Ministerie van Defensie

Jaarverslag 2024

Beveiligingsautoriteit

Colofon

Beveiligingsautoriteit

Adres
Kalvermarkt 32
Postbus 20701
2511 CB 's-Gravenhage

Postadres
2500 ES 's-Gravenhage
MPC 58B

Opstellers
Sectie Toezicht van de Beveiligingsautoriteit

Datum
Maart 2025

Voorwoord

Met genoegen presenteren wij ons toezichtjaarverslag 2024. Dit jaarverslag beschrijft een transitiefase, want de Beveiligingsautoriteit (BA) gaat stapsgewijs van traditioneel toezicht (voornamelijk normatief toezicht) naar een aanpak waarbij parallel systeemgericht toezicht en beveiligingstesten worden ingezet. Dit leidt uiteraard ook tot wijzigingen in de opzet van de jaarverslagen. In dit jaarverslag worden deze wijzigingen toegelicht.

De BA wil van de traditionele toegangsmethodieken het positieve behouden en tegelijk verrijken met systeemgericht toezicht, waarbij data en kwaliteitsmanagementsystemen een grotere rol gaan spelen. Dit verbetert de kwaliteitscirkel (*Plan-Do-Check-Act*-cyclus, kortweg PDCA-cyclus), wat weer leidt tot een versterking van het zelflerend vermogen van Defensie op het gebied van integrale beveiliging.

Toezicht is in ontwikkeling, ook met het oog op de wendbaarheid die nodig is bij hoofdtaak 1. Waar het toezicht zich eerder alleen concentreerde op het beoordelen van de naleving van normen en eisen, wordt er nu ook meer ingezet op systeemgericht toezicht en beveiligingstesten. Door de toevoeging van deze toezichtmethodieken kijken we met meer detail naar de gehele werking van de integrale beveiliging. We kijken ook naar de opzet, het bestaan en de effectiviteit van het kwaliteitsmanagementsysteem. We zoeken naar antwoord op vragen als: In hoeverre is het kwaliteitsmanagementsysteem 'volwassen'? Wordt er geleerd van gemaakte fouten? Bestaat er een cultuur waarin leren en verbeteren centraal staan? Op basis van de antwoorden op deze vragen kunnen we er een oordeel vormen over de kwaliteit van de beveiliging.

Het doel van de BA is om in de toekomst meer te kijken naar de mate waarin Defensie in het beveiligingsdomein *in control* is. Waar traditioneel toezicht zich met name richt op naleving, stelt de combinatie met systeemgericht toezicht ons in staat om de PDCA-cyclus te toetsen en te bezien of er binnen Defensie continu en actief naar verbetering wordt gezocht. Beveiliging is immers van cruciaal belang bij het waarborgen van de continuïteit en betrouwbaarheid van de bedrijfsprocessen. Hiervoor dienen niet alleen de betreffende onderdelen intern goed samen te werken, maar dient vanuit toezicht ook te worden gekeken naar de manieren waarop onderdelen samenwerken en van elkaar leren. Zo beveiligen we onze Te Beschermen Belangen (TBB's) optimaal. Dat is in ons aller belang.

De Beveiligingsautoriteit,
voor deze,
het afdelingshoofd Beveiliging en Gegevensbescherming

Kolonel H.J. Schuthof, MSc, EMSD, MA

Inhoud

1 De Beveiligings-autoriteit

Binnen het Ministerie van Defensie houdt de BA toezicht op de integrale beveiliging. De toezichthoudende taak van de BA betreft in het algemeen het toezicht houden op de naleving van het Defensie Beveiligingsbeleid (DBB) bij alle defensieonderdelen.

Daarnaast voert de BA de *National Security Authority*-rol uit voor het militaire domein (NSA-MoD) en de *Security Accreditation Authority* (SAA). Deze rol vloeit voort uit het NATO-beleid. Vanuit deze rol houdt de BA toezicht op basis van het beveiligingskader uit het NATO- en EU-beleid, of op basis van afspraken die voortvloeien uit bi- en multilaterale verdragen (bijvoorbeeld *Special Access Programs* (SAP's)). Tot slot houdt de BA toezicht op de naleving van het toetsingskader Beveiligingsnormen Inlichtingen & Veiligheidsdiensten (BNIVD) als het toezicht op de inlichtingendiensten betreft.

