Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

12. Februar 2026

Prüfbericht «Überprüfung der als erledigt gemeldeten Massnahmen»

Abklärung A 2025-06

The Institute of Internal Auditors
IIA Switzerland

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

Herr
Bundesrat Martin Pfister
Chef VBS
Bundeshaus Ost
3003 Bern

Bern, 12. Februar 2026

Prüfbericht «Überprüfung der als erledigt gemeldeten Massnahmen»

Sehr geehrter Herr Bundesrat Pfister

Gerne lassen wir Ihnen unseren Prüfbericht «Überprüfung der als erledigt gemeldeten Massnahmen» zukommen. Den vorliegenden Bericht haben wir mit unseren Ansprechpersonen besprochen. Die Stellungnahme der Gruppe Verteidigung zu unserem Bericht ist in Kapitel 5 ersichtlich.

Diese Prüfung wurde in Übereinstimmung mit den internationalen Standards für die berufliche Praxis der internen Revision durchgeführt.

Sollten Sie Fragen zu unserem Bericht haben, stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
– Generalsekretär VBS
– Chef der Armee

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

Management Summary

Die Wirksamkeit, Zweckmässigkeit und Rechtmässigkeit von Prozessen, Organisationsstrukturen und Massnahmen innerhalb des Departements werden regelmässig durch die Interne Revision VBS (IR VBS) beurteilt.

Im Zeitraum von 2021 – 2024 führte die IR VBS bei der Gruppe Verteidigung (Gruppe V) diverse IT-Prüfungen und Abklärungen durch. Im Rahmen der vorliegenden Prüfung wurde risikobasiert die Umsetzung von 19 Empfehlungen aus früheren Berichten ausgewählt. Ziel war es zu beurteilen, ob die ausgesprochenen Empfehlungen umgesetzt wurden.

Von den 19 als erledigt gemeldeten Massnahmen konnte die IR VBS deren zehn als umgesetzt bestätigen. Weitere acht Massnahmen wurden als «teilweise umgesetzt» und eine Massnahme als «nicht umgesetzt» eingestuft. Die nur teilweise oder nicht umgesetzten Empfehlungen werden im Monitoring der IR VBS infolgedessen weiterhin als pendent geführt. Die vollständige Umsetzung der beauftragten Massnahmen wird zu einem späteren Zeitpunkt nochmals überprüft.

1 Ausgangslage

Die Interne Revision VBS (IR VBS) führt regelmässig Prüfungen durch, um die Wirksamkeit, Zweckmässigkeit und Rechtmässigkeit von Prozessen, Organisationsstrukturen und Massnahmen innerhalb des Departements sicherzustellen. Die aus den Prüfungen resultierenden Empfehlungen werden durch die Departementsvorsteherin bzw. den Departementvorsteher VBS als verbindliche Massnahmen zur Verbesserung der Sicherheit, Effizienz und Steuerungsfähigkeit zur Umsetzung beauftragt. Deren systematische Überprüfung stellt sicher, dass identifizierte Risiken wirksam reduziert, Schwachstellen behoben und die angestrebten Verbesserungen erreicht werden.

Im Zeitraum von 2021 – 2024 führte die IR VBS bei der Gruppe Verteidigung (Gruppe V) diverse IT-Prüfungen und Abklärungen durch. Im Rahmen der aktuellen Prüfung wurden risikobasiert insgesamt 19 Massnahmen ausgewählt, die von der geprüften Stelle als erledigt gemeldet worden sind. Ziel war es zu beurteilen, ob die ausgesprochenen Empfehlungen umgesetzt wurden.

2 Auftrag, Methodik und Abgrenzung

Am 15. Oktober 2025 beauftragte der Chef VBS die IR VBS risikoorientiert zu beurteilen, ob die an die Gruppe V beauftragten Massnahmen aus den Prüfungen der Jahre 2021 – 2024 umgesetzt worden sind.

Dazu führte die IR VBS Interviews mit Schlüsselpersonen durch, welche mit der Umsetzung der Massnahmen beauftragt worden waren. Ergänzend analysierte die IR VBS die für die Beurteilung der Umsetzung relevanten Dokumentationen.

Die Feststellungen beziehen sich auf den Umsetzungsstand bis zum Abschluss der Prüfungshandlungen Mitte Dezember 2025. Auf dieser Grundlage wurden die Beurteilungen und Empfehlungen formuliert. Entwicklungen nach Abschluss der Prüfungshandlungen sind in diesem Bericht nicht berücksichtigt.

3 Unterlagen und Auskunftserteilung

Die Interviewpartnerinnen und Interviewpartner der Gruppe V haben der IR VBS die notwendigen Auskünfte umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam mehrheitlich zur Verfügung. Die IR VBS dankt für die gewährte Unterstützung.

4 Feststellungen und Beurteilungen zum Stand der Umsetzung

In diesem Kapitel werden die als erledigt gemeldeten Massnahmen beurteilt. Die Empfehlungen sind gegliedert pro Prüfung aus den Jahren 2021 – 2024.

4.1 Social Media im VBS (A 2021-02)

Empfehlung 2:
Wir empfehlen der Kommunikation Verteidigung, in Anlehnung an die übergeordneten Kommunikationsdokumente, eine Social Media Strategie für die Gruppe Verteidigung abzuleiten. Darin sind die strategische Gesamtkonzeption (z. B. Zielpublikum, Plattformen, Inhalt) sowie die relevanten Governance-Aspekte (z. B. Monitoring, Reporting zuhanden Armeeführung) festzuhalten.

Für die Schweizer Armee wurde eine Social Media Strategie erarbeitet. Diese enthält die strategische Gesamtkonzeption sowie die relevanten Governance-Aspekte und regelt die externe Kommunikation in den Kanälen der sozialen Medien der Schweizer Armee. Die Strategie ist an die übergeordneten Kommunikationskonzepte des VBS und der Schweizer Armee angelehnt und daraus abgeleitet. Ergänzend wurde ein Social Media Handbuch erstellt, welches insbesondere der Truppe verbindliche Richtlinien für die Verwendung/Nutzung der Social-Media-Kanäle vorgibt.

