2.1 De basis van informatiebeveiliging

Deze paragraaf beschrijft welke plaats risicomanagement inneemt in de informatiebeveiliging van de meldkamersystemen.

Verwachting

Van het SMB wordt verwacht dat het toeziet dat de meldkamersystemen zijn beveiligd op basis van risicomanagement, en het de LMS aanstuurt op het beheer daarvan[13].

Bevinding

Beveiligingsafspraken voor de meldkamersystemen

Het SMB werkt ten tijde van het onderzoek aan het ontwikkelen van informatiebeveiliging van de meldkamersystemen op basis van risicomanagement. Dit is aangekondigd in het *Beleids- en bestedingsplan Meldkamers 2021.*

De LMS coördineert deze werkzaamheden en de informatiebeveiliging zal bestaan uit een set van afspraken voor het gebruik en beheer van de meldkamersystemen, en uit een uitvoeringsplan. Dat blijkt uit gesprekken met de LMS en documenten die de Inspectie heeft ingezien[14]. De basis voor de beveiligingsafspraken zijn het *Bouwplan LMS* en het *Faseplan 4 voor het verbeteren Informatiebeveiliging LMS en de meldkamers*[15]. De Inspectie stelt vast dat deze basisdocumenten conceptversies zijn en niet door het SMB zijn vastgesteld.

De kaders voor het uitwerken van de beveiligingsafspraken worden opgesteld door de Werkgroep Informatiebeveiliging Meldkamers. Deze bestaat uit vertegenwoordigers van Ambulancezorg Nederland, de Nationale Politie, de ministeries van Defensie en JenV, de veiligheidsregio's en de LMS. De werkgroep doet het SMB een voorstel voor het gewenste beveiligingsniveau, en een voorstel voor het informatiebeveiligingsbeleid waarbij rekening wordt gehouden met specifieke beveiligingsvoorschriften die binnen ambulancezorg, brandweer, politie en marechaussee van toepassing zijn.

Een stafafdeling van de LMS zal volgens de voorstellen de risico's beheren. De nadere invulling van dit aangekondigde risicomanagement is ten tijde van het onderzoek nog niet uitgewerkt. De LMS verwacht dat het SMB in september 2021 een definitieve beslissing neemt over het uitvoeren van de voorstellen.

---

[13] Zoals bedoeld in het wettelijk kader dat bestaat uit de *Regeling hoofdlijnen beleid en beheer meldkamers*, het *Voorschrift informatiebeveiliging rijksdienst, de Baseline informatiebeveiliging overheid (BIO)* en de standaarden *ISO/IEC 27001, 27002 en 27005.* Zie paragraaf 1.4.
[14] *Procesvoorstel Beleidskader voor Informatie-beveiligingsbeleid voor multi-meldkamervoorzieningen*, 10 juli 2020 (LMS) en *Notitie SvZ informatiebeveiligingsbeleid*. Concept 5 juli 2021. (LMS)
[15] *Bouwplan LMS*, concept 0.5 (LMS 2021) *Verbetering Informatiebeveiliging LMS en MKs*, concept 1.0 (LMS 2020) en *Verbeteren Informatiebeveiliging LMS en Meldkamers. Faseplan Fase 4*, versie 0.3 (LMS 2021)

Conclusie

De Inspectie concludeert dat het SMB de informatiebeveiliging van de meldkamersystemen ten tijde van het onderzoek nog niet aanstuurt op basis van risicomanagement.

2.2 Het inrichten en borgen van risicomanagement

Nu blijkt dat de meldkamersystemen nog niet zijn beveiligd op basis van risicomanagement, is de Inspectie aan de hand van het toetsingskader nagegaan op welke onderdelen van het ontwikkelingsproces inmiddels al wel stappen zijn gezet, en welke bouwstenen voor het inrichten en borgen van risicomanagement inmiddels aanwezig zijn.

Verwachting

Van het SMB wordt verwacht dat dit het risicomanagement voor de veiligheid van informatie inricht en borgt[16]. Dit houdt het volgende in:

Het stuurt op het bepalen van de context voor het beheren van informatie risico's. Dat houdt in: het vaststellen van basiscriteria voor het risicobeheer; het definiëren van de reikwijdte en de grenzen; en het organiseren van het uitvoeren van informatierisicomanagement.

Het stuurt op het beschrijven hoe het proces van risicomanagement op de informatiebeveiliging is ingericht en wordt toegepast. Hierbij worden criteria voor het evalueren van risico's opgesteld, en criteria voor het bepalen van de gevolgen van incidenten, en voor het accepteren van deze risico's[17].

Vervolgens stuurt het op het analyseren en beschrijven van de omgeving waarin de meldkamers de taken uitvoeren. Hierbij worden ook alle relevante bedrijfsprocessen en bedrijfsmiddelen in kaart gebracht. De uitkomsten van de omgevingsanalyse en de relevante bedrijfsprocessen en bedrijfsmiddelen zijn in de risicobeoordeling meegenomen.

Tenslotte stuurt het SMB op het vastleggen van de verantwoordelijkheden en de wijze waarop het informatie risicomanagement zal worden uitgevoerd.

Bevinding

Uit de gesprekken en de ontvangen documenten blijkt dat het hierboven beschreven proces voor het inrichten en borgen van risicomanagement als volgt is doorlopen:

Basiscriteria en het definiëren van reikwijdte en grenzen

Uit de documenten die de Inspectie heeft bestudeerd, blijkt dat de verwachte basiscriteria om de informatierisico's te kunnen beheren nog niet zijn opgesteld.

[16] Zoals bedoeld in het wettelijk kader dat bestaat uit de *Regeling hoofdlijnen beleid en beheer meldkamers*, het *Voorschrift informatiebeveiliging rijksdienst*, *de Baseline informatiebeveiliging overheid (BIO)* en de standaarden *ISO/IEC 27001, 27002 en 27005.* Zie paragraaf 1.4.
[17] Zoals bedoeld in 7.2.2, 7.2.3 en 7.2.4 van *NEN-ISO/IEC 27005*.

Ook de reikwijdte en de grenzen van het beheer van de informatiebeveiliging zijn nog niet duidelijk vastgelegd. In 2020 is wel vastgelegd welke processen en systemen van vitaal belang zijn voor de continuïteit van de meldkamers. In 2017 zijn de processen van het Meldkamerdienstencentrum beschreven[18]. Ondanks dat relevante bedrijfsprocessen en bedrijfsmiddelen in kaart zijn gebracht, is er nog geen relatie gelegd met het vastleggen van de reikwijdte van het informatie-risicomanagement.

