



12. Februar 2026

---

# **Prüfbericht «Informationssicherheit beim Beschaffungs- und Vertragsmanagement»**

## IT-Prüfung I 2025-03

---





Herr  
Bundesrat Martin Pfister  
Chef VBS  
Bundeshaus Ost  
3003 Bern

Bern, 12. Februar 2026

**Prüfbericht «Informationssicherheit beim Beschaffungs- und Vertragsmanagement»**

Sehr geehrter Herr Bundesrat Pfister

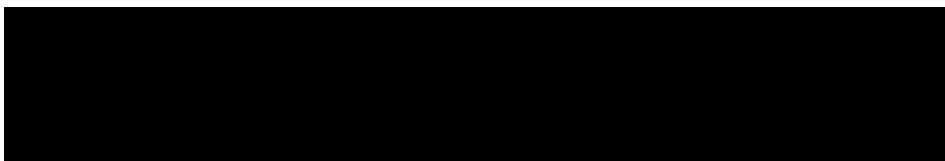
Gerne lassen wir Ihnen unseren Prüfbericht «Informationssicherheit beim Beschaffungs- und Vertragsmanagement» zukommen. Den vorliegenden Bericht haben wir mit unseren Ansprechpersonen besprochen. Die Stellungnahme zu unserem Bericht ist in Kapitel 7 ersichtlich.

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**



**Verteiler**

- Generalsekretär VBS
- Rüstungschef

## Management Summary

Die Zusammenarbeit des VBS mit externen Lieferanten ist für die Beschaffung und den Unterhalt von Systemen, Gütern und Dienstleistungen von zentraler Bedeutung. Damit verbunden können erhebliche Risiken im Bereich der Informationssicherheit entstehen, da Lieferanten oftmals direkten oder indirekten Zugang zu sensiblen Daten und kritischen Systemen erhalten. Idealerweise wird die Informationssicherheit bei der Bedarfserhebung berücksichtigt, um die sicherheitsrelevanten Anforderungen bereits bei der Lieferantenauswahl abdecken zu können. Die Interne Revision VBS hat in diesem Zusammenhang geprüft, ob die Informationssicherheit im Beschaffungs- und Vertragsmanagement angemessen verankert ist und ob die bestehenden Prozesse eine wirksame Steuerung der Informationssicherheitsrisiken gewährleisten. Die Prüfung hat gezeigt, dass die Verantwortlichkeiten im Bereich der Informationssicherheit im Rahmen von Beschaffungsvorhaben klar geregelt sind. Bei grossen und/oder komplexen Beschaffungsvorhaben erfolgt die Abwicklung in einer Projektstruktur nach anerkannten Projektmanagementmethoden, wobei die Informationssicherheitsbeauftragten der Verwaltungseinheit (ISBO) frühzeitig und laufend einbezogen werden. Demgegenüber zeigt sich bei kleineren Projekten sowie den Dienstleistungsbeschaffungen ein differenziertes Bild. In knapp der Hälfte aller geprüften Beschaffungsvorhaben konnte keine Schutzbedarfsanalyse vorgelegt werden und die gemäss den Prozessvorgaben zwingend auszufüllende Checkliste Sicherheit – als Nachweis über die Beurteilung der Sicherheitsrelevanz – lag in keinem der geprüften Vorhaben vor. *Deshalb empfiehlt die Interne Revision VBS armasuisse, über die Bedarfsstelle sicherzustellen, dass die Anforderungen an die Informationssicherheit für jedes Beschaffungsvorhaben erfüllt werden, um einen effizienten Beschaffungsablauf zu gewährleisten.* Damit diese Vorgaben auch in der Praxis durchgängig umgesetzt werden, ist es erforderlich, dass die mit Beschaffungsaufgaben betrauten Personen regelmässig geschult und sensibilisiert werden. Zwar existieren bereits selektive Schulungen, allerdings werden nicht alle relevanten Funktionen systematisch geschult. Eine solche Sensibilisierung ist jedoch unabdingbar, damit die Informationssicherheit über den gesamten Lebenszyklus von Beschaffungsvorhaben hinweg ausreichend berücksichtigt wird.