Beurteilung

Die Empfehlung ist umgesetzt.

Die Nutzung von Social Media ist für die Schweizer Armee ein wichtiger Bestandteil ihrer Kommunikationsmassnahmen. Die IR VBS beurteilt positiv, dass neben der Social Media Strategie zusätzlich ein Handbuch erarbeitet wurde, welches die operative Umsetzung unterstützt und zur einheitlichen Anwendung beiträgt.

4.2 Einhaltung Grundschutz Bund bei externen IT-Partnern des VBS: Projekt Rechenzentrum 2020 (I 2021-05)

Empfehlung 1:
Wir empfehlen den Projektverantwortlichen «RZ VBS/BUND 2020 IKT A&I»:
- sämtliche wesentlichen Anforderungen aus dem Grundschutz Bund sowie deren geplante Umsetzung bis zum Ende der Konzeptphase, zusammen mit der Swisscom, im Modellierungstool zu dokumentieren und abzunehmen.
- die Kommunikation im Bereich Sicherheit zwischen den Projektverantwortlichen und der Swisscom weiter zu verfeinern.

Die Anforderungen aus dem Grundschutz Bund sind im Modellierungstool der strategischen Partnerin Swisscom AG (nachfolgend Swisscom) als Teil des «Erweiterten Grundschutzes» modelliert. Die Einhaltung der Anforderungen in den einzelnen Arbeitspaketen wird durch das Kommando Cyber (Kdo Cy) überwacht.

Auf der Stufe Projektleitung findet ein regelmässiger Abgleich statt, um die Sicherheit und den allgemeinen Fortschritt des Projekts zu besprechen sowie bei Bedarf Massnahmen einzuleiten. Weiter wurde auch die Zusammenarbeit im Bereich der Informationssicherheit sowie des Datenschutzes intensiviert. Auf der Stufe der Sicherheitsarchitektur findet eine enge Abstimmung mit den Sicherheitsverantwortlichen des Projekts und der Swisscom statt.

Beurteilung

Die Empfehlung ist umgesetzt.

Die IR VBS begrüsst es, dass die Anforderungen aus dem Grundschutz Bund modelliert und die Kommunikation zwischen dem Kdo Cy und Swisscom auf verschiedenen Ebenen verfeinert und intensiviert wurden. Die eingeleiteten Massnahmen zeigen ein zielgerichtetes Vorgehen.

4.3 Einhaltung Grundschutz Bund bei externen IT-Partnern des VBS (I 2021-06)

Empfehlung 1:
Wir empfehlen der Gruppe Verteidigung, zusammen mit den Verantwortlichen der RUAG Real Estate AG eine Domotikstrategie für den zielführenden Betrieb auszuarbeiten und die Domotiksysteme zu inventarisieren.

Für einen zielführenden Betrieb wurde durch die RUAG Real Estate AG (RRE) per 1. Juli 2023 eine Domotikstrategie[1] erarbeitet und freigegeben. Zudem wurden alle Domotiksysteme, welche im IP[2]-Netz eingebunden sind, systematisch erfasst und inventarisiert.

Beurteilung

Die Empfehlung ist umgesetzt.

Die Empfehlung wurde konsequent und nachvollziehbar umgesetzt. Die laufende Aktualisierung des Inventars der Domotiksysteme soll konsequent weitergeführt werden.

Empfehlung 2:
Wir empfehlen der Gruppe Verteidigung, zusammen mit den Verantwortlichen der RUAG Real Estate AG Prozesse für die Domotiksysteme zu erstellen bzw. an das neue IT-Umfeld anzupassen sowie die dazugehörigen Kontrollen zu definieren und anschliessend zu implementieren.

Im Rahmen der Restrukturierung des Konzerns wurde bei der RRE die Fachgruppe Domotik geschaffen, welche direkt an das Facility Management Competence Center rapportiert und als übergeordnete Instanz für sämtliche vernetzten Gebäudetechnologien fungiert. Das Leistungsspektrum des Fachbereichs umfasst eine Vielzahl technischer Disziplinen, u. a. Gebäudeleitsysteme (GLS), Türsteuerungssysteme, IP-basierte Videoüberwachungsanlagen, Brand- und Einbruchmeldeanlagen. In den Aufgabenbereich fallen u. a. auch die Inventarisierung, der Life Cycle, der Betrieb, die zyklische Wartung sowie Planung/Bau im Bereich Domotik.

Die Prozessabläufe im Bereich des Berechtigungswesens sowie die Dokumentationen mit den Prozessschritten für den Änderungsprozess der aktuellen Prozesslandschaft liegen vor. Auch wurde die Netzwerkdokumentation erstellt, welche im Rahmen des regulären Betriebs kontinuierlich aktualisiert wird.

[1] Bezeichnung der Einrichtungen, Software und Dienstleistungen für automatische Steuerung und Regelung, Überwachung und Optimierung von Gebäuden und technischen Steuerungen.

[2] IP steht für Internet Protocol (Internetprotokoll) und ist ein grundlegender Satz von Regeln, der die Adressierung und Weiterleitung von Datenpaketen in Netzwerken (wie dem Internet) steuert; eine IP-Adresse ist die eindeutige numerische Kennung (z. B. 192.168.1.1 oder eine IPv6-Adresse), die jedem mit einem Netzwerk verbundenen Gerät zugewiesen wird, damit es Daten senden und empfangen kann.

Damit Domotiksysteme ans Netzwerk angebunden werden können, müssen diese einen standardisierten Service Request Prozess durchlaufen. Dieser stellt sicher, dass die Domotiksysteme vorgängig beurteilt und im Inventar fortlaufend erfasst bzw. nachgetragen werden. Zudem unterstehen sämtliche ICT[3]-Komponenten der Domotik dem ICT Service Continuity Management Prozess.

Im Rahmen der Prüfung im Jahr 2021 wurden die Domotiksysteme in den Gebäuden an jeweils einem Standort in Bern und Thun beurteilt. Während die IT-Sicherheitsdokumente (u. a. Schutzbedarfsanalyse, Grundschutz Bund, Informationssicherheits- und Datenschutzkonzept) für die Türsteuerungssysteme vorliegen, werden die Dokumente für die anderen Domotiksysteme (u. a. Gebäude- und Sicherheitsleitsystem; Heizung, Lüftung, Klima) bis Mitte 2026 erarbeitet und finalisiert.