1.1 Defensie Beveiligingsbeleid

Het DBB bevat het geheel aan beveiligingsnormen en bestaat uit verschillende deelgebieden:
- algemene beveiliging;
- fysieke beveiliging;
- personele beveiliging;
- informatiebeveiliging (inclusief beveiligingsmaatregelen tegen compromitterende emissies en cryptografische normen);
- *special access programs;*
- industriebeveiliging.

Dit beleid dient als basis en fundament voor de taak van de BA als toezichthouder. Ook controleert de BA periodiek het bestaan, de opzet en de werking van het beleid. Waar nodig herziet de BA het DBB met betrekking tot de correctheid en actualiteit van het DBB ten opzichte van veranderingen in NATO-, EU-, en VS-normeringen.

1.2 Verantwoordelijkheid voor integrale beveiliging

Op basis van de aanwijzing SG-A948 is de BA namens de Secretaris-Generaal (SG) verantwoordelijk voor het opstellen van het beveiligingsbeleid en het toezicht houden op de uitvoering daarvan. De BA is lid van het Toezichtberaad Defensie en heeft zodoende ook een richtende positie. De Commandant der Strijdkrachten (CDS) is verantwoordelijk voor de aansturing en coördinatie; een inrichtende positie. Tot slot is de commandant (hieronder valt ook het hoofd van dienst, de lijnmanager, enzovoorts) verantwoordelijk voor de integrale uitvoering bij zijn organisatie-eenheid binnen de kaders van het DBB; een verrichtende positie.
De toezichttaak is op basis van een decentraal concept ingericht en belegd binnen de gehele functionele beveiligingsketen. De BA is daarbij in haar rol als toezichthouder formeel benoemd tot interne toezichthouder. Defensieonderdelen zien zelf ook intern toe op de toepassing en de naleving van het DBB.

1.3 Toezicht op overige normenkaders

Inlichtingendiensten

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) hanteren een additioneel beveiligingsnormenkader (BNIVD). Zowel de beveiligingsambtenaar van de MIVD en de AIVD, als van de BA Defensie, houden toezicht op de naleving op dit normenkader.

F-35

Naast het nationale beleid conformeert Defensie zich met het F-35 *Air System* aan richtlijnen van de Amerikaanse overheid. De BA houdt in haar rol als *Program Security Officer* (PSO) normatief toezicht op alle *Special Access Program Facilities* (SAPF's) die onder Nederlandse verantwoordelijkheid vallen.
Hieronder vallen zowel gerealiseerde als in aanbouw zijnde SAPF-locaties in Nederland en in de Verenigde Staten. In haar rol als PSO houdt de BA het toezicht.
De Amerikaanse PSO kan tevens aangekondigd of onaangekondigd toezicht uitvoeren op de Nederlandse SAPF's. Het nationale toezicht vindt jaarlijks plaats.

Overig

Organisaties als de Auditdienst Rijk, de Algemene Rekenkamer (AR), de NATO en de EU zijn externe toezichthouders. Deze toezichthouders houden systeemgericht toezicht en normatief toezicht.
De BA begeleidt hierbij en bereidt toezicht, onderzoeken en/of inspecties voor.

1.4 Methoden van toezicht

Met systeemgericht toezicht bekijkt de BA de opzet, het bestaan en het effect van de processen en beheersingsmaatregelen die noodzakelijk zijn voor een defensieonderdeel om te garanderen dat aan het DBB wordt voldaan. Bij deze vorm van toezicht staat de mate van borging van de PDCA-cyclus centraal.