Ein weiterer Schwerpunkt der Prüfung betraf das Vertrags- und Lieferantenmanagement. armasuisse verfügt gegenwärtig über kein vollumfänglich etabliertes und standardisiertes Lieferantenmanagement, obwohl Umfang und Komplexität der Lieferantenbeziehungen eine systematische Steuerung erforderlich machen. Der Handlungsbedarf wurde erkannt und der Aufbau eines solchen Systems wurde bereits vor der durchgeführten Prüfung eingeleitet.

Die gegenwärtig vorliegenden Vertragsvorlagen sowie die «Vereinbarung betreffend Umgang mit schutzwürdigen Informationen und Cyberrisiken» erfüllen die Minimalanforderungen an die Informationssicherheit sowie die Sicherheitsvorgaben zur einheitlichen Zusammenarbeit mit Lieferanten gemäss den im Oktober 2025 vom Staatssekretariat für Sicherheitspolitik (SEPOS) veröffentlichten Standardbestimmungen. Gleichwohl ist eine regelmässige kritische Überprüfung der Vertragsklauseln hinsichtlich Informationssicherheit, um neuen technischen und regulatorischen Entwicklungen Rechnung zu tragen, empfehlenswert.

## 1 Ausgangslage

Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) ist auf leistungsfähige, sichere und verfügbare IT-Systeme angewiesen. In diesem Zusammenhang werden jährlich zahlreiche Verträge mit Lieferanten des Bundes abgeschlossen, hauptsächlich über die zentrale Beschaffungsstelle armasuisse. Die Hauptaufgabe von armasuisse liegt in der effizienten Projektabwicklung zur Evaluation und Beschaffung komplexer Systeme, Güter und Dienstleistungen für die Armee, unter Berücksichtigung der rechtlichen, finanziellen und zeitlichen Rahmenbedingungen. Sie ist gemäss Anhang 2 in der Verordnung über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (Org-VöB)<sup>1</sup> für die strategische und operative Beschaffung zuständig. Dies umfasst u. a. Rüstungsgüter sowie Waren, Dienstleistungen und Personalverleih im Bereich der IKT, die für Verteidigungs- und Sicherheitszwecke unerlässlich sind oder die im Zusammenhang mit der Beschaffung von Waffen, Munition, Kriegsmaterial stehen. Des Weiteren sind Waren und Dienstleistungen, deren primärer Verwendungszweck die Verschlüsselung von Zeichen und Daten (Kryptografie) oder die Entschlüsselung ohne Kenntnis des Schlüssels (Kryptoanalyse) ist, über armasuisse zu beschaffen. In begründeten Ausnahmefällen können Beschaffungskompetenzen von armasuisse gemäss Artikel 17 Org-VöB an die Verwaltungseinheiten (VE) des VBS delegiert werden.

Die Zusammenarbeit zwischen der Gruppe Verteidigung (Gruppe V) und armasuisse ist über alle Lebenswegphasen von Systemen, Material und IT hinweg definiert und wird durch die Weisungen über die Zusammenarbeit der Departementsbereiche Verteidigung und armasuisse (ZUVA) vom 1. Dezember 2022 geregelt.

Mit dem Einsatz von Lieferanten gehen Risiken für die Informationssicherheit einher. Dazu zählen unter anderem ungenügende vertragliche Regelungen zu Datenschutz, Geheimhaltung und Zugriffsschutz, eine fehlende Kontrolle über Subunternehmer oder unsichere Schnittstellen bei Datenverarbeitung und Systemintegration. Da Lieferanten des Bundes oft direkten oder indirekten Zugang zu sensiblen Informationen erhalten, gelten hohe Anforderungen an den Schutzbedarf – insbesondere für klassifizierte oder kritische Systeme im Zuständigkeitsbereich des VBS.