Der Aufbau des Security Operations Centers (SOC) wurde im Jahr 2021 in Zusammenarbeit mit einem externen Partner initiiert. Seit 2025 ist das SOC vollständig in das übergreifende Service Level Agreement (SLA) der RUAG AG integriert. Die operativen Leistungen werden seither durch einen externen Dienstleister erbracht. Die übergeordnete Koordination sowie das Security Incident Management wird durch die RUAG-interne Sicherheitsabteilung (Security Operations Management) sichergestellt.

Beurteilung

Die Empfehlung ist teilweise umgesetzt.

Die IR VBS beurteilt positiv, dass die Prozesse etabliert sowie die Domotiksysteme bei einer Neuerfassung oder Anpassung fortlaufend inventarisiert werden. Dies unterstützt die konsequente Umsetzung. Obwohl gegenwärtig die IT-Sicherheitsdokumente noch nicht für alle Domotiksysteme vorliegen, kann angemerkt werden, dass diese in die Roadmap aufgenommen wurden und bis Mitte 2026 erarbeitet und finalisiert werden.

Die Empfehlung 2 wurde teilweise umgesetzt. Aus diesem Grund wird diese Empfehlung im Monitoring der Internen Revision VBS weiterhin als pendent geführt. Die vollständige Umsetzung der beauftragten Massnahme wird zu einem späteren Zeitpunkt nochmals überprüft.

[3] ICT (engl. Information and Communications Technology): Informations- und Kommunikationstechnik (IKT)

Empfehlung 3:
Wir empfehlen der Gruppe Verteidigung, zusammen mit den Verantwortlichen der RUAG Real Estate AG ein formalisiertes Lifecycle Management für die Domotiksysteme auszuarbeiten.

Im Rahmen der Lifecycle Strategie der RUAG Real Estate AG wird festgehalten, dass alle operativen Anlagen vom jeweiligen Hersteller über einen gültigen Wartungs- und Supportvertrag verfügen müssen. Weiter muss ein Wechsel der Anlage vorgenommen oder die Anlage ausser Betrieb genommen werden, sobald ein Hersteller den Support einstellt. Nicht zuletzt sind im Zuge des regulären Lifecycle Managements Harmonisierungen der jeweiligen Anlagekategorien anzustreben. Der Lebenszyklus von Domotiksystemen wird in der Fachgruppe GLS eng begleitet.

In den letzten Jahren wurden Anlagen, welche am Ende des Lebenszyklus angelangt sind, fortlaufend ersetzt und inventarisiert. Gemäss Vorgabe der Strategie wurde das Schwergewicht bei der Neubeschaffung von Anlagen auf einen Hersteller gelegt, um die Harmonisierung voranzutreiben.

Zudem konnte mit den Herstellern der Domotiksysteme ein systematischer Austausch etabliert werden.

Beurteilung

Die Empfehlung ist umgesetzt.

Die IR VBS begrüsst es, dass ein formalisiertes Lifecycle Management für die Domotiksysteme ausgearbeitet wurde und dieses konsequent umgesetzt wird.

4.4 Honorarbeziehende in der Gruppe Verteidigung (A 2022-01)

Empfehlung 1:
Aufgrund unserer Feststellungen und Beurteilungen empfehlen wir dem Chef der Armee, zur besseren Einhaltung der beschaffungsrechtlichen Vorgaben für die Bewirtschaftung von Honorarverträgen in der Gruppe Verteidigung ein Vertragsmanagementsystem zu verwenden, welches insbesondere zur Steuerung, Überwachung und Controlling geeignet ist. Zudem sollen die Mitarbeitenden hinsichtlich der Abgrenzung zwischen Arbeitsverträgen und Aufträgen und deren Folgen bei Honorarverträgen sensibilisiert werden.

Per Anfang 2025 wurde eine einheitliche Erfassung der Honorarverträge über das Geschäftsverwaltungssystem initiiert, um eine zentrale Steuerung, Überwachung und Kontrolle zu ermöglichen. Die Mitarbeitenden werden nun workflow-basiert durch die Prozessschritte geführt, um die Einhaltung der beschaffungsrechtlichen Vorgaben sicherzustellen. Die Umsetzung obliegt den Bedarfskoordinationsstellen (BEKO) in den Verwaltungseinheiten (VE).

Gemäss Weisungen Chef der Armee für die Gruppe Verteidigung vom 1. Januar 2025 sind die BEKO auf Stufe der VE für die Bewirtschaftung des Controllings und Reportings verantwortlich (Ziffer 5, Art. 5 Bst. f). Die Informationen zu den Honorarverträgen werden nun zentral erfasst und können durch die BEKO ausgewertet werden. Auf Stufe Gruppe V findet gegenwärtig jedoch weder eine aktive Überwachung noch ein entsprechendes Controlling dieser Verträge statt.

Des Weiteren werden die Mitarbeitenden laufend für die Abgrenzung zwischen Arbeitsverträgen und Aufträgen und deren Konsequenzen bei Honorarverträgen geschult und sensibilisiert.

Beurteilung

Die Empfehlung ist teilweise umgesetzt.

Die IR VBS wertet positiv, dass die Mitarbeitenden regelmässig zu Honorarverträgen geschult und sensibilisiert werden, da in diesem Bereich sowohl rechtliche, finanzielle als auch organisatorische Risiken bestehen. Besonders in der Gruppe V mit hohen Compliance- und Transparenzanforderungen ist ein sorgfältiger Umgang mit Honorarverträgen entscheidend.

Damit aus der Erfassung der Verträge im Vertragsmanagementsystem, welches grundsätzlich zur Steuerung, Überwachung und dem Controlling geeignet ist, auch ein Mehrwert erzielt und die Verantwortung des Controllings wahrgenommen werden kann, sollten die Honorarverträge aktiv gesteuert und überwacht werden. Gegenwärtig ist ein formeller Controllingprozess auf Stufe der Gruppe V jedoch nicht aufgesetzt.