Bij normatief toezicht kijkt de toezichthouder naar de geïmplementeerde beveiligingsmaatregelen en beoordeelt of aan de beveiligingsnormen is voldaan. Normatief toezicht kan onder andere gericht zijn op TBB's, fysieke en elektronische informatie, IT-voorzieningen en fysieke locaties. Toezicht kan ook gericht zijn op samengestelde en complexe belangen, zoals een informatie- of wapensysteem. Naast het toezien op de naleving omvat het toezicht tevens:

- vervolgtoezicht, waarbij veranderingen en verbeteringen worden gemonitord;
- signaalgestuurd toezicht, om snel te reageren op onverwachte gebeurtenissen;
- thematisch toezicht, waarbij de nadruk ligt op specifieke relevante thema's.

Deze diverse benaderingen versterken de toezichtinspanningen en dragen bij aan de effectiviteit en kwaliteit van het toezicht.

Met beveiligingstesten evalueert de BA de kwaliteit en effectiviteit van operationele en tactische beveiligingsmaatregelen. Via fysieke/integrale penetratietesten, ook bekend als *redteaming*, worden kwetsbaarheden geïdentificeerd.

1.5 Samenwerking

Om de samenhang en de kwaliteit van toezicht te verbeteren, werken de interne toezichthouders bij Defensie samen. De interne toezichthouders zijn de BA, de Functionaris voor Gegevensbescherming (FG), de Inspectie Militaire Gezondheidszorg (IMG), de Inspectie Veiligheid Defensie (IVD), het Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS) en de Militaire Luchtvaart Autoriteit (MLA). Zij zoeken de samenwerking op verschillende onderdelen, zoals de afstemming van toezichtagenda's. Ook versterken zij gezamenlijk het toezichtproces op het gebied van methodologie en redactie. In 2024 voerde de BA toezichtactiviteiten uit in samenwerking met de FG en het KMCGS.

Toezichtberaad

In 2020 verenigden de interne toezichthouders zich in het Toezichtberaad Defensie met als doel de kwaliteit te verbeteren en de samenhang en effectiviteit van het interne toezicht te versterken. Het Toezichtberaad wordt ondersteund door het Bureau Toezicht Defensie (BTD). De Inspecteur-Generaal der Krijgsmacht (IGK) en een vertegenwoordiger van het Bureau Secretaris-Generaal (Bureau SG) nemen als toehoorder deel aan het beraad. De IGK is geen toezichthouder, maar zijn onderzoeken verrijken wel het inzicht in de staat en het functioneren van de defensieorganisatie. De Inspecteur-Generaal Veiligheid is als coördinerend toezichthouder voorzitter van het beraad.