Informationssicherheit beginnt jedoch nicht erst mit dem Abschluss des Vertrages, sondern bereits bei der Bedarfserhebung. Die Bedarfsstellen müssen die sicherheitsrelevanten Anforderungen bereits frühzeitig definieren, während die Beschaffungsstelle dafür zu sorgen hat, dass diese Vorgaben in den Ausschreibungsunterlagen respektive bei den Offertanfragen

---

<sup>1</sup> SR 172.056.15 - [Verordnung vom 1. Mai 2024 über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung \(Org-VöB\)](#)

korrekt abgebildet werden. Auf diese Weise sollen die Sicherheitsanforderungen (z. B. hinsichtlich Informationssicherheit, Datenschutz) potenziellen Lieferanten des Bundes bereits bei der Angebotserstellung transparent dargelegt werden.

Die Schnittstelle zwischen Beschaffung und Informationssicherheit ist somit ein besonders sensibler Bereich, in dem strategische, technische, rechtliche und operative Aspekte ineinandergreifen. Eine enge Koordination zwischen armasuisse und den Bedarfsstellen ist dabei entscheidend, um Risiken frühzeitig zu erkennen, angemessen zu adressieren und eine nachhaltige Sicherheitskultur im Beschaffungswesen zu gewährleisten.

## **2 Auftrag, Methodik und Abgrenzung**

Am 11. Juli 2025 beauftragte der Chef VBS die Interne Revision VBS (IR VBS) mit der Prüfung, die Informationssicherheit beim Beschaffungs- und Vertragsmanagement zu beurteilen.

Die IR VBS führte strukturierte Interviews mit Schlüsselpersonen in den VE durch. Ergänzend analysierte die IR VBS interne Dokumente sowie öffentlich zugängliche externe Quellen, die für die Beurteilung relevant waren.

Die Feststellungen beziehen sich auf den Zustand bis zum Abschluss der Prüfungshandlungen per Ende Oktober 2025. Auf dieser Basis wurden auch die Beurteilungen und Empfehlungen formuliert. Entwicklungen nach Abschluss der Prüfungshandlungen sind in diesem Bericht nicht berücksichtigt.

## **3 Unterlagen und Auskunftserteilung**

Die Interviewpartnerinnen und Interviewpartner bei armasuisse, der Gruppe V, dem Generalsekretariat VBS sowie dem Staatssekretariat für Sicherheitspolitik (SEPOS) haben der IR VBS die notwendigen Auskünfte umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung. Die IR VBS dankt für die gewährte Unterstützung.

## **4 Verantwortlichkeiten im Bereich Informationssicherheit**

In Artikel 6 des Bundesgesetzes vom 18. Dezember 2020 über die Informationssicherheit (Informationssicherheitsgesetz, ISG)<sup>2</sup> wird festgehalten, dass die verpflichteten Behörden und Organisationen dafür sorgen, dass der Schutzbedarf der Informationen, für die sie zu-

---

<sup>2</sup> SR 128 - [Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit \(Informationssicherheitsgesetz, ISG\)](#)

ständig sind, hinsichtlich einer allfälligen Beeinträchtigung der Interessen nach Artikel 1 Absatz 2 ISG beurteilt wird. Artikel 9 schreibt zudem vor, dass die verpflichteten Behörden und Organisationen bei der Zusammenarbeit mit Dritten sicherstellen, dass die Anforderungen und Massnahmen des ISG in den entsprechenden Vereinbarungen und Verträgen festgehalten werden. Sie sind jedoch weiterhin für die angemessene Überprüfung der Umsetzung dieser Massnahmen verantwortlich.

Darüber hinaus regelt die Verordnung über das öffentliche Beschaffungswesen (VöB)<sup>3</sup> vom 12. Februar 2020 die Grundsätze und Verfahren für die Vergabe von Aufträgen an externe Leistungserbringer. Sie gewährleistet Transparenz, Gleichbehandlung und den wirtschaftlichen Einsatz von Ressourcen.