Het toepassen van risicomanagement organiseren

Het risicomanagement voor informatiebeveiliging kan op dit moment nog niet worden toegepast vanwege het ontbreken van de genoemde basiscriteria, en het vastleggen van de reikwijdte en de grenzen van het beheer van de informatiebeveiliging. In 2020 wordt dit ontbreken van risicomanagement door de LMS als onvolkomenheid geadresseerd in de notitie *Verbetering Informatiebeveiliging LMS en MKs*. De LMS onderkent daarin dat er nog geen regie is op risicobeheersing en dat hieraan structureel onvoldoende aandacht wordt besteed. Zij stelt vast dat informatiebeveiliging en continuïteit nog onvoldoende zijn ingebed in de staande organisatie.

De Inspectie stelt vast dat LMS in deze notitie de ernst van de situatie onderkent, als zij schrijft dat er beveiligingsrisico's aanwezig zijn die weggenomen moeten worden: *'Om deze risico's te kunnen beheersen is een beheersingsproces nodig. Zonder zo'n proces zijn risico's niet inzichtelijk, kan geen juiste risicoafweging plaatsvinden, worden niet altijd de juiste tegenmaatregelen getroffen en worden budgetten suboptimaal gebruikt.*[19]' Ook benoemt de LMS in 2021 het risicomanagement en informatiebeveiliging als essentiële, maar afzonderlijke kennisgebieden waarin moet worden geïnvesteerd voor de opbouw van de landelijke samenwerking van meldkamers[20].

De Inspectie stelt vast dat het proces voor het inrichten en toepassen van risicomanagement op de informatiebeveiliging ten tijde van het onderzoek nog niet is beschreven. Een PDCA-cyclus voor informatiebeveiliging is bijvoorbeeld niet ingericht. Ook de criteria voor risico-evaluatie, de criteria voor impact en criteria voor risico-acceptatie zijn nog niet vastgelegd. De LMS benoemt in de notitie *Verbetering Informatiebeveiliging LMS en MKs*, al wel het belang van het inrichten van een planning- en controlcyclus met elementen uit de *BIO*[21].

---

[18] *Plan van aanpak. Continuïteit meldkamers en meldkamer-processen tijdens Covid-19 crisis*, versie 7-4-2020 (LMS 2020) blz. 6-8. De lijst met vitale processen en systemen is goedgekeurd in het SMB van 27 maart 2020.
Procesbeschrijving Release & Deployment Management, concept 1.9 (Nationale Politie 2017); *Procesbeschrijving Configuration and Asset Management*, concept 1.x (Nationale Politie 2017); *Procesbeschrijving Problem management*, concept 1.1 (Nationale Politie 2017); *Procesbeschrijving Change management*, concept 1.7 (Nationale Politie 2017); *Procesbeschrijving Incident management*, concept 0.2 (Nationale Politie 2017).

[19] *Verbetering Informatiebeveiliging LMS en MKs*, concept 1.0 (LMS 2020) blz. 9. Zie ook *Beleids- en bestedingsplan Meldkamers 2021* versie 30 september 2020 (LMS 2020)

[20] Bouwplan LMS, concept 0.5 (LMS 2021) blz. 3-6 en *Bouwtekening LMS*, concept 0.7 (LMS)

[21] *Verbetering Informatiebeveiliging LMS en MKs*, concept 1.0 (LMS 2020) blz.10.
De CIS 20-controls is een set van 20 kritische beveiligingscontroles die is ontwikkeld door het Center for Internet Security.

Het vastleggen van criteria

Uit een risicoanalyse uit 2017 van het communicatienetwerk C2000[22] blijkt dat voor dit systeem de gevolgen van incidenten zijn geëvalueerd. Dit was op initiatief van het Meldkamerdienstencentrum. De criteria die hiervoor werden gehanteerd, zijn niet bij andere meldkamersystemen toegepast[23]. Wel zijn voor het accepteren van risico's aantoonbaar criteria opgesteld. Daarover meer in paragraaf 2.5.

Omgevingsanalyse

De omgeving waarin de meldkamers hun taken uitvoeren, is nog niet geanalyseerd en beschreven. Ook de relevante bedrijfsprocessen zijn nog niet beschreven. De relevante bedrijfsmiddelen zijn met een inventarisatie van het applicatielandschap al wel in kaart gebracht. De LMS kon in de gesprekken niet aangeven in hoeverre het genoemde overzicht van vitale processen en systemen, en de procesbeschrijvingen van het Meldkamerdienstencentrum volledig en actueel zijn[24].

Verantwoordelijkheden

Uit de gesprekken blijkt dat er tussen het ministerie van JenV en de LMS een verschil van inzicht bestaat over het invullen van de verantwoordelijkheden. Voor de LMS als beheerder blijft daardoor onduidelijk wie nu waarvoor verantwoordelijk is en dit staat een vlotte inrichting van de informatiebeveiliging in de weg.

Het gaat hier volgens JenV om een verschil in inzicht in de interpretatie van de taak van de LMS op basis van de *Regeling hoofdlijnen beleid en beheer meldkamers*. JenV vindt dat de LMS op basis van deze regeling een regiefunctie moet vervullen op het gebied van informatiebeveiliging.[25] Het benadrukt dat de LMS en de meldkamers deze bepaling verder moeten uitwerken naar de praktijk. Het ministerie gaf in het gesprek aan hierover met de LMS in gesprek te zijn en aanbiedt om hen bij te staan in het maken van de vertaalslag.

Conclusie

De Inspectie concludeert dat het proces voor het vaststellen van basiscriteria voor het inrichten, toepassen en borgen van het risicomanagement nog niet volledig is doorlopen. Essentiële processtappen ontbreken of zijn maar ten dele uitgevoerd. Dit staat een vlotte inrichting en borging van de informatiebeveiliging in de weg.

Het SMB heeft de context waarin het de risico's in de informatiebeveiliging laat beheren nog niet vastgesteld. Het proces voor het inrichten en toepassen van risicomanagement is nog niet beschreven. Er zijn nog geen criteria opgesteld voor het evalueren van de risico's en de gevolgen van informatiebeveiligingsincidenten.

---

[22] C2000: een gesloten communicatienetwerk voor de hulpverleningsdiensten, maakt deel uit de vitale infrastructuur.
[23] *Resultaten Risicoanalyse C2000*, versie 1.0 (Nationale Politie, QSight IT 2017)
[24] *Rapportage LMS. Technische architectuur. Vooronderzoek*, versie 1.0 (KPMG 2020) blz. 13; *Overzicht business applicaties en koppelingen per voorziening en thema.* (LMS 29-1- 2020); *Applicatieoverzicht entiteiten*. Versie 14 (LMS)
[25] *Regeling hoofdlijnen beleid en beheer meldkamers*, Toelichting onder 2: 'De Landelijke Meldkamer Samenwerking ondersteunt de partijen en neemt daarbij initiatief om de samenwerking te stimuleren, zodat de betrokken partijen gezamenlijk komen tot goed ingerichte en functionerende meldkamers waar de partijen hun meldkamerfunctie kunnen uitoefenen.'