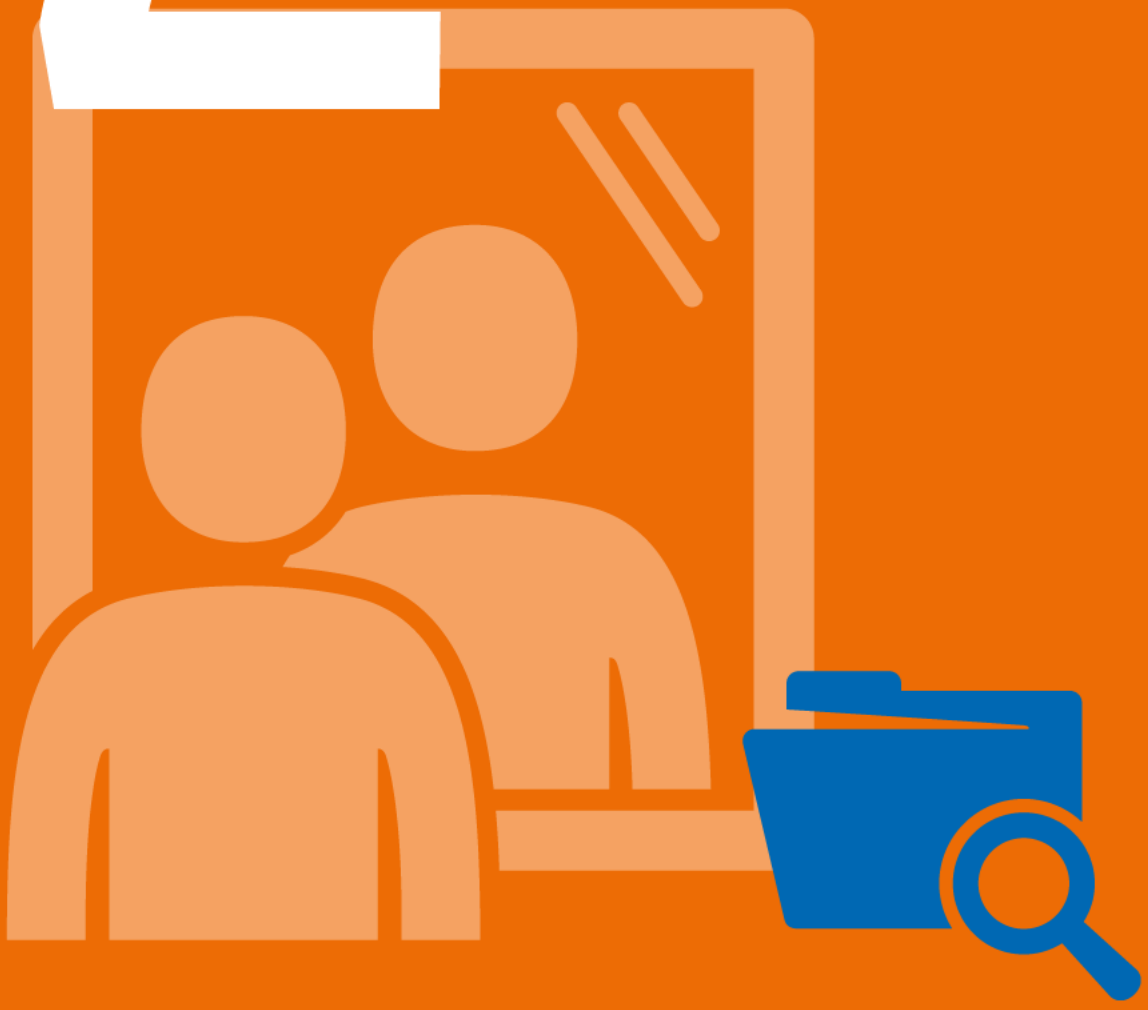
Functionaris voor Gegevensbescherming

De aandacht voor de beveiliging van persoonsgegevens is in sterke mate toegenomen vanwege maatschappelijke ontwikkelingen en de inwerkingtreding van de Algemene verordening gegevensbescherming. De BA en de FG werken incidenteel samen aan toezichtactiviteiten.

Korps Militaire Controleurs Gevaarlijke Stoffen

Het KMCGS en de BA hebben een gemeenschappelijk toezichtgebied: de opslag en het vervoer van munitie, explosieven en springmiddelen. De gehanteerde normering is voor beide toezichthouders wel verschillend. Het KMCGS vervult voor de BA een 'oog- en oorfunctie' voor de naleving van de DBB-normering.

2 Beoordelings-systeem



2.1 Openbaarheid gegevens versus bescherming defensiegegevens

De BA rapporteert op verschillende wijzen. Ze rapporteert zowel over de feitelijke toezichtresultaten als in een jaarlijks geaggregeerd beeld. Dat laatste wordt op twee manieren gedaan. Ten eerste rapporteert de BA separaat aan de verschillende defensieonderdelen over beveiliging binnen Defensie. Deze rapportages zijn, afhankelijk van het onderwerp, vertrouwelijk of confidentieel. Daarnaast stelt de BA een openbaar jaarverslag op, waarmee ze tegemoet komt aan de wens van transparantie over de mate waarin Defensie wat betreft beveiliging *in control* is en over de aangewende middelen. Uiteraard worden eventuele specifieke kwetsbaarheden en verbeterplannen ten aanzien van specifieke locaties of risico's niet prijsgegeven. Zo rapporteert de BA op algemene wijze over de mate waarin geluidsdichte werkruimtes bij Defensie voldoen aan de normen. Daarbij blijven specifieke getallen of locaties intern en confidentieel.