Im Kontext von Informationssicherheit und Datenschutz ist sicherzustellen, dass die Vorgaben des Datenschutzgesetzes<sup>4</sup>, des ISG und deren Ausführungsverordnungen vom 8. November 2023 (u. a. Informationssicherheitsverordnung<sup>5</sup>; Verordnung über das Betriebssicherheitsverfahren<sup>6</sup>; Verordnung über die Personensicherheitsprüfungen<sup>7</sup>) in öffentlichen Ausschreibungen respektive bei Offertanfragen berücksichtigt werden.

Bei armasuisse hat die Informationssicherheit einen grossen Stellenwert. Nebst den rechtlichen Grundlagen erarbeitet armasuisse gegenwärtig die Richtlinie «Informationssicherheit im Projektmanagement», welche die systematische Integration der Informationssicherheit in Projekten regelt, in denen armasuisse als zentrale Beschaffungsstelle agiert. Zudem ist das (Informationssicherheits-Management-System, ISMS) von armasuisse gemäss ISO-Standard ISO/IEC 27001:2022 zertifiziert. Im Rahmen der Rezertifizierung im Oktober 2025 wurde die Wirksamkeit der Kontrolle A.5.8 «Information security should be integrated into project management» erneut bestätigt.<sup>8</sup>

## Beurteilung

Gestützt auf den rechtlichen Grundlagen im ISG und dessen Ausführungsverordnungen (u. a. ISV, VBSV, VPSP) sowie dem Sicherheitsverfahren<sup>9</sup> gemäss Bundesamt für Cybersicherheit (BACS) sind die Verantwortlichkeiten bezüglich der Informationssicherheit im Rahmen von Beschaffungsvorhaben geregelt. Zudem ist hervorzuheben, dass armasuisse gegenwärtig die Richtlinie «Informationssicherheit im Projektmanagement» erarbeitet, welche

---

<sup>3</sup> SR 172.056.11 - [Verordnung vom 12. Februar 2020 über das öffentliche Beschaffungswesen \(VöB\)](#)

<sup>4</sup> SR 235.1 - [Bundesgesetz vom 25. September 2020 über den Datenschutz \(Datenschutzgesetz, DSG\)](#)

<sup>5</sup> SR 128.1 - [Verordnung vom 8. November 2023 über die Informationssicherheit in der Bundesverwaltung und der Armee \(Informationssicherheitsverordnung, ISV\)](#)

<sup>6</sup> SR 128.41 - [Verordnung vom 8. November 2023 über das Betriebssicherheitsverfahren \(VBSV\)](#)

<sup>7</sup> SR 128.31 - [Verordnung vom 8. November 2023 über die Personensicherheitsprüfungen \(VPSP\)](#)

<sup>8</sup> Schweizerische Vereinigung für Qualitäts- und Managementsysteme (SQS): Auditbericht - Assessmentbericht z. Hd. armasuisse, 13. Oktober 2025

<sup>9</sup> Bundesamt für Cybersicherheit (BACS): [Sicherheitsverfahren](#) (Stand: 10.09.2025)

die Verantwortlichkeiten und den Einbezug der Schlüsselfunktionen im Bereich der Informationssicherheit weiter präzisiert.

## 5 Informationssicherheit beim Beschaffungsprozess

### 5.1 Projekte und Beschaffungen nach ZUVA

Nach ZUVA können Beschaffungsvorhaben in vier Kategorien eingeteilt werden. Die komplexen *Erst- und Initialbeschaffungen* werden in der Regel als Projekte der Kategorie A oder B mittels der dafür vorgesehenen Projektmanagementmethode HERMES VBS<sup>10</sup> abgewickelt. Dies umfasst die erstmalige Beschaffung von Systemen/ Material, IT (IKT-Systeme, Daten/ Informationen) inkl. Immobilienvorhaben.

*Folgebeschaffungen* (Kategorie C) sind neue Beschaffungen im Zusammenhang mit einer Erst-/ Initialbeschaffung, z. B. mit Konfigurationsänderung. Handelt es sich dabei um die Folgebeschaffung eines Grosssystems oder sind die Abhängigkeiten zu anderen Systemen oder Immobilien gross, wird auch in der Folgebeschaffung ein Projekt der Kategorie A oder B gewählt. Bei *Nachbeschaffungen* (Kategorie D) handelt es sich um die wiederholte Beschaffung mit geringer oder keiner Konfigurationsänderung.