Ook ontbreken de criteria voor het accepteren van beveiligingsrisico's, met uitzondering van de criteria die Meldkamer Dienstencentrum heeft vastgesteld bij de risicoanalyse C2000 uit 2017. Een omgevingsanalyse is nog niet uitgevoerd en de verdeling van de verantwoordelijkheden is voor de LMS niet voldoende begrijpelijk uitgewerkt.

2.3 Het beoordelen van de risico's

Deze paragraaf beschrijft hoe de risico's voor de informatiebeveiliging van de meldkamersystemen zijn geïdentificeerd, geanalyseerd en geëvalueerd.

Verwachting

Van het SMB wordt verwacht dat het de risico's voor de informatiebeveiliging van de meldkamersystemen beoordeelt, en deze vervolgens vergelijkt met de criteria voor het evalueren en accepteren van risico's[26]. Dit houdt het volgende in:

Het SMB stuurt op het identificeren van de risico's, dat deze worden beschreven en geprioriteerd ten opzichte van de eerdergenoemde criteria voor risico-evaluatie en de beveiligingsdoelstellingen die voor de meldkamers relevant zijn. Ook het identificeren van de bedrijfsmiddelen die relevant zijn voor de reikwijdte van de risicobeoordeling valt hieronder.

Daarnaast stuurt het op het identificeren van de relevante dreigingen en de bronnen voor deze dreigingen; het identificeren van de relevante bestaande en geplande maatregelen; en het identificeren van de kwetsbaarheden die geëxploiteerd kunnen worden door de geïdentificeerde dreigingen die kunnen leiden tot schade aan de geïdentificeerde bedrijfsmiddelen.

Ook stuurt het SMB op het identificeren van de gevolgen van het verstoren van de beschikbaarheid, integriteit en de vertrouwelijkheid van zijn bedrijfsmiddelen. Het bepalen van de kans op optreden van de incidenten, en bepalen van het risico voor elk van de relevante incidenten.

Bevinding

Uit de gesprekken en documenten blijkt dat het proces voor het beoordelen van de risico's voor de veiligheid van informatie als volgt is doorlopen:

Identificeren van risico's voor bedrijfsmiddelen

De LMS benoemt het belang van het volledig doorlopen van het proces van identificeren van de risico's voor de bedrijfsmiddelen. Dit blijkt uit de gesprekken en de conceptnotitie *Verbetering Informatiebeveiliging LMS en MKs* uit 2020[27].

Hiervoor zijn drie aanleidingen: De informatiebeveiligingsfunctionaris benoemde de noodzaak hiertoe. De uitkomsten van Quickscans en Securityscans meldkamers die het meldkamerdienstencentrum van de politie tussen 2019 en 2020 door Deloitte liet uitvoeren. Ook benadrukte een KPMG-rapportage uit 2020 dat de risico's en

[26] Zoals bedoeld in het wettelijk kader dat bestaat uit de *Regeling hoofdlijnen beleid en beheer meldkamers*, het *Voorschrift informatiebeveiliging rijksdienst*, *de Baseline informatiebeveiliging overheid (BIO)* en de standaarden *ISO/IEC 27001, 27002 en 27005.* Zie paragraaf 1.4.
[27] *Rapportage LMS. Technische architectuur. Vooronderzoek*, versie 1.0 (KPMG 2020) en *Verbetering Informatiebeveiliging LMS en MKs*, concept 1.0 (LMS 2020) blz. 8.

hiaten in de technische architectuur transparant moeten worden vastgelegd, want het is voor de LMS en de meldkamers niet duidelijk welke beveiligingsrisico's zij nemen.

Echter, de risico's voor de meldkamersystemen zijn nog niet volledig geïdentificeerd. De Inspectie stelde dit vast na het inzien van de risicoanalyses van 112, GMS, NL-Alert, de *Risicoanalyse C2000* uit 2017 en 2018 en van een reeks onderzoeken naar kwetsbaarheden in de technische infrastructuur van de meldkamers uit 2019 en 2020[28].

In de risicoanalyses van 112, GMS en NL-Alert is een reeks van dreigingen voor de meldkamersystemen benoemd, maar deze dreigingen zijn niet als risico's geïdentificeerd in de zin van de ISO/IEC 27005. De risicoanalyse van C2000 laat wel een identificatie, analyse en een evaluatie van de risico's zien en is wel uitgevoerd zoals bedoeld in ISO/IEC 27005. De LMS kon overigens in de gesprekken niet aangeven in hoeverre de uitkomsten uit 2017 nog actueel zijn.

De onderzoeken naar de technische infrastructuur[29] brachten kwetsbaarheden aan het licht die ten tijde van het onderzoek projectmatig met beheermaatregelen worden verholpen.

De onderzoeken zijn uitgevoerd aan de hand van de CIS-20 controls. Hiermee is de informatiebeveiliging van de meldkamers getoetst op weerbaarheid tegen de wereldwijd meest voorkomende soorten cyberaanvallen. Dit is anders uitgevoerd dan het inrichten en borgen van een beveiliging op maat die is gebaseerd op een risicoanalyse zoals bedoeld in ISO/IEC 27005. Doordat is getoetst op de meest voorkomende bedreigingen is het lastig om met de uitkomst daarvan een volledig en actueel beeld te vormen van de specifieke risico's voor de meldkamersystemen.

Identificeren van dreigingen en kwetsbaarheden

Het dreigingsbeeld voor de meldkamers is op hoofdlijnen door de Nationaal Coördinator Terrorismebestrijding en Veiligheid benoemd[30]. Het is bij de LMS niet bekend of deze dreigingen verder in een identificatie zijn uitgewerkt. Het belang van het in beeld hebben van passende maatregelen is in 2020 benoemd in een onderzoek van KPMG naar technische architectuur. De LMS kreeg daarbij de aanbeveling om met de ambulance, brandweer, politie en de marechaussee, op basis van risicoanalyses periodiek te evalueren of voldoende maatregelen zijn getroffen[31].

Het SMB heeft de kwetsbaarheden in de informatiebeveiliging van de meldkamersystemen in kaart gebracht, maar het is niet bekend in hoeverre deze identificatie volledig en actueel is. De volgende paragraaf gaat hierop verder in.