Gerubriceerde informatie

In de opvolging van een toezichtbezoek ontvangen de verantwoordelijke defensieonderdelen en medewerkers alle relevante informatie, zoals de geïdentificeerde kwetsbaarheden met bijbehorende aanbevelingen.

Waardering in sterren

De BA hanteert de komende twee jaar een sterrensysteem, waarin de kwaliteit van de PDCA-cyclus van een onderdeel wordt geduid:

BA-sterrensysteem

Aantal sterren	Kwaliteitsduiding
*	Zeer slecht
**	Slecht
***	Onvoldoende
****	Voldoende
*****	Goed

3 Hoofdlijnen uit het toezicht

Het jaarverslag geeft een overzicht van de belangrijkste bevindingen gebaseerd op de resultaten van het toezichtjaar 2024.

3.1 Beveiliging algemeen

Binnen Defensie zijn alle processen rondom integrale beveiliging ingericht op basis van de PDCA-cyclus. Echter wordt op basis van de toezichtresultaten de effectieve werking hiervan als onvoldoende beoordeeld. Dit is vooral geconstateerd op de CHECK- en ACT-fases, waarbij randvoorwaarden erg relevant zijn. Het gaat dan om randvoorwaarden zoals capaciteit, kwaliteit van de functionele beveiligingsketen, maar ook het beveiligingsbewustzijn van verantwoordelijke commandanten en medewerkers. De toezichthouder ziet dat onder aansturing van de CDS een project is gestart voor de verbetering van beveiliging van militaire objecten. Dit zou onder andere onvolkomenheden op dit vlak, zoals vastgesteld door de AR, moeten adresseren. Het is nog te vroeg om hier een kwalificerende uitspraak over te doen, waardoor dit zich nog niet heeft vertaald in een ander oordeel door de BA.

Het is belangrijk op te merken dat de personele uitbreiding die in 2024 was voorzien ter versterking van de toezichtcapaciteit bij de BA, nog niet volledig is gerealiseerd. Met de beperkte toezichtcapaciteit volgde de BA op de hoofdonderwerpen wel het toezichtjaarplan, maar zijn niet alle geplande toezichtonderwerpen aan bod gekomen. Zo zijn bijvoorbeeld de geplande gezamenlijke toezichtbezoeken met de FG verplaatst

Aantal sterren	
***	De effectieve werking van de PDCA-cyclus, met nadruk op de CHECK-fase en ACT-fase, wordt beoordeeld als onvoldoende.

Aanbeveling 1
De toezichthouder beveelt de CDS en de functionele beveiligingsorganisatie aan om specifieke aandacht te besteden aan de CHECK- en ACT-fases van de PDCA-cyclus. Het is van belang om gerichte verbeteringen door te voeren om de organisatievolwassenheid te verhogen. De verbeteringen zijn gerelateerd aan capaciteit, kwaliteit en beveiligingsbewustzijn van medewerkers, eigenaren van TBB's en/of informatie en aan commandanten.

Aanbeveling 2
De toezichthouder beveelt de CDS aan prioriteit te geven aan de plannen voor verbetering van beveiliging van militaire objecten en het plan van aanpak *Crypto*.

3.2 NATO- en *Special Acces Program Facilities*

De BA voert inspecties uit op de registratie van specifieke NATO-documentatie en houdt toezicht op alle SAPF's.

Aantal sterren	
***	De personele bezetting is ontoereikend om aan alle gestelde normen te kunnen voldoen binnen de SAPF.
****	De toezichthouder beoordeelt de mate waarin de organisatie in control is voor wat betreft NATO-inspecties en toezicht op alle SAPF's, als goed. Vanwege rubricering is er geen verdere informatie beschikbaar.