Die Empfehlung 1 wurde teilweise umgesetzt. Aus diesem Grund wird diese Empfehlung im Monitoring der IR VBS weiterhin als pendent geführt. Die vollständige Umsetzung der beauftragten Massnahme wird zu einem späteren Zeitpunkt nochmals überprüft.

4.5 Betrieb Security Operations Center (SOC) (I 2022-03)

Empfehlung 1:
Aufgrund unseres Fazits empfehlen wir der Gruppe Verteidigung, den hohen Anteil an externen Fachkräften im Bereich des Firewall Managements zu reduzieren. Damit ein permanenter 7/24-Betrieb des SOC ab Anfang 2025 sichergestellt werden kann, sollten die dafür notwendigen Stellen im SOC rasch möglichst besetzt werden.

Nach anfänglichen Schwierigkeiten bei der Rekrutierung geeigneter Spezialisten und Spezialistinnen konnten inzwischen genügend neue Mitarbeitende gewonnen und die entsprechenden Stellen besetzt werden. Der 7/24-Betrieb kann nun auch ausserhalb der Bürozeiten mittels einer Pikettorganisation gewährleistet werden.

Mit der Entflechtung der Informations- und Kommunikationstechnik (IKT) fokussiert sich das Kdo Cy auf die Erbringung von sicheren und hochverfügbaren (krisenresistenten) IKT-Leistungen. Gegenwärtig sind die Mitarbeitenden im Bereich des Firewall Managements beim Bundesamt für Informatik und Telekommunikation (BIT) in der Hauptabteilung Defence Plattform angesiedelt und somit ausserhalb des Verantwortungsbereichs der Gruppe V.

Beurteilung

Die Empfehlung ist umgesetzt.

Die IR VBS begrüsst es, dass das Kdo Cy die relevanten Stellen mit qualifizierten Fachkräften besetzen konnte, sodass der 7/24-Betrieb des SOC nun sichergestellt ist.

Empfehlung 2:
Aufgrund unseres Fazits empfehlen wir der Gruppe Verteidigung, geeignete Schutzmechanismen im Bereich der Netzwerkzugangskontrolle (NAP/NAC) zu implementieren.

Die Abklärungen mit dem Bundesamt für Rüstung (armasuisse) haben ergeben, dass die geforderten Schutzmechanismen im Bereich der Netzwerkzugangskontrolle mit den netzseitig erforderlichen technischen und betrieblichen Voraussetzungen im Rahmen von Secure Network Access (SNA) im Führungsnetz Schweiz implementiert wurden.

Netzwerkzugangskontrollen werden bereits durch verschiedene Systeme wie die Domotik-, Landesknoten und im Rahmen des Projektes CCTV V[4] angewendet. Ab Mitte 2026 werden die ersten militärischen Endgeräte (MEG) diesen Service nutzen.

Beurteilung

Die Empfehlung ist umgesetzt.

Die Empfehlung wurde im bisherigen Projektverlauf des Führungsnetzes Schweiz netzwerkseitig umgesetzt. Damit inskünftig auch die MEG überwacht werden können, müssen die Voraussetzungen für den SNA zuerst noch geschaffen werden, u. a. müssen die entsprechenden Clients/Endgeräte mit Maschinen-Zertifikaten ausgestattet werden. Dieser Service soll laufend ab Mitte 2026 angeboten werden.

[4] CCTV (engl.): Closed-circuit television

4.6 Videoüberwachung in der Gruppe Verteidigung (I 2022-04)

Empfehlung 1:
Aufgrund unseres Fazits empfehlen wir der Gruppe Verteidigung, die Standorte mit Videoüberwachungsanlagen zu inventarisieren.

Ende 2023 wurde bestätigt, dass ein Inventar der Standorte mit Videoüberwachungsanlagen erstellt wurde und die Nachführung, insbesondere im Zusammenhang mit dem Projekt «CCTV Verteidigung» (CCTV V), sichergestellt ist. Mit diesem Projekt unter der Federführung der Logistikbasis der Armee (LBA) soll bis Ende 2026 an über 30 Standorten der LBA eine standardisierte, skalierbare und über alle Lagen verfügbare Überwachungslösung umgesetzt werden. Nach Projektabschluss sollen die erarbeiteten Grundlagen allen VE der Gruppe V zur Verfügung gestellt werden, damit eine Vereinheitlichung im Bereich CCTV vorangetrieben werden kann.

Gegenwärtig ist geplant, die 33 Standorte im Rahmen von CCTV V nach einem Standardverfahren fortlaufend bis im Jahr 2028 auszurüsten und zu inventarisieren. Zudem wurden in den vergangenen zwei Jahren verschiedene Standorte (u. a. Militärflugplätze, Munitionsdepots) kontinuierlich inventarisiert. Eine systematische und vollständige Inventarisierung aller Standorte der Gruppe V kann zum Zeitpunkt dieser Prüfung jedoch nicht bestätigt werden.

Beurteilung

Die Empfehlung ist teilweise umgesetzt.

Die IR VBS begrüsst, dass die Standorte der Videoüberwachungsanlagen im Rahmen des Projekts CCTV V systematisch erfasst werden und auch bei den weiteren wesentlichen Standorten Fortschritte erzielt wurden. Demgegenüber muss festgehalten werden, dass gegenwärtig eine vollständige Inventarisierung aller Standorte nicht vorhanden ist. Aktuell sind auch keine Prozesse zur Beschaffung, zum Lifecycle Management und zur Inventarisierung von Videoüberwachungsanlagen etabliert.

Empfehlung 2:
Aufgrund unseres Fazits empfehlen wir der Gruppe Verteidigung, die Einhaltung der Bundesvorgaben regelmässig zu überprüfen. Insbesondere ist sicherzustellen, dass Reglemente für die Videoüberwachung vorliegen und den standortspezifischen Gegebenheiten ausreichend Rechnung getragen wird. Dabei ist auch die Verantwortlichkeit für die Datenbearbeitung, v. a. bei verschiedenen involvierten Parteien, für jeden Standort abschliessend zu klären.