---

[28] *Risicoanalyse 112*, concept 0.1 (LM0 2017); *Risicoanalyse C2000* (QsightIT 2017) status onbekend; *Risicoanalyse GMS*, concept 0.2 (LMO 2017); *Risicoanalyse NL-Alert*, concept 0.1 (LMO 2018) en *Quickscans en Security scans meldkamers* (Deloitte 2019-2020)
[29] Quickscans en Security scans meldkamers (Deloitte 2019-2020)
[30] Communicatie met en tussen hulpdiensten middels 112 en C2000 is als vitaal proces aangewezen in: *Nationaal crisisplan digitaal* (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020)
[31] *Rapportage LMS. Technische architectuur. Vooronderzoek*, versie 1.0 (KPMG 2020) blz. 16 en 21.

Identificeren van gevolgen van verstoring

De Inspectie kon uit de toegezonden documenten opmaken dat de gevolgen van het verstoren van de beschikbaarheid, integriteit en de vertrouwelijkheid van zijn meldkamersystemen en informatie nog niet zijn geïdentificeerd.

Het risico van elk van de relevante incidenten is niet bepaald, met uitzondering van de gevolgen van een verstoring van C2000. De risicoanalyse van C2000 is door het Meldkamerdienstencentrum uitgevoerd. De resultaten zijn niet aan het SMB gepresenteerd met als gevolg dat het SMB geen inzicht heeft in de gevolgen van een verstoring van C2000.

Conclusie

De Inspectie concludeert dat de risico's voor informatiebeveiliging van de meldkamersystemen nog niet volledig zijn beoordeeld en vergeleken met de criteria voor het evalueren en accepteren van risico's. Hierdoor heeft het SMB geen volledig en actueel inzicht van de specifieke risico's voor de meldkamersystemen.

2.4 Het kiezen en vaststellen van risicobeperkende maatregelen

Deze paragraaf beschrijft hoe de maatregelen voor risicobeperking zijn gekozen en vastgesteld.

Verwachting

Van het SMB wordt verwacht dat het de LMS stuurt op het kiezen van maatregelen voor risicobeperking, dat deze maatregelen worden vastgesteld en aanstuurt op het uitvoeren van deze maatregelen[32].

Bevinding

De LMS heeft naar aanleiding van de onderzoeken naar de kwetsbaarheden in de technische infrastructuur van de meldkamers maatregelen voor beperking vastgesteld, en voert deze maatregelen uit[33]. Paragraaf 2.3 beschrijft dat de toetsing op de meest voorkomende bedreigingen het lastig maakt om een zo volledig mogelijk en actueel beeld te vormen van de specifieke risico's voor de meldkamersystemen. De toegepaste CIS-20 methode maakt het eveneens lastig om een zo volledig en actueel mogelijk beeld te vormen van de benodigde risicobeperkende maatregelen. De beveiliging van de meldkamersystemen is hiervoor beperkt en afhankelijk van de professionele inzichten en loyale inzet van medewerkers van de LMS.

De gekozen maatregelen worden op dit moment uitgevoerd binnen het project Verbeteren Informatiebeveiliging LMS en MK's. De LMS rapporteert het SMB maandelijks over de voortgang.

---

[32] Zoals bedoeld in het wettelijk kader dat bestaat uit de *Regeling hoofdlijnen beleid en beheer meldkamers*, het *Voorschrift informatiebeveiliging rijksdienst*, *de Baseline informatiebeveiliging overheid (BIO)* en de standaarden *ISO/IEC 27001, 27002 en 27005.* Zie paragraaf 1.4.

[33] *Maandelijkse rapportage aanbevelingen analyses Cyberprogramma, 20 mei 2020 en 22 maart 2021 (LMS*) en *Verbeteren Informatiebeveiliging LMS en Meldkamers. Faseplan Fase 4, versie 0.3 (LMS 2021) blz. 11*

In 2019 liet het Ministerie van JenV binnen het programma Implementatie Vernieuwing C2000 tweemaal een penetratietest uitvoeren, waarbij diverse technische kwetsbaarheden aan het licht kwamen. De uitkomsten daarvan zijn verwerkt in het *Beveiligingsplan C2000*. Dit plan is bedoeld voor het uitvoeren van maatregelen voor de verbetering van de informatiebeveiliging. Het gaat hier om maatregelen om de beleidsvorming en aanvullende operationele uitwerking aan te passen.

Conclusie

De Inspectie concludeert dat voor de meldkamersystemen maatregelen zijn getroffen voor risicobeperking. Deze zijn gekozen op basis van de meest voorkomende bedreigingen. Hierdoor bestaat het risico dat bij het SMB ontbreekt aan de juiste informatie voor het gericht aansturen op risicobeperkende maatregelen.

2.5 Het accepteren van de overblijvende risico's

Deze paragraaf beschrijft in welke mate de overblijvende risico's zijn geaccepteerd.

Verwachting

Van het SMB wordt verwacht dat aan de hand van de risicocriteria is beschreven welke rest-risico's het aanvaardt. Daarnaast dat het goedkeuring verleent aan de overblijvende risico's en de LMS aanstuurt op het beheer van deze risico's[34].

Bevinding

Uit de gesprekken komt het beeld naar voren dat de LMS bekend is met het toepassen van criteria voor het accepteren van rest-risico's. De conceptnotitie *Verbetering Informatiebeveiliging LMS en MKs* en het daarmee verbonden faseplan uit 2020 beschrijven dat specifiek voor het projectmatig inhalen van de beveiligingsachterstanden bij de meldkamers criteria zijn opgesteld voor de overblijvende risico's[35]. De notitie beschrijft een werkwijze waarin de expertgroep voor informatiebeveiliging advies geeft aan een stuurgroep van de LMS over het accepteren van risico's. Volgens de conceptnotitie gelden de volgende criteria voor het accepteren van de risico's:

- *'De betreffende projectdocumenten zijn overgedragen aan de beheerorganisatie.*
- *De oplevering van documenten is actueel en door de (lokale) beheerorganisatie getoetst en akkoord bevonden.*
- *De wijze waarop maatregelen worden doorgevoerd zijn akkoord bevonden door de leden van de Expertgroep en daarmee in lijn met vigerend beleid, architectuur, of andere relevante kwaliteitscriteria.'*

Buiten het kader van het projectmatig wegwerken van achterstanden in de informatiebeveiliging worden geen criteria voor risico-acceptatie toegepast. Uit de documenten en de gesprekken zijn geen aanwijzingen naar voren gekomen dat er

[34] Zoals bedoeld in het wettelijk kader dat bestaat uit de *Regeling hoofdlijnen beleid en beheer meldkamers*, het *Voorschrift informatiebeveiliging rijksdienst*, *de Baseline informatiebeveiliging overheid (BIO)* en de standaarden *ISO/IEC 27001, 27002 en 27005.* Zie paragraaf 1.4.
[35] *Verbetering Informatiebeveiliging LMS en MKs*, concept 1.0 (LMS 2020) en *Verbeteren Informatiebeveiliging LMS en Meldkamers. Faseplan Fase 4*, versie 0.3 (LMS 2021) blz. 19

voor het inrichten en borgen van risicomanagement criteria voor het accepteren van rest-risico’s zijn opgesteld en vastgesteld.