Aanbeveling 1
De toezichthouder beveelt de CDS en de functionele beveiligingsorganisatie aan om specifiek aandacht te besteden aan uitbreiding van de personele capaciteit binnen alle SAPF's. Tevens dient de DAOG personele capaciteit in te regelen voor de exploitatie van de nieuw te bouwen SAPF in Den Haag.

3.3 Crypto

Hoewel het onderwerp crypto geen verplicht onderdeel is van het managementsysteem ten behoeve van integrale beveiliging, is het essentieel genoeg om te vermelden in dit jaarverslag vanwege de overlappende verantwoordelijkheden op het gebied van richtinggevend en inrichtend beleid. De BA is verantwoordelijk voor het richtinggevende beleid, maar is ook al jarenlang betrokken op inrichtend niveau. De BA zal zich, overeenkomstig het besturingsmodel Defensie, in de toekomst meer richten op de richtende positie. Vanwege de betrokkenheid van de BA op zowel richtend als inrichtend niveau en het holistisch beeld dat hierdoor is ontstaan, wordt hieronder de status van de logistieke processen en beleidsprocessen beschreven.

Aantal sterren	
***	In de processen wordt tijdens crypto-*audits* vastgesteld dat met name de ACT-fase verbetering behoeft. De opvolging van aanbevelingen uit controles en monitoring krijgt onvoldoende aandacht, wat het zelflerende vermogen van het managementsysteem belemmert. Dit is een overblijfsel van onvolkomenheid in 2023 en wordt verbeterd naar aanleiding van interne of externe rapportages. In bestaan en werking wordt het proces daarom beoordeeld als onvoldoende.
****	De processen voor uitgifte, beheer en inname van cryptomiddelen en -sleutels zijn ingericht op basis van de PDCA-cyclus. Deze processen worden in opzet beoordeeld als voldoende.

3.4 Beoordeelde onderdelen van het kwaliteitsmanagementsysteem

Voor informatiesystemen en koppelingen geldt dat hiertoe genestelde PDCA-cycli aanwezig zijn in verschillende processen. Dit betekent dat op verschillende niveaus binnen de organisatie specifieke PDCA-processen bestaan, elk gericht op de continue verbetering en evaluatie van integrale beveiliging ten behoeve van informatiesystemen en koppelingen.
In dit toezichtjaarverslag wordt alleen de opzet, het bestaan en de werking beoordeeld, gerelateerd aan de kritieke informatiesystemen.

Fysieke beveiliging - beveiligingsplannen

Voor elke defensielocatie dient een actueel beveiligingsplan aanwezig te zijn. Dit is een onderdeel van het kwaliteitsmanagementsysteem. In een beveiligingsplan staat beschreven hoe de beveiliging van de locatie en de beveiliging van de lokale TBB's georganiseerd is, met inbegrip van beveiligingsrisico's en mitigerende maatregelen.

Aantal sterren	
***	De status van de beoordeelde beveiligingsplannen laat zien dat, hoewel de processen volgens de PDCA-cyclus zijn opgezet, de plannen in de praktijk niet altijd actueel zijn of precies overeenkomen met de werkelijkheid. Hieruit blijkt dat gerichte inspanningen nodig zijn om de actualiteit en nauwkeurigheid van de beveiligingsplannen te verbeteren. Hoewel dit onderdeel is van het plan van aanpak tot verbetering van de beveiliging van militaire objecten, is het te vroeg om op dit punt de waardering te herzien.

Incidentbeheersing

De BA kan alle gemelde beveiligingsincidenten inzien en voert hierop analyses uit.

Aantal sterren	
****	Eerder oordeelde de BA het onderdeel incidentbeheersing als voldoende. Incidenten worden conform een proces gronding beoordeeld, kunnen dienen als basis voor verbeteracties en vormen een signaalfunctie voor het interne toezicht. De BA oordeelt dat de organisatie op dit onderdeel voldoende *in control* is.

Risicobeheersing

Afhankelijk van het classificatieniveau worden de restrisico's aan de BA voorgelegd. Hierdoor heeft de BA zicht op geaccepteerde restrisico's van de hogere TBB's en kunnen deze worden bewaakt. Voor informatiesystemen geldt dat risicobeheersing geborgd is in het accreditatieproces.