Für öffentliche Aufträge über Dienstleistungen gelten die Weisungen über den Abschluss von Dienstleistungsverträgen (WDL) vom 10. Januar 2024. Diese bezwecken ein koordiniertes und abgestimmtes Vorgehen und gelten für alle VE des VBS und die Armee. Ausgenommen sind Leistungen, die der Materialverordnung<sup>11</sup> unterstehen.

Die Informationssicherheitsvorgaben des Bundes sehen im Rahmen des Sicherheitsverfahrens vor, bei jedem Informatikvorhaben vorab eine Schutzbedarfsanalyse (Schuban) durchzuführen. Diese soll nach HERMES VBS während der Initialisierungsphase erstellt werden, um die Informatiksicherheit von Anfang an zu berücksichtigen. Anhand der Schuban wird u. a. beurteilt, ob der Auftrag die Ausübung einer sicherheitsempfindlichen Tätigkeit einschliesst (sicherheitsempfindlicher Auftrag) und folglich bei der Fachstelle für Betriebssicherheit ein Betriebssicherheitsverfahren (BSV) respektive eine Personensicherheitsprüfung (PSP) eingeleitet werden muss.

Anlässlich der Stichprobenprüfung wurde beurteilt, ob die Informationssicherheitsbeauftragten der VE (ISBO) bei Beschaffungsvorhaben einbezogen werden und ob bei den Informatikvorhaben vorab eine Schuban durchgeführt wird.

---

<sup>10</sup> 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.

<sup>11</sup> SR 514.20 - [Verordnung des VBS vom 26. März 2018 über die Beschaffung, die Nutzung und die Ausserdienststellung von Material \(Materialverordnung VBS, MatV\)](#)

Die Gespräche mit den ISBO bei der Gruppe V ergaben, dass sie bei Projekten der Kategorien A und B in den Beschaffungsprozess einbezogen werden. Demgegenüber stehen die Beschaffungsvorhaben der Kategorien C und D sowie Dienstleistungsbeschaffungen, wo ein durchgehender Einbezug nicht sichergestellt ist. Diese Einschätzung wird im Rahmen der Stichprobenprüfung insofern bestätigt, als dass eine Schuban im Zusammenhang mit den geprüften Beschaffungsvorhaben nur in knapp der Hälfte aller Fälle vorgelegt werden konnte. V. a. bei Beschaffungsvorhaben im Bereich der Innovationen wurde auf die Erstellung einer Schuban verzichtet. Ohne das Vorliegen einer entsprechenden Einstufungsbeurteilung des beim Beschaffungsvorhaben zugrundeliegenden Informatikschutzobjektes<sup>12</sup> konnte folglich auch nicht abschliessend beurteilt werden, ob die ISBO nach Artikel 37 Absatz 2 Buchstabe g ISV einen Antrag auf Einleitung des BSV hätten stellen müssen und eine PSP nach Artikel 27 Absatz 1 ISG erforderlich ist.

Die Durchsicht der Prozessbeschreibungen von armasuisse haben im Weiteren ergeben, dass die Sicherheitsanforderungen in der Konzeptphase zu verifizieren sind und die Checkliste Sicherheit für jedes Beschaffungsvorhaben als Nachweis über die Beurteilung der Sicherheitsrelevanz auszufüllen ist. Dieses Dokument deckt u. a. generelle Fragen zum Sicherheitsverfahren, der PSP sowie dem BSV ab, adressiert aber gegenwärtig nicht sämtliche Aspekte der Informationssicherheit und konnte für keine der Stichproben vorgelegt werden. Daneben müssen von der Bedarfsstelle bei Dienstleistungsbeschaffungen auch der Leistungsbeschrieb sowie die Checkliste WDL als Pflichtdokumente ausgefüllt werden. Beim Pflichtdokument des Leistungsbeschriebs sind generelle Anforderungen an die Sicherheit bereits definiert, müssen jedoch u. a. hinsichtlich Geheimhaltung, Datenschutz und Datensicherheit sowie Informationsschutz konkretisiert werden.