Conclusie

De Inspectie concludeert dat voor het inrichten en borgen van risicomanagement nog geen criteria zijn vastgesteld voor het accepteren van rest-risico’s. Hierdoor staat niet vast welke rest-risico’s het SMB aanvaardt in de aansturing van de LMS op het beheer van de meldkamersystemen.

3. Samenvattend oordeel en aanbevelingen

Het SMB beslist over de uitvoering van het beleid en beheer van de meldkamers. Alles overziend blijkt dat het SMB ten tijde van het onderzoek nog geen risicomanagement heeft ingericht en geborgd om de LMS te sturen op het beveiligen van de meldkamersystemen.

Hoewel op onderdelen van het inrichtingsproces stappen zijn gezet, is de informatieveiligheid van de meldkamersystemen tot nu toe vooral te danken aan de loyale inzet van medewerkers van de LMS. Deze inzet wordt door het SMB nog niet beantwoord met actieve betrokkenheid en aansturing. Illustratief is het groot aantal concepten die het uitgangspunt vormen voor de informatiebeveiliging, maar waarvan onduidelijk is wat het SMB hiervan vindt.

Verstoring door cybercriminaliteit vormt volgens de Nationaal Coördinator Terrorismebestrijding en Veiligheid een toenemende bedreiging. Tegen deze achtergrond is een solide kader voor de aansturing op de informatiebeveiliging van vitaal belang voor de continuïteit van de samenwerkende meldkamers. Aansturing op basis van een zo volledig mogelijke en actuele informatie bepaalt uiteindelijk hoe weerbaar de meldkamersystemen zijn tegen verstoring.

Daarvoor is het van groot belang dat alle partijen van elkaar weten wie waarvoor verantwoordelijk is. Uit het onderzoek kwam echter naar voren dat binnen het ministerie van JenV en de meldkamersamenwerking tegenstrijdige opvattingen leven over de verdeling van de verantwoordelijkheid voor de meldkamersystemen. Voor de LMS is nog onvoldoende duidelijk voor welke risico’s zij verantwoordelijk is en hoe zij deze moet beheersen.

Oordeel

De Inspectie oordeelt dat het SMB nog onvoldoende in staat is om digitale risico’s te signaleren en tot een aanvaardbaar niveau te reduceren. De LMS is hierdoor onvoldoende weerbaar tegen de toenemende dreiging van verstoring. Dit is een risico voor de veiligheid van de meldkamersystemen en daarmee voor de continuïteit van de meldkamers als onderdeel van de vitale infrastructuur van Nederland. Vanwege de ernst van de situatie is een strakke aansturing nodig.

De Inspectie oordeelt ook dat de tegenstrijdige opvattingen van het ministerie van JenV en de meldkamersamenwerking over de verdeling van de verantwoordelijkheid voor de meldkamersystemen een vlotte inrichting en borging van het risicomanagement in de weg staat. Dit verschil van inzicht vormt eveneens een risico voor de veiligheid van de meldkamersystemen en daarmee voor de continuïteit van de meldkamers.

Aanbeveling aan het BMB en het SMB

Het is noodzakelijk dat het BMB en het SMB zich meer committeren aan informatiebeveiliging en prioriteit geven aan het versneld ontwikkelen en toepassen

van risicomanagement op de meldkamersystemen door de risico's te waarborgen met rapportages, audits en door gerichte sturing op de voortgang van het beheer.

Aanbeveling aan de LMS

Het is noodzakelijk dat de LMS de basis van haar uitvoeringsverantwoordelijkheid waarborgt door de informatiebeveiliging uit te voeren op basis van vastgestelde documenten, en door het belang daarvan bij het SMB te benadrukken.

Aanbeveling aan het ministerie van JenV en de LMS

Het is noodzakelijk dat DG Politie en Veiligheidsregio's en de LMS op korte termijn heldere afspraken maken en vastleggen over hoe de verantwoordelijkheden in de uitvoeringspraktijk gestalte krijgen zoals bedoeld in de *Wijzigingswet meldkamers*, de *Regeling hoofdlijnen beleid en beheer meldkamers* (2020) en de *Ministeriële regeling C2000* (concept).

Bijlage I Toetsingskader

De Inspectie heeft voor dit onderzoek gebruikgemaakt van de standaard ISO/IEC 27005, en daarvan de paragrafen 7, 8, 9 en 10 die specifiek gaan over de opzet en toepassing van risicomanagement op de informatiebeveiliging.

Reikwijdte, context en criteria (context establishment)	
Het bepalen van de context (Referentie aan ISO/IEC 27005 parr. 7.1)	De organisatie bepaalt de externe en interne context voor het beheren van informatie-risico's. Hiervoor stelt zij de basiscriteria op, definieert de reikwijdte en de grenzen, en organiseert het uitvoeren van informatierisicomanagement.
Het inrichten en toepassen van informatie risicomanagement (Referentie aan ISO/IEC 27005 parr. 7.2.1)	De organisatie beschrijft hoe zij het proces van risicomanagement heeft ingericht en toepast. Hierin zijn criteria opgenomen voor risico evaluatie, criteria voor impact en criteria voor risico acceptatie. (Zoals bedoeld in 7.2.2, 7.2.3 en 7.2.4)
Het bepalen van criteria voor risico-evaluatie (Referentie aan ISO/IEC 27005 parr. 7.2.2)	De organisatie definieert criteria voor het evalueren van risico's.
Het bepalen van criteria voor gevolgen (Referentie aan ISO/IEC 27005 parr. 7.2.3)	De organisatie definieert criteria voor het bepalen van de gevolgen van incidenten.
Het bepalen van criteria voor acceptatie van risico's (Referentie aan ISO/IEC 27005 parr. 7.2.4)	De organisatie definieert criteria voor het accepteren van risico's.
Het bepalen van de reikwijdte van het informatie risicomanagement (Referentie aan ISO/IEC 27005 parr. 7.3)	De omgeving waarin de organisatie haar taken uitvoert, is geanalyseerd en beschreven. De organisatie brengt alle relevante bedrijfsprocessen en bedrijfsmiddelen in kaart. De uitkomsten van de omgevingsanalyse en de relevante bedrijfsprocessen en bedrijfsmiddelen zijn in de risicobeoordeling meegenomen.
Het vastleggen van de verantwoordelijkheden en het uitvoeren van informatie risicomanagement (Referentie aan ISO/IEC 27005 parr. 7.4)	De organisatie legt de verantwoordelijkheden en de uitvoering van informatie risicomanagement vast. De wijze van uitvoering van het informatie risicomanagement is vastgelegd.