Die VE der Gruppe V haben im Dezember 2023 bestätigt, dass standortspezifische Reglemente vorliegen und dies anhand von Stichproben kontrolliert wurde. Audits zur Prüfung der Einhaltung sollten in den Folgejahren durchgeführt werden. Zum Prüfungszeitpunkt konnten weder Nachweise zur durchgeführten Stichprobenprüfung noch zu Audits vorgelegt werden. Während Mustervorlagen und Hilfsmittel für standortspezifische Reglemente mittlerweile

existieren, kann gegenwärtig nicht bestätigt werden, dass standortspezifische Reglemente für alle Standorte mit Videoüberwachungsanlagen erarbeitet wurden. Dies betrifft auch die vier im November 2025 in Betrieb genommenen Standorte im Rahmen des Projektes CCTV V und wurde anhand einer Stichprobenprüfung durch die IR VBS nochmals bestätigt. Auch die Verantwortlichkeit für die Datenbearbeitung ist nicht für jeden Standort abschliessend geklärt. Dies ist u. a. auch dem Umstand geschuldet, dass bislang keine systematische und vollständige Inventarisierung aller Standorte stattgefunden hat (vgl. Empfehlung 1) und folglich die Anforderungen an die Dokumentationen nicht genügend durchgesetzt wurden.

Beurteilung

Die Empfehlung ist teilweise umgesetzt.

Obwohl während den Gesprächen mündlich bestätigt wurde, dass für die Standorte im Rahmen des Projektes CCTV V entsprechende standortspezifische Reglemente vorliegen, konnten diese nicht zeitnah vorgelegt werden. Für die übrigen Standorte konnte nicht abschliessend bestätigt werden, dass Reglemente existieren und Verantwortlichkeiten klar definiert sind. Die IR VBS nimmt zur Kenntnis, dass die beauftragte Massnahme noch nicht vollständig umgesetzt wurde.

Empfehlung 3:
Aufgrund unseres Fazits empfehlen wir der Gruppe Verteidigung, die Einhaltung der minimalen Sicherheitsanforderungen im Rahmen der Inventarisierung kritisch zu beurteilen. Die IT-Sicherheitsdokumente sind zu erstellen bzw. zu überarbeiten sowie regelmässig zu überprüfen und bei Bedarf zu aktualisieren, um den aktuellen Sicherheitsbedürfnissen Rechnung zu tragen.

Ende 2023 verfolgte die Gruppe V den Ansatz, dass die Videoüberwachungsanlagen von den VE der Gruppe V zu je einem «Schutzobjekt CCTV» (gemäss Art. 7 Abs. 2 Bst. b ISV[5]) zusammengefasst und die zugehörigen IT-Sicherheitsdokumente (u. a. Schutzbedarfsanalyse, Informationssicherheits- und Datenschutzkonzept, Nachweis der Umsetzung der Massnahmen zum Grundschutz Bund) erstellt werden. Dies entspricht dem Ansatz des Projektes CCTV V für standardisierte und skalierbare Überwachungslösungen mit standortspezifischen Reglementen.

Während für das Projekt CCTV V Nachweise zu den IT-Sicherheitsdokumenten erbracht werden konnten, fehlte der Nachweis für die restlichen Standorte mit Videoüberwachungsanlagen mit einer Ausnahme gänzlich. Zudem waren die IT-Sicherheitsdokumente des Projektes CCTV V zum Prüfungszeitpunkt abgelaufen.

[5] SR **128.1** - Verordnung vom 8. November 2023 über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV)

Beurteilung

Die Empfehlung ist teilweise umgesetzt.

Aufgrund der festgestellten Sachverhalte kann nicht abschliessend beurteilt werden, ob die Videoüberwachungsanlagen regelmässig überprüft werden, um den aktuellen Sicherheitsbedürfnissen Rechnung zu tragen.

Die Empfehlungen 1–3 wurden teilweise umgesetzt. Aus diesem Grund werden diese Empfehlungen im Monitoring der IR VBS weiterhin als pendent geführt. Die vollständige Umsetzung der beauftragten Massnahmen wird zu einem späteren Zeitpunkt nochmals überprüft.

4.7 Lagerhaltung von Armeematerial durch Dritte (A 2023-03)

Empfehlung 1:
Wir empfehlen der Logistikbasis der Armee (LBA), das bei den Auftragnehmern befindliche einfach verwendete Armeematerial ebenfalls in den Befehl für die Inventur des Armeematerials des Chef LBA einzubeziehen, um die Aufsicht der Lager zu vervollständigen.

Im «Befehl für die Inventur des Armeematerials» des Chefs LBA gültig ab dem 1. Januar 2025 wurde die Bestandskontrolle des einfach verwendeten Ersatzmaterials in Konsignationslagern aufgenommen. Die Inventuren in den Konsignationslagern bei den Industriepartnern sind ab dem Jahr 2026 geplant und sollen im gleichen Inventurrhythmus wie bei der LBA erfolgen.

Beurteilung

Die Empfehlung ist umgesetzt.

Die IR VBS beurteilt positiv, dass der Befehl entsprechend angepasst wurde, um die Aufsicht des eigenen Armeematerials zu vervollständigen.

Empfehlung 2:
Die IR VBS empfiehlt der Gruppe Verteidigung, das bestehende Lagerkonzept hinsichtlich Widerstandsfähigkeit und Robustheit der Konsignationslager zu überprüfen.

Bis zum heutigen Zeitpunkt ist die Thematik Widerstandsfähigkeit und Robustheit der Konsignationslager in verschiedene Konzepte und Projekte eingeflossen, u. a. Gesamtkonzeption Armeelogistik, Projekt LERAL (Leistungserbringung RUAG in allen Lagen) sowie Teilprojekt Dezentralisierung der Instandhaltung.

Die in der Empfehlung geforderte Überprüfung hat innerhalb dieser Konzepte stattgefunden. Die erarbeiteten Lösungen sehen vor, die Werkstätten und das Ersatzmaterial der Industrie

angemessen zu dezentralisieren und vor Waffenwirkung zu schützen. Die physische Umsetzung dieser Konzepte ist zum Prüfungszeitpunkt jedoch noch offen.