## **Beurteilung**

Bei den Sicherheitsorganisationen der Gruppe V wird grosser Wert auf das Vorliegen und die Aktualität der Sicherheitsdokumente gelegt. Während die ISBO bei den grossen Projekten regelmässig und frühzeitig einbezogen werden und die Schuban während der Initialisierungsphase erstellt wird, zeichnet sich bei den kleineren Projekten sowie den Dienstleistungsbeschaffungen ein differenziertes Bild. Dies ist nicht weiter überraschend, da der administrative Aufwand bei Letzteren in Grenzen gehalten werden soll. Bei den grossen Projekten müssen nach anerkannten Projektmanagementmethoden (z. B. HERMES VBS) hingegen

---

<sup>12</sup> Als Schutzobjekte gelten gemäss Informationssicherheitsverordnung (ISV) Artikel 7 Absatz 2 einzelne oder mehrere gleichartige oder zusammenhängende:

- a. Sammlungen von Informationen, die zur Abwicklung eines Geschäftsprozesses des Bundes bearbeitet werden;
- b. Informatikmittel: Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen.

Module jeweils abgeschlossen sowie Phasen und Meilensteine durchlaufen respektive freigegeben werden, wobei Anforderungen an die Informationssicherheit einen integralen Bestandteil bilden.

Die IR VBS ist der Ansicht, dass die Anforderungen an die Informationssicherheit in der bereits im Beschaffungsprozess vorgesehenen Checkliste Sicherheit überarbeitet sowie präzisiert werden sollten, um einen effizienten Beschaffungsablauf sicherzustellen und sämtliche Aspekte der Informationssicherheit abzudecken. Die Checkliste Sicherheit soll durch die Bedarfsstelle für jedes Beschaffungsvorhaben als verpflichtendes Dokument ausgefüllt werden müssen, analog zum Leistungsbeschrieb sowie der Checkliste WDL bei Dienstleistungsbeschaffungen. Alternativ könnten die Anforderungen an die Informationssicherheit auch in den Leistungsbeschrieb integriert werden. Ohne entsprechende Bestätigung der Anforderungen an die Informationssicherheit durch die Bedarfsstelle sollte der Beschaffungsprozess seitens armasuisse nicht ausgelöst werden.

Die Bedarfsstellen und deren ISBO müssen frühzeitig einbezogen werden, um ihrer Verantwortung gemäss ISV gerecht zu werden. Zudem gewährleistet eine vollständige und transparente Erfassung aller Sicherheitsanforderungen seitens Bedarfsstelle, dass armasuisse diese bereits bei der Ausschreibung respektive der Offertanfrage an die Lieferanten kommunizieren kann. Dadurch lässt sich das Risiko zeit- und kostenintensiver nachgelagerter Arbeitsschritte – aufgrund möglicher Nichterfüllung der Mindestanforderungen – deutlich reduzieren.

#### **Empfehlung 1: Anforderungen an die Informationssicherheit**

Die Interne Revision VBS empfiehlt armasuisse, über die Bedarfsstelle sicherzustellen, dass die Anforderungen an die Informationssicherheit für jedes Beschaffungsvorhaben erfüllt werden, um einen effizienten Beschaffungsablauf zu gewährleisten.

## **5.2 Delegation von Beschaffungskompetenzen**

Delegationen der Beschaffungskompetenzen gemäss Artikel 17 Org-VöB liegen gegenwärtig für das Bundesamt für Bevölkerungsschutz (BABS) im Bereich der Projekte vor. Des Weiteren gibt es mit der Gruppe V im Rahmen der Vereinbarung «Konvention 150» eine sogenannte unterschwellige Delegation, wonach Beschaffungen von Gütern und Dienstleistungen im freihändigen Verfahren bis zu 150 000<sup>13</sup> Franken durch die Gruppe V selbst getätigt werden können.