Risicobeoordeling (risk assessment)	
Het beoordelen van de risico's (Referentie aan ISO/IEC 27005 parr. 8.1)	De organisatie identificeert de risico's, beschrijft deze en prioriteert deze ten opzichte van de risico- evaluatie criteria en de doelstellingen die relevant zijn voor de organisatie.
Het identificeren van de informatiemiddelen (assets) (Referentie aan ISO/IEC 27005 parr. 8.2.2)	De organisatie identificeert de bedrijfsmiddelen die relevant zijn voor de reikwijdte van de risicobeoordeling.
Het identificeren van dreigingen (Referentie aan ISO/IEC 27005 parr. 8.2.3)	De organisatie identificeert de relevante dreigingen en de bronnen voor deze dreigingen.
Het identificeren van de bestaande maatregelen (Referentie aan ISO/IEC 27005 parr. 8.2.4)	De organisatie identificeert de relevante bestaande en geplande maatregelen.
Het identificeren van de kwetsbaarheden (Referentie aan ISO/IEC 27005 parr. 8.2.5)	De organisatie identificeert de kwetsbaarheden die geëxploiteerd kunnen worden door de geïdentificeerde dreigingen en die kunnen leiden tot schade aan de geïdentificeerde bedrijfsmiddelen.
Het identificeren van de gevolgen (Referentie aan ISO/IEC 27005 parr. 8.2.6)	De organisatie identificeert de gevolgen van het aantasten van de beschikbaarheid, integriteit en de vertrouwelijkheid van haar bedrijfsmiddelen en informatie.
Het bepalen van de gevolgen (Referentie aan ISO/IEC 27005 parr. 8.3.2)	De organisatie bepaalt de gevolgen voor haar bedrijfsvoering van een mogelijk of daadwerkelijk beveiligingsincident. Zij houdt daarbij rekening met de gevolgen van het doorbreken van haar informatiebeveiliging zoals het aantasten van de beschikbaarheid, integriteit en vertrouwelijkheid van haar bedrijfsmiddelen.
Het bepalen van de kansen op een incident (Referentie aan ISO/IEC 27005 parr. 8.3.3)	De organisatie bepaalt de kans op optreden van de incidenten.
Het bepalen van het risiconiveau (Referentie aan ISO/IEC 27005 parr. 8.3.4)	De organisatie bepaalt het risico voor elk van de relevante incidenten.
Het evalueren van de risico's (Referentie aan ISO/IEC 27005 parr. 8.4)	De organisatie vergelijkt de risico's met de criteria voor het evalueren en accepteren van risico's.

Risicobehandeling en risico-acceptatie (risk treatment en risk acceptance)	
(Referentie aan ISO/IEC 27005 parr. 9)	De organisatie kiest maatregelen voor risicobeperking en stelt dit vast.
(Referentie aan ISO/IEC 27005 parr. 10)	De organisatie beschrijft aan de hand van de risicocriteria welke restrisico's de organisatie aanvaardt. De directie heeft goedkeuring verleend aan de overblijvende risico's.

Risicomanagement volgens ISO/IEC 27005

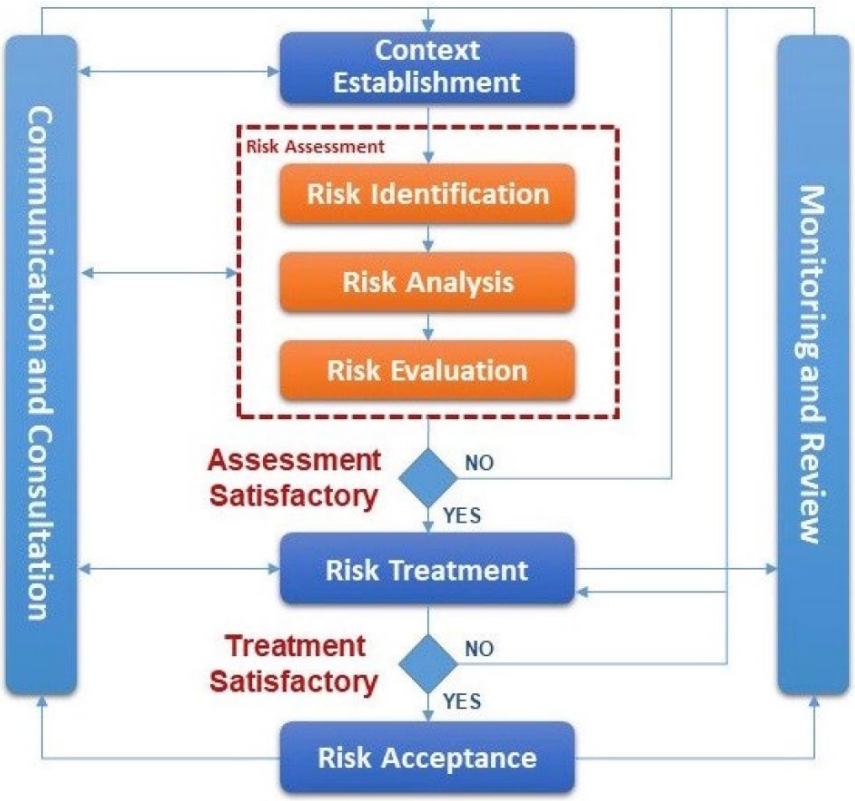
ISO /IEC 27005 biedt de standaardrichtlijnen voor het inrichten van informatie risicomanagement. Deze werkt de planfase uit zoals bedoeld in de onderstaande afbeelding:

- Het bepalen van de reikwijdte, context en criteria voor het risicomanagement (context establishment)
- Het beoordelen van de risico's (risk assessment)
- Het treffen van risicobeperkende maatregelen (risk treatment)
- en het accepten van de rest-risico's (risk acceptance).

Deze handelingen vormen de kern van het inrichten van risicomanagement. De andere activiteiten voor monitoren en evalueren en communiceren, blijven echter in dit onderzoek buiten beschouwing.

Het bepalen van de reikwijdte, context en criteria voor het risicomanagement is het feitelijke opzetten van het raamwerk voor risicomanagement. De beoordeling van risico's is onderverdeeld in drie deelactiviteiten: risico-identificatie, risicoanalyse en risico-evaluatie.

Het eerste onderdeel, risico-identificatie, gaat over het in kaart brengen van de relevante risico's. De omvang van de geïdentificeerde risico's worden vervolgens tijdens de tweede stap, de risicoanalyse, geschat. De derde stap richt zich op het vergelijken van de omvang van de geïdentificeerde risico's met de van tevoren bepaalde risico criteria. Tijdens deze stap wordt bepaald of het risico acceptabel is. Als het risico niet acceptabel is, zal in de volgende activiteit van risicobehandeling bepaald gaan worden op welke wijze het risico zal worden afgehandeld. Voorbeelden van afhandeling zijn daarbij het risico mijden, het risico overdragen of maatregelen nemen om de omvang van het risico te verkleinen. Bij de laatste stap wordt vastgelegd welke overblijvende risico's worden aanvaard.