Aantal sterren	
**	Net als bij het onderdeel incidentbeheersing zijn de processen voor risicobeheersing ingericht op basis van de PDCA-cyclus. De BA dient te worden geïnformeerd over restrisico's op de hogere TBB's. Het aantal bij de BA gemelde beveiligingsrisico's is in 2024 ongeveer gelijk gebleven ten opzichte van 2023. Daarbij merkt de BA wederom op dat tijdens toezicht beveiligingsrisico's zijn ontdekt die niet eerder door de organisatie zijn geïdentificeerd en behandeld volgens het beleid. Dit betreft risico's van toepassing op alle TBB-classificaties. Op dit onderdeel is de organisatie onvoldoende *in control*, waarbij specifieke aandacht nodig is voor de CHECK-fase.

Aanbeveling 3
Effectieve risicobeheersing is essentieel voor de organisatie, omdat het de organisatie in staat stelt te kunnen sturen op risico's. Zo kan proactief worden omgegaan met potentiële dreigingen, maar ook met kansen. Tevens biedt effectieve risicobeheersing een solide basis voor weloverwogen besluitvorming. Aan de defensieonderdelen wordt aanbevolen om gerichte verbeteringen door te voeren in de CHECK-fase met betrekking tot risicobeheersing. Dit betreft zowel het tijdig identificeren, communiceren, escaleren en behandelen van beveiligingsrisico's, overeenkomstig het beleid.

Aantal sterren	
****	Risicobeheersing voor informatiesystemen zit verankerd in het accreditatieproces en is voldoende *in control*.

Personele beveiliging

Onderdeel van personele beveiliging betreft het uitvoeren van veiligheidsonderzoeken door de Unit Veiligheidsonderzoeken (UVO), een samengestelde afdeling van de AIVD en MIVD. Met de Tweede Kamer is afgesproken dat 90% van de veiligheidsonderzoeken binnen de wettelijke termijn van acht weken dient te worden afgerond. Het blijkt dat de wettelijke termijn en de 90%-norm binnen de DO-fase niet gehaald worden, wat effect heeft op de ACT-fase.

Aantal sterren	
***	Defensie loopt een risico in de ACT-fase op het onderdeel personele beveiliging, omdat veiligheidsonderzoeken niet binnen de afgesproken termijn worden afgerond. Dit kan leiden tot uitdagingen ten aanzien van de beschikbare capaciteit, wat een mogelijke beveiligingskwetsbaarheid kan zijn. Eind 2024 werden veiligheidsonderzoeken binnen deze termijn afgerond, waardoor dit risico kleiner werd.

Accreditatie kritieke informatiesystemen

Samen met de beveiligingsketen houdt de BA zicht op de voortgang van de accreditaties van kritieke informatiesystemen.

Aantal sterren	
****	De beoordeling van het proces ten behoeve van het accrediteren van kritieke informatie-systemen toont aan dat de processen ingericht zijn volgens de PDCA-cyclus. Daarbij staat het streven naar continue verbetering centraal. Voor alle kritieke informatiesystemen geldt dat deze zijn voorzien van een (tijdelijke) accreditatie. Verbeterplannen gekoppeld aan tijdelijke accreditaties worden gemonitord. Accredita-ties hebben een beperkte geldigheid, wat betekent dat deze cyclisch worden herzien en aangepast op basis van de PDCA-principes.

Accreditatie locaties

In haar rol als *Security Accreditation Authority* (SAA) behandelt de BA meerdere locatie-accreditatieverzoeken van locaties en/of compartimenten (hierna: locaties) voor een beperkt aantal hoog gerubriceerde informatiesystemen.