Einhergehend mit einer Delegation sieht Artikel 20 Absatz 1 Org-VöB vor, dass die Delegationsempfängerin die Aufgaben und Zuständigkeiten der zentralen Beschaffungsstelle ab dem Zeitpunkt der Delegation übernimmt. Armasuisse steht in diesen Fällen weiterhin beratend

---

<sup>13</sup> SR 172.056.1 - [Bundesgesetz vom 21. Juni 2019 über das öffentliche Beschaffungswesen \(BöB\)](#), Anhang 4, Absatz 2

zur Seite und stellt die Vertragsvorlagen zur Verfügung, ist aber nicht mehr aktiv in die Beschaffungsvorhaben involviert.

In der «Konvention 150» wird in Artikel 9.4 festgehalten, dass für Dienstleistungen die Vertragsvorlagen der Gruppe V in Absprache mit armasuisse genutzt werden müssen. Die beschaffende Stelle in der Gruppe V ist ebenfalls verantwortlich, dass die «Vereinbarung betreffend Umgang mit schutzwürdigen Informationen und Cyberrisiken» mit den Lieferanten des Bundes abgeschlossen wird, wobei die Vorlage von armasuisse zur Verfügung steht. Des Weiteren müssen die in den Beschaffungsprozess involvierten Personen seitens Gruppe V ein Minimum an Schulungen absolvieren.

Im Zusammenhang mit den Delegationen der Beschaffungskompetenzen bei Projekten des BABS existiert ein entsprechender Beschaffungsprozess für Dienstleistungen und Güter. Dieser sieht bereits bei der Bedarfsanalyse den Einbezug der Informationssicherheitsaspekte vor. Zudem verfügt das BABS über einen digitalen Beschaffungsauftrag, mit dem jede einzelne Beschaffung eingesteuert werden muss und die Informationssicherheit wiederum thematisiert wird.

### **Beurteilung**

Die IR VBS begrüsst, dass sowohl die Prozesse des BABS wie auch die «Konvention 150» mit der Gruppe V die frühzeitige und umfassende Berücksichtigung der Informationssicherheitsaspekte explizit vorsehen. Damit dies auch in der Praxis durchgehend umgesetzt wird, ist es von Bedeutung, dass die in den Beschaffungsprozess involvierten Personen regelmässig geschult und sensibilisiert werden.

### **5.3 Schulung und Sensibilisierung**

Die Bedarfskoordinatoren der Gruppe V werden drei Mal jährlich durch armasuisse geschult. Dabei werden die Koordinatoren u. a. über Anpassungen in den Vertragsvorlagen und sicherheitsrelevante Themen (z. B. Vereinbarung zur Auftragsdatenbearbeitung oder Schuban) orientiert.

### **Beurteilung**

Damit die Informationssicherheit bei der Zusammenarbeit mit der Privatwirtschaft sichergestellt werden kann, ist es aus Sicht der IR VBS unerlässlich, dass die Prozesse im Sicherheitsbereich allen Beteiligten klar und verständlich vermittelt werden. Die ISBO müssen frühzeitig in den Beschaffungsprozess einbezogen werden, damit die Weichen bzgl. Informationssicherheitsanforderungen rechtzeitig gestellt werden können. Nur so kann gewährleistet werden, dass die Informationssicherheit bereits zu Beginn berücksichtigt und kontinuierlich mit dem Fortschreiten der Auftragsvergabe und des Projekts weiterentwickelt wird. Zudem

muss den Lieferanten des Bundes schon zum Zeitpunkt ihrer Angebotseinreichung transparent dargelegt werden, welche sicherheitsmässigen Voraussetzungen (z. B. hinsichtlich Informationssicherheit, Datenschutz) sie erfüllen müssen.