Afbeelding: Weergave van de uitgangspunten voor het procesgericht beheer van risico's in de informatiebeveiliging volgens ISO/IEC 27005.

Bijlage II: Aansturing van de LMS

De Landelijke meldkamersamenwerking wordt bestuurd door vertegenwoordigers van de ministeries van Justitie en Veiligheid en Volksgezondheid, Welzijn en Sport, de veiligheidsregio's[36], Ambulancezorg Nederland, Koninklijke Marechaussee en de Nationale Politie. De vertegenwoordigers komen regelmatig in verschillende samenstellingen bijeen voor overleg en afstemming. Zo kunnen zij de kwaliteit van de meldkamers behouden en waar nodig verbeteren. Deze multidisciplinaire sturing bestaat formeel uit twee overleggen op landelijk niveau, te weten het Bestuurlijk Meldkamer Beraad en het Strategisch Meldkamer Beraad. Dit is bepaald in artikel 3 en 4 van de *Regeling hoofdlijnen beleid en beheer meldkamers*.

- Het Bestuurlijk Meldkamer Beraad (BMB) is door de minister van JenV ingesteld voor de landelijke sturing op beleid en beheer van de meldkamers[37]. Het Bestuurlijk Meldkamer Beraad fungeert als bestuurlijk escalatieniveau voor het Strategisch Meldkamer Beraad en stelt jaarlijks een concept van het beleids- en bestedingsplan vast en adviseert de Minister van Justitie en Veiligheid over de vaststelling daarvan.

  Het Bestuurlijk Meldkamer Beraad monitort de werking van het beleid en beheer van de meldkamers en beslist over voorstellen van het Strategisch Meldkamer Beraad die binnen het vastgestelde beleids- en bestedingsplan bestuurlijke borging behoeven.

  Een vertegenwoordiger van de Minister van Justitie en Veiligheid is voorzitter van het Bestuurlijke Meldkamer Beraad. De voorzitter van het Strategisch Meldkamer Beraad kan de vergadering van het Bestuurlijk Meldkamer Beraad bijwonen.

- Het Strategische meldkamerberaad (SMB) vervult een centrale rol in landelijke strategische sturing op het beleid en beheer van de meldkamers[38]. Het SMB verzamelt de inbreng voor het beleids- en bestedingsplan; draagt zorg voor het opstellen daarvan en voor de jaarverantwoording op landelijk niveau. Het beslist binnen de kaders van het beleids- en bestedingsplan over de uitvoering van beleid en beheer; bewaakt de uitvoering van het beleids- en bestedingsplan; en doet voorstellen voor de agenda van het Bestuurlijk Meldkamer Beraad.

  Het SMB adviseert het Bestuurlijk Meldkamer Beraad en kan hulpstructuren instellen die bijdragen aan het realiseren van de vastgestelde kaders voor beleid en beheer. Het Discipline Overleg is een van die hulpstructuren die het SMB adviseert. Dit is een landelijk overleg met vertegenwoordigers van de vier hulpdiensten ('disciplines'), de LMS en het ministerie van JenV. Het Overleg Hoofden Meldkamers is een andere hulpstructuur dat is ingesteld voor de verbinding tussen lokaal, regionaal en landelijk beleid. De hoofden

[36] De brandweer is onderdeel van de veiligheidsregio's.
[37] Het BMB is ingesteld bij art.3 *Regeling hoofdlijnen beleid en beheer meldkamers*.
[38] Het SMB is ingesteld bij art.4 *Regeling hoofdlijnen beleid en beheer meldkamers.*

van de meldkamers formuleren de behoeften voor het beleid en beheer, zodat de meldkamers elkaars werkzaamheden kunnen overnemen.

De korpschef van de Nationale Politie is bestuurlijk verantwoordelijk voor het beheer van de meldkamers[39].

Het ministerie van JenV, de regioburgemeesters, de voorzitter van het college van procureurs-generaal, en de korpschef, voeren ten minste viermaal per jaar overleg over de taakuitvoering en het beheer ten aanzien van de politie. Hierbij gaat het ondermeer om: de inrichting van de politie, het beleid en bestedingsplan, en eventuele wetsvoorstellen en regelingen die betrekking hebben op de taakuitvoering en het beheer ten aanzien van de politie. Dit is de beheertaak.

De korpschef is vertegenwoordigd in het BMB en in het SMB. Daarnaast is de Korpschef ook gebruiker van meldkamersystemen en leverancier van ICT-diensten middels het Meldkamerdienstencentrum (MDC).

[39] Zoals bedoeld in art. 19 lid 1 en 3 onder d en art. 23 a lid 3 Politiewet

Bijlage III: Geraadpleegde bronnen

Geïnterviewde personen

De directeur LMS, heeft zitting in het Strategisch meldkamerberaad, voorzitter Disciplineoverleg, voorzitter van het Overleg hoofden meldkamers en is Chief information officer LMS.

De plv. directeur en hoofd Beleidsondersteuning LMS. Heeft zitting in het Strategisch meldkamerberaad.

De Coördinator vraagarticulatie meldkamervoorzieningen, voorzitter Werkgroep Informatiebeveiliging Meldkamers.

Het Sectorhoofd Meldkamerdienstencentrum, Nationale politie.

De Coördinator Integrale Beveiliging bij het Meldkamerdienstencentrum, Nationale politie.

De Stafmedewerker LMS, continuïteit en risicomanagement, contactpersoon voor de Inspectie JenV.

De Beleidsadviseur LMS, contactpersoon voor de Inspectie JenV.

De Manager voor het project Verbetering Informatiebeveiliging.

De Information securitymanager en Kwartiermaker Informatiebeveiligingsorganisatie van de Nationale Politie. Lid werkgroep cybersecurity.

De Verantwoordelijke informatiebeveiligingsbeleid en bewustwording, sector informatiebeveiliging Nationale Politie.

Het Hoofd van de Meldkamer Oost Nederland en regionale kwartiermaker meldkamersamenvoeging voor oost-Nederland, lid van het Overleg van hoofden meldkamers en voorzitter van de landelijke Commissie gegevensverwerking Meldkamers.

Een lid van Kwartiermakers bedrijfsvoering en Kwartiermaker bedrijfsvoering van de meldkamer Den Haag.

Een sr. beleidsmedewerker cybersecurity en informatiebeveiligingsbeleid voor het programma Meldkamer bij het DG Politie en Veiligheidsregio’s ministerie JenV.