Beurteilung

Die Empfehlung ist umgesetzt.

Die Widerstandsfähigkeit und Robustheit der Konsignationslager wurde im Rahmen diverser Konzepte und Projekte beurteilt, eine zeitliche Abschätzung der Umsetzung ist aktuell aber nicht möglich.

4.8 Neue Digitalisierungsplattform (NDP) (I 2023-03)

Empfehlung 1:
Die IR VBS empfiehlt der Gruppe Verteidigung zu prüfen, wie das Risiko bezüglich der Alimentierung des Fachpersonals sowie der Überlastung der Betriebsorganisation weiter reduziert werden kann. Möglichkeiten dazu bilden zum Beispiel die Suche nach Partnerschaften mit internen und externen Stellen («Preferred Partnership»). Um der Überlastung der Betriebsorganisation entgegenzuwirken, sollte die Zusammenarbeit mit dem Portfoliomanagement des Armeestabs in Bezug auf die ressourcenmässige Machbarkeit vertieft werden.

Partnerschaften mit internen und externen Stellen («Strategische Partner») konnten bereits etabliert werden und der Rahmenvertrag mit einem weiteren strategischen Partner ist gegenwärtig in Erarbeitung.

Zur Vermeidung einer Überlastung der Betriebsorganisation werden interne Ressourcen weiterhin aufgebaut und eine Internalisierung von Fachkräften angestrebt.

Der Wissenstransfer vom Lieferanten hin zum Kdo Cy wird im Rahmen des Befähigungskonzeptes angestrebt und sieht den Wissensaustausch auf mehreren Ebenen vor. Die Mitarbeitenden sollen alle benötigten Fähigkeiten im Rahmen des Betriebsmodells und der neuen IT-Services der Plattform sowie einsatzkritischen Anwendungen aufbauen und anwenden können. Basierend auf den ersten Betriebserfahrungen werden dann die Prognosen für den Bedarf der Folgejahre angepasst und die entsprechenden Massnahmen getroffen. Mit den gegenwärtigen Ressourcen sowie den getroffenen Massnahmen kann die Betriebsbereitschaft per 1. Juli 2026 aussagegemäss sichergestellt werden. Der Ressourcenbedarf für die Folgejahre unterliegt jedoch verschiedenen Einflussfaktoren, welche momentan nur schwer abgeschätzt werden können.

Beurteilung

Die Empfehlung ist umgesetzt.

Die Empfehlung wurde im bisherigen Projektverlauf konsequent und nachvollziehbar umgesetzt und soll nach Aussagen der Projektleitung in den folgenden Phasen entsprechend weitergeführt werden.

Empfehlung 2:
Die IR VBS empfiehlt der Gruppe Verteidigung, in Zusammenarbeit mit armasuisse und im Dialog mit der Bundeskanzlei, der Eidgenössischen Finanzverwaltung und dem Eidgenössischen Personalamt zu prüfen, wie die Beschaffungs-, Finanzierungs- und Personalprozesse auch auf die agile Arbeitsweise angewendet werden können.

Im gegebenen Rahmen ist das VBS bereits heute bestrebt flexibel und dynamisch zu agieren (z. B. fähigkeitsbasierte Armeebotschaft). Der Beschaffungsprozess im Projekt NDP erfolgt mittels agiler Arbeitsmethoden und für die Betriebsunterstützung wird mit zwei strategischen Partnern zusammengearbeitet. Die agilen Arbeitsweisen sind in den Rahmenverträgen geregelt.

Auf Stufe Bundeskanzlei ist ein Vertreter des Kdo Cy in diversen Arbeitsgruppen vertreten, um die Projektmanagementmethode HERMES[6] weiterzuentwickeln und die agile Arbeitsweise zu fördern bzw. abzubilden.

Auf Stufe Gruppe V lassen die aktuellen Finanzprozesse bereits heute eine agile Vorgehensweise situativ zu. Geplant ist, dass mit der Armeebotschaft 2027 für die einsatzkritische IKT sowie dem Verpflichtungskredit Digitale Transformation diese Richtung eingeschlagen werden soll. Entsprechende Arbeiten wurden initiiert und die beiden Aspekte wurden bereits in der Armeeführung behandelt. Fortführende Diskussionen sind für den Sommer 2026 geplant; darüber hinaus sind weitere Arbeiten notwendig.

Die Abteilung Einsatz IKT des Kdo Cy arbeitet im Rahmen der Entwicklung der NDP mit dem agilen Vorgehensmodell «Scaled Agile Framework» (SAFe). Anlässlich der Implementierung des Vorgehensmodells hat die Gruppe V die rechtlichen und prozessualen Rahmenbedingungen geprüft und sowohl mit dem Generalsekretariat VBS (GS-VBS) als auch mit dem Eidgenössischen Personalamt (EPA) abgesprochen. Daraus resultierte die Beurteilung, dass die Umsetzung von agilen Arbeitsmethoden sowohl rechtlich als prozessual möglich ist.

Die Rahmenbedingungen beim Kdo Cy für diese Agilität wurden durch die Governance NDP und den Programmauftrag NDP, der nach «HERMES 2022 Programm Management» erarbeitet wurde, etabliert. Das Programm NDP soll per 2028 in ein Lean Portfolio Management

[6] HERMES ist die Projektmanagementmethode für Projekte im Bereich der Informatik, der Entwicklung von Dienstleistungen und Produkten sowie der Anpassung der Geschäftsorganisation. HERMES unterstützt die Steuerung, Führung und Ausführung von Projekten verschiedener Charakteristiken und Komplexität.

des Kdo Cy für einsatzkritische IKT-Leistungen überführt werden. Das Kdo Cy muss schnell reagieren können, wenn neue Anforderungen und technische Änderungen im hochdynamischen IKT-Umfeld entstehen. Das Vorhabensziel besteht daher aus der schrittweisen Bildung eines Lean Budgets für DevOps[7] der einsatzkritischen IKT. Die nötige Handlungsfreiheit im Einsatz der finanziellen Mittel soll durch die Bündelung der Investitionskredite[8] für einsatzkritische IKT für vier Jahre, sowie der Kredite für Betrieb und Lebensweg erhöht werden. Damit soll das Potential des Lean Portfolio Managements ab 2028 genutzt und die Armee in der Fähigkeitsentwicklung mit optimaler Handlungsfreiheit unterstützt werden.