Ohne Einstufungsbeurteilung der Anwendung oder des Projektes durch die Bedarfsstelle mit Hilfe einer Schuban ist nicht sichergestellt, dass nachgelagerte Prozesse wie z. B. das BSV oder eine PSP durchgeführt werden. Dem BSV kommt dabei eine tragende Rolle zu, denn die Lieferanten sollen von Beginn an wissen, was im Informationssicherheitsbereich von ihnen verlangt wird. Aus diesem Grund sollen die Bedarfsstellen bei der Fachstelle Betriebsicherheit die Einleitung des BSV beantragen, bevor ein öffentliches Vergabeverfahren in die Wege geleitet wird. Dies bedingt jedoch, dass nebst den ISBO auch die Bedarfskoordinatoren, die Projektleitenden und die Anwendungsverantwortlichen mit den entsprechenden Prozessen vertraut sind und im Bereich der Informationssicherheit regelmässig geschult und sensibilisiert werden.

## **6 Vertragsmanagement**

### **6.1 Aufbau des Vertragsmanagements im Rahmen des Lieferantenmanagements**

Ein Aufgabenschwerpunkt in der Beschaffung bildet das Lieferantenmanagement, das die Beziehung zum Lieferanten systematisch steuert. Bis auf die Beschaffungsmarktanalyse verfügt armasuisse gegenwärtig jedoch über kein vollumfängliches, strategisches und standardisiertes Lieferantenmanagement wie es in der Industrie sowie in bundesnahen Betrieben mittlerweile Standard ist. Das grosse Beschaffungsvolumen und die komplexen Beschaffungsgeschäfte und Lieferantenbeziehungen erfordern allerdings, dass auch armasuisse ein Lieferantenmanagement aufbaut. Den Handlungsbedarf hat armasuisse bereits erkannt und im Bereich Unternehmensentwicklung und Portfoliomanagement eine Stelle geschaffen, welche sich diesem Thema seit dem Frühjahr 2024 widmet. Das Vertragsmanagement als Unterkategorie stellt dabei ein Element dar, welches sich gegenwärtig im Aufbau befindet. Auch auf Stufe Departement respektive Bundesverwaltung fehlt aktuell ein gesamtheitliches Vertragsmanagement. Die neue Beschaffungs- und Vergabemanagementlösung (BVML) soll jedoch per Ende Juni 2026 über die gesamte Bundesverwaltung eingeführt werden.

Im Rahmen eines Projektes zur Harmonisierung der Prozesse zwischen den Kommerz-Bereichen wurde der Vertragsmanagementprozess entlang des Vertragslebenszyklus neu definiert. Das Ziel ist ein einheitliches Verständnis im Kompetenzbereich Beschaffung zu entwickeln (u. a. einheitliche Vertragsvorlagen, Vertragsübersicht etc.). Dieses Vorhaben wurde im Herbst 2025 abgeschlossen. Für die Mitarbeitenden (d. h. Direktbetroffene und restliche Belegschaft) wurde ein Ausbildungskonzept erstellt, welches ein E-Learning in Kombination mit einer Präsenzveranstaltung vorsieht. Der Hauptfokus liegt dabei allerdings auf der Einführung des neuen Vertragsmanagements und nicht explizit auf dem Thema Informationssicherheit bei Beschaffungsvorhaben (vgl. Abschnitt 5.3).

## Beurteilung

Der IST-Zustand birgt das Risiko, dass u. a. Doppelspurigkeiten und damit einhergehend Effizienzverluste vorliegen oder Reputationsschäden gegenüber Lieferanten aufgrund von z. T. nicht einheitlicher Vorgehensweisen entstehen. Mit der Schaffung einer Stelle im Bereich Unternehmensentwicklung und Portfoliomanagement und dem initiierten Aufbau des Lieferantenmanagements sowie der Harmonisierung der Vertragsmanagementprozesse wurde ein wichtiger Grundstein gelegt, um die systematische Steuerung der Beziehungen zu externen Leistungserbringern sicherzustellen sowie die Beschaffungspolitik der öffentlichen Hand nachhaltig, wirtschaftlich und rechtssicher zu gestalten. Des Weiteren soll mit der Einführung der neuen BVML per Mitte 2026 ein weiterer Meilenstein in Richtung einheitlichem