De Coördinerend beleidsmedewerker Programma Meldkamer, Crisiscommunicatie en Alerteren, DG Politie en veiligheidsregios, ministerie van JenV.

Een consultant informatiebeveiliging bij DG Politie en veiligheidsregios, ministerie van JenV.

Geraadpleegde documenten

Analyse voorgestelde beveiligingsmaatregelen C2000 (Deloitte 2019)

Applicatie portfolio management. Legenda applicatieoverzicht (LMS 29-1- 2020)

Applicatieoverzicht entiteiten, versie 14 (LMS)

Beleids- en bestedingsplan Meldkamers 2021, versie 30 september 2020 (LMS 2020)

Beveiligingsplan Dienst 1-1-2, versie 7.0 (KPN 2019)

Beveiligingsrapport GMS-RTIC Mobiel, versie 1.2 (2019)

Bouwplan LMS, concept 0.5 (LMS 2021)

Bouwtekening LMS, concept 0.7 (LMS)

Continuïteit van meldkamers (Inspectie Justitie en Veiligheid en Agentschap Telecom 2019)

Cybersecuritybeeld Nederland 2020 en Cybersecuritybeeld Nederland 2021, (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020 en 2021)

Cyberprogramma, 20 mei 2020 en 22 maart 2021 (LMS)

Follow-up Development Status C2000 - Eurofunk - final report (Xebia 2018)

Jaaraanschrijving Politie 2021-2022, Concept, def. (Ministerie van JenV 2020)

Maandelijkse rapportage aanbevelingen analyses Cyberprogramma, 20 mei 2020 en 22 maart 2021 (LMS)

Meldkamer Drachten. Cybersecurity analyse, versie 1.0 (Nationale Politie 2019)

Meldkamers (Inspectie Justitie en Veiligheid en Agentschap Telecom 2015);

Memo Quickscan, versie 2.3 (LMS)

Notitie SvZ informatiebeveiligings-beleid, concept 5 juli 2021. (LMS 2021) document in wording

Notitie Verbeterplan LMS IV/ICT-infrastructuur, versie Hoofd Staf LMS 19 oktober 2020 (Triple A 2020)

Onderzoek C2000. Managementrapport, versie 1.0 (Fox-IT 2019)

Opvolging aanbevelingen onderzoek continuïteit meldkamers. Brief van de Inspecteur-generaal Justitie en Veiligheid aan de korpsleiding van de Nationale Politie en aan de voorzitter van het Bestuurlijk Meldkamerberaad, 1 juli 2021.

Overzicht business applicaties en koppelingen per voorziening en thema. (LMS 29-1- 2020)

Patching Procedure HHS LMS, concept 1.10 (LMS 2021)

Penetratietest C2000, versie 1.0 (Fox-IT 2019)

Pentest rapport Stas C2000, versie 1.0 (Strict 2019)

Plan van aanpak. Continuïteit meldkamers en meldkamer-processen tijdens Covid-19 crisis, versie 7-4-2020 (LMS 2020)

Procesbeschrijving Change management, concept 1.7 (Nationale Politie 2017)

Procesbeschrijving Configuration and Asset Management, concept 1.x (Nationale Politie 2017)

Procesbeschrijving Incident management, concept 0.2 (Nationale Politie 2017)

Procesbeschrijving Problem management, concept 1.1 (Nationale Politie 2017)

Procesbeschrijving Release & Deployment Management, concept 1.9 (Nationale Politie 2017)

Procesvoorstel Beleidskader voor Informatie-beveiligingsbeleid voor multi-meldkamervoorzieningen. (LMS 2020)

Quickscans en Security scans meldkamers (Deloitte 2019-2020) 16 rapportages

Rapportage hertest C2000, versie 1.0 (Fox-IT 2019)

Rapportage LMS. Technische architectuur. Vooronderzoek, versie 1.0 (KPMG 2020)

Resultaten Risicoanalyse C2000, versie 1.0 (Nationale Politie, QSight IT 2017)

Risico Analyse Manual Master, versie 1.0 (Nationale Politie, Kwartier Informatiebeveiliging 2020)

Risicoanalyse 112, concept 0.1 (LM0 2017)

Risicoanalyse C2000 (QsightIT 2017) status onbekend

Risicoanalyse GMS, concept 0.2 (LMO 2017)

Risicoanalyse meldkamer Den Haag. spreadsheetversie 19-9-2020

Risicoanalyse NL-Alert, concept 0.1 (LMO 2018)

Transitieakkoord meldkamer van de toekomst

Uitwerking risicoanalyse, versie 1.0 (Nationale Politie Meldkamerdienstencentrum 2018-2021)

Veranderingen maken ook kwetsbaarder. Rapport risicoanalyse Geïntegreerd Meldkamer Systeem (GMS), versie 1.0 (Ministerie van JenV 2017)

Verbeteren Informatiebeveiliging LMS en Meldkamers, Fase eindrapport-Fase 3, versie 0.4 (LMS 2020)

Verbeteren Informatiebeveiliging LMS en Meldkamers. Faseplan Fase 4, versie 0.3 (LMS 2021)

Verbetering Informatiebeveiliging LMS en MKs, concept 1.0 (LMS 2020)

Bijlage IV: Gebruikte afkortingen

BIO: de *Baseline Informatiebeveiliging Overheid*, de richtlijn voor de informatiebeveiliging voor Nederlandse overheidsinstellingen.

C2000: een gesloten communicatienetwerk voor de hulpverleningsdiensten, maakt deel uit de vitale infrastructuur.

DG Politie en Veiligheidsregio's: het Directoraat-Generaal Politie en Veiligheidsregio's van het ministerie van Justitie en Veiligheid.

GMS: het Geïntegreerd Meldkamersysteem, een softwarepakket dat is ontwikkeld om te werken met het communicatiesysteem C2000. Wordt vervangen door een nieuw nationaal meldkamersysteem (NMS).

ICT: informatie- en communicatietechnologie.

ISO/IEC 27001, 27002 en 27005: internationale standaard van de International Organization for Standardization(ISO) en de International Electrotechnical Commission (IEC).

LMS: Landelijke Meldkamersamenwerking

Minister JenV: de minister van Justitie en Veiligheid.

MKs: meldkamers

PDCA-cyclus: Deze cyclus geeft het principe weer van continue verbetering volgens W.E. Deming en wordt gevormd door de facetten Plan-Do-Check-Act.

SMB: het Strategisch Meldkamerberaad van de Landelijke Meldkamersamenwerking.

Inspectie Justitie en Veiligheid
Toezicht, omdat rechtvaardigheid en veiligheid niet vanzelfsprekend zijn.

Dit is een uitgave van:
Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP Den Haag
Postbus 20301 | 2500 EH Den Haag
Contactformulier | www.inspectie-jenv.nl

Januari 2022