Aantal sterren	
***	Voor een beperkt aantal informatiesystemen geldt dat locaties met een werkplek moeten worden beoordeeld aan de hand van de van toepassing zijnde beveiligingsnormen. De locatie-accreditatie is randvoorwaardelijk. Net als bij de accreditatie van kritieke informatie-systemen zijn de processen voor een locatie-accreditatie ingericht volgens de PDCA-cyclus. Het afgelopen jaar lag de focus van de BA als toezichthouder vooral op de CHECK-fase bij het accrediteren van locaties. Het blijkt echter belangrijk om verbeterplan-nen actief te monitoren (ACT-fase). Door de beperkte capaciteit is de BA onvoldoende toegekomen aan de werkzaam-heden die met de aandacht op de ACT-fase beoogd waren. Inmiddels is capaciteit verhoogd en zal de ACT-fase onderdeel zijn van het interne toezicht.

Elektronische Veiligheidsonderzoeken

Elektronische Veiligheidsonderzoeken (EVO) moeten uitsluiten dat er ongeautoriseerd meegeluisterd kan worden met hoog gerubriceerde gesprekken in gerubriceerde ruimtes.

Aantal sterren	
***	Defensieonderdelen wijzen gerubriceerde gespreksruimtes aan en een interne dienstverlener onderzoekt of deze aan de eisen voldoen. De onderzoekscapaciteit bleek in de voorgaande toezichtjaren onvoldoende om aan de vraag te kunnen voldoen. Na een eerste uitbreiding in 2022 is de onderzoekscapaciteit van de interne dienstverlener in 2024 verder uitgebreid tot een verdubbeling ten opzichte van 2021. Met de huidige onderzoekscapaciteit kan deze dienstverlener een groot deel van de EVO-aanvragen behandelen. Dit onderwerp omvat echter meer dan alleen het uitvoeren van onderzoeken, zoals het toewijzen en beheren van gerubriceerde gespreksruimtes door de defensieonderdelen. In het proces gericht op het toewijzen en beheren van gerubriceerde gespreksruimtes, de ACT-fase, zijn de defensieonderdelen nog onvoldoende in control. Hier is in 2024 onvoldoende verbetering in geweest.

Industriebeveiliging

Bedrijven die voor Defensie gerubriceerde en/of vitale opdrachten uitvoeren, moeten voldoen aan de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO).

Aantal sterren	
****	De processen ten behoeve van industriebeveiliging zijn ingericht op basis van de PDCA-cyclus. De verantwoordelijkheden voor dit onderdeel zijn bij verschillende entiteiten belegd en de organisatie is voldoende *in control*. Ondanks dit oordeel hangt het succes vooral af van het vroegtijdig identificeren van de ABDO-plicht in bijvoorbeeld het behoeftestellingenproces. De komende jaren zal de ontwikkeling van ABRO, als vervanging van ABDO, relevanter worden.

4 Bijlage

Afkortingen

ABDO	Algemene Beveiligingseisen voor defensieopdrachten
ABRO	Algemene Beveiligingseisen voor Rijksoverheidsopdrachten
AR	Algemene Rekenkamer
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BA	Beveiligingsautoriteit
BNIVD	Beveiligingsnormen Inlichtingen- & Veiligheidsdiensten
CDS	Commandant der Strijdkrachten
DBB	Defensie Beveiligingsbeleid
EU	Europese Unie
EVO	Elektronische Veiligheidsonderzoeken
FG	Functionaris voor Gegevensbescherming
IGK	Inspecteur-Generaal der Krijgsmacht
IMG	Inspectie Militaire Gezondheidszorg
IVD	Inspectie Veiligheid Defensie
KMCGS	Korps Militaire Controleurs Gevaarlijke Stoffen
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MLA	Militaire Luchtvaart Autoriteit
NATO	*North Atlantic Treaty Organization*
NSA	*National Security Authority*
NSA-MoD	*National Security Authority – Ministry of Defence*
PDCA	*Plan-Do-Check-Act*
PSO	*Program Security Officer*
SAA	*Security Accreditation Authority*
SAP	*Special Access Program*
SAPF	*Special Access Program Facility*
SG	Secretaris-Generaal
TBB	Te Beschermen Belang
UVO	Unit Veiligheidsonderzoeken