Beurteilung

Die Empfehlung ist umgesetzt.

Die IR VBS begrüsst, dass die Optimierungen entlang des Austausches mit den Partnern der Bundesverwaltung diskutiert und nach Möglichkeit aufgenommen werden.

4.9 Sicherheitsdokumentation (I 2024-02)

Empfehlung 2:
Die Interne Revision VBS empfiehlt der Gruppe Verteidigung, die Unterschriftsberechtigungen und Kompetenzen im Bereich der Sicherheit im Hinblick auf die neue Informationssicherheitsverordnung in den jeweiligen Geschäftsordnungen, Weisungen etc. zu regeln.

In den Geschäftsordnungen der Gruppe V und deren VE sowie den «Weisungen Chef der Armee für die Gruppe Verteidigung» vom 1. Januar 2025 sind die Unterschriftsberechtigungen und Kompetenzen im Bereich der Informationssicherheit gegenwärtig nicht definiert.

Die Sicherheitsorganisation der Gruppe V befindet sich gegenwärtig in einer Reorganisation. Um eine zielgerichtete Steuerung und eine reibungslose Zusammenarbeit zu ermöglichen, wird die Fachverantwortung per 1. Januar 2026 neu definiert und zugewiesen. Die Umsetzung wird anlässlich der Erstellung der «Weisungen über die Sicherheit in der Gruppe Verteidigung (WeSich V)» im Detail beschrieben. Im Rahmen der neuen Rollenbesetzung sollen auch die Unterschriftsberechtigungen und Kompetenzen festgelegt werden. Gegenwärtig werden das Informationssicherheits- und Datenschutzkonzept (ISDS) sowie der Grundschutz Bund aussagegemäss jeweils vom sicherheitsverantwortlichen Direktunterstellten des Chefs der Armee unterschrieben.

[7] DevOps ist eine Softwareentwicklungsmethodik, die die Bereitstellung leistungsstarker Anwendungen und Dienste beschleunigt, indem sie die Arbeit von Softwareentwicklungs- (Dev) und IT-Betriebsteams (Ops) kombiniert und automatisiert.

[8] Die Risiko-Reserven in den Rüstungsprogrammen werden durch das Prinzip Design To Cost (DTC) ersetzt

Beurteilung

Die Empfehlung ist nicht umgesetzt.

Die IR VBS begrüsst, dass die Unterschriftsberechtigungen und Kompetenzen im Bereich der Sicherheit im Rahmen der Reorganisation der Sicherheitsorganisation der Gruppe V kritisch beurteilt und festgelegt werden sollen.

Empfehlung 3:
Die Interne Revision VBS empfiehlt der Gruppe Verteidigung sicherzustellen, dass für alle Public-Cloud-Anwendungen vor deren operativen Nutzung durch die Verwaltungseinheiten eine Schutzbedarfs- und Risikoanalyse durchgeführt wird.

Das VBS erlaubt den Einsatz von verschiedenen Public-Cloud-Anwendungen zu Geschäftszwecken und führt gemäss Ziffer 11 Absatz 1 Buchstabe m der Informatiknutzungsweisung VBS vom 1. Januar 2025 eine Liste mit zugelassenen Public-Cloud-Anwendungen.

Um eine zielgerichtete Steuerung und reibungslose Zusammenarbeit zwischen den VE der Gruppe V zu ermöglichen, wird die Fachverantwortung im Rahmen der Reorganisation der Sicherheitsorganisation V neu definiert und zugewiesen. Der Sicherheitsbereich Informationssicherheit wird ab 1. Januar 2026 beim Kdo Cy angesiedelt. Diese VE verfügt bereits heute über eine «ISMS Richtlinie Information Security zur Nutzung von Cloud-Services (RL015)», welche grundsätzlich für alle Mitarbeitenden (intern und extern) der Armee und der Militärverwaltung gilt.

Aktuell sind bei der Gruppe V keine Kontrollen etabliert, welche den Einsatz von Public-Cloud-Anwendungen aktiv überwachen und somit identifizieren, ob eine Schutzbedarfs- und Risikoanalyse vor deren operativen Nutzung durchgeführt wurde.

Beurteilung

Die Empfehlung ist teilweise umgesetzt.

Gegenwärtig wird für den Einsatz von Public-Cloud-Anwendungen in der Gruppe V auf die Informatiknutzungsweisung VBS sowie die Richtline RL015 verwiesen. Obwohl die beauftragte Massnahme als umgesetzt gemeldet wurde, konnte kein Nachweis zur Umsetzung einer formellen Kontrolle zur Identifikation und Überwachung von eingesetzten Public-Cloud-Anwendungen erbracht werden. Der Zustand gegenüber dem Zeitpunkt der initialen Prüfung ist de facto unverändert.

Empfehlung 4:
Die Interne Revision VBS empfiehlt der Gruppe Verteidigung, die Informationssicherheitsbeauftragten bzw. zuständige Fachstelle der Verwaltungseinheiten frühzeitig zu Vorhaben mit Fachanwendungen einzubeziehen.

Das Standard-Sicherheitsverfahren sieht vor, dass die Informationssicherheitsbeauftragten der VE (ISBO) bereits in der Initialisierungsphase eines Projektes involviert sind und jeweils die Sicherheitsdokumentationen unterschreiben. Die Prüfung «Informationssicherheit beim Beschaffungs- und Vertragsmanagement» (I 2025-03) hat jedoch gezeigt, dass dies nicht durchgehend der Fall ist. Die Gespräche mit den ISBO bei der Gruppe V ergaben, dass sie bei Projekten der Kategorien A und B, d. h. bei komplexen Erst- und Initialbeschaffungen, in den Beschaffungsprozess einbezogen werden. Demgegenüber stehen die Beschaffungsvorhaben der Kategorien C (Folgebeschaffungen) und D (Nachbeschaffungen) sowie Dienstleistungsbeschaffungen, wo ein durchgehender Einbezug nicht sichergestellt ist.

Beurteilung

Die Empfehlung ist teilweise umgesetzt.

Obwohl die Informationssicherheitsvorgaben des Bundes im Rahmen des Sicherheitsverfahrens vorsehen, bei jedem Informatikvorhaben vorab eine Schutzbedarfsanalyse (Schuban) durchzuführen, werden die ISBO nicht durchgängig und frühzeitig einbezogen. Die IR VBS sieht den Handlungsbedarf primär darin, dass einerseits die im Sicherheitsprozess beteiligten Personen stufengerecht geschult und sensibilisiert (siehe nachfolgend Empfehlung 5) werden müssen und andererseits die Rollen und Verantwortlichkeiten an der Schnittstelle zwischen der Gruppe V und armasuisse zu konkretisieren sind (siehe *Empfehlung 1 im Prüfbericht I 2025-03*).

Empfehlung 5:
Die Interne Revision VBS empfiehlt der Gruppe Verteidigung, in Zusammenarbeit mit dem Generalsekretariat (GS-VBS), die Schulung und Sensibilisierung der im Sicherheitsprozess beteiligten Personen stufengerecht zu gewährleisten.

Die im Sicherheitsprozess beteiligten Personen wie beispielsweise Projektleitende, Anwendungsverantwortliche, Bedarfskoordinatoren sowie ISBO werden durch armasuisse periodisch geschult und sensibilisiert. Zudem fanden durch das Staatssekretariat für Sicherheitspolitik (SEPOS) nach der Inkraftsetzung des Informationssicherheitsgesetzes (ISG) sowie deren Ausführungsverordnungen per 1. Januar 2024 entsprechende Schulungen für die ISBO sowie weiteres Fachpersonal statt.

Ein formelles Konzept zur regelmässigen stufengerechten Schulung und Sensibilisierung von im Sicherheitsprozess beteiligten Personen existiert seitens Gruppe V nicht.

Beurteilung

Die Empfehlung ist teilweise umgesetzt.

Obwohl seitens armasuisse und SEPOS periodisch Schulungen zu Themen im Bereich der Informationssicherheit durchgeführt werden, liegt seitens Gruppe V kein Konzept vor, welches eine stufengerechte Schulung und Sensibilisierung vorsieht und diese aktiv steuert und überwacht.

Die Empfehlungen 2–5 wurden nicht bzw. teilweise umgesetzt. Aus diesem Grund werden diese Empfehlungen im Monitoring der IR VBS weiterhin als pendent geführt. Die vollständige Umsetzung der beauftragten Massnahmen wird zu einem späteren Zeitpunkt nochmals überprüft.

5 Stellungnahme

Gruppe Verteidigung

Die Gr V dankt für die Möglichkeit der Stellungnahme, die sie in zwei Teilen vornimmt; nämlich im Rahmen von allgemeinen Bemerkungen und im Rahmen von einer Stellungnahme zu einzelnen als erledigt gemeldeten Massnahmen, die bei der Nachprüfung als nur teilwiese oder gar nicht umgesetzt beurteilt wurden.

Allgemeine Bemerkungen:
Anlässlich einer Besprechung am 27.01.2026 wurde der Prüfbericht und mögliche Ursachen zwischen Vertretern des GS-VBS und dem A Stab besprochen. Der Gr V ist es wichtig, dass beim Erlass von Empfehlungen in den Prüfberichten das Erwartungsmanagement geschärft wird, indem die Messkriterien betreffend Umsetzungsgrad der Empfehlungen und Massnahmen (umgesetzt, teilweise umgesetzt, nicht umgesetzt) sehr klar definiert sind. Im Rahmen von Schlussbesprechungen ist verbindlich zu regeln, in welchem Zeitfenster Empfehlungen und Massnahmen umzusetzen sind. Besprechungen der Prüfberichte sind zudem dem Korrespondenzweg immer vorzuziehen. Wichtig ist, dass im Rahmen der Besprechung eine Priorisierung vorgenommen wird – es soll eine sinnvolle Anzahl von Massnahmen definiert werden, die innerhalb einer vernünftigen Zeit umgesetzt werden können.

Bemerkungen zu den Empfehlungen, die nur teilweise oder nicht umgesetzt sind:
4.3 – Einhaltung Grundschutz Bund bei externen IT-Partnern des VBS
Empfehlung 2: IT-Sicherheitsdokumente liegen nicht vollständig vor; und ausstehend sind noch die Systeme der Gebäudetechnik. Umsetzung bis 31.12.2026.

4.4 – Honorarbeziehende in der Gr V
Empfehlung 1: Formelles Controllingkonzept mit klaren fachlichen Zuständigkeiten fehlt. Umsetzung bis 30.06.2027.

4.6 – Videoüberwachung in der Gr V
Empfehlung 1: Systematische und vollständige Inventarisierung der Videoüberwachungsanlagen fehlt. Umsetzung bis 30.11.2026.
Empfehlung 2: Standortspezifische Reglemente sowie Definition der Zuständigkeiten für alle Standorte mit Videoüberwachung fehlen. Umsetzung bis 30.06.2027.
Empfehlung 3: Es fehlen gültige IT-Sicherheitsdokumente der Videoüberwachungsanlagen. Umsetzung bis 30.09.2027.

4.9 - Sicherheitsdokumentation
Empfehlung 2: Die Unterschriftsberechtigungen und Kompetenzen sind nicht festgelegt. Umsetzung bis 30.09.2027.
Empfehlung 3: Kontrollen zur Identifikation und Überwachung von eingesetzten Public-Cloud-Anwendungen fehlen. Umsetzung bis 31.01.2027.

Empfehlung 4: ISBO werden nicht durchgängig und frühzeitig einbezogen. Rollen und Verantwortlichkeiten an der Schnittstelle zwischen der Gruppe V und armasuisse fehlen. Umsetzung bis 31.01.2027.
Empfehlung 5: Es fehlt ein formelles Konzept zur regelmässigen stufengerechten Schulung und Sensibilisierung von im Sicherheitsprozess beteiligten Personen. Umsetzung bis 30.09.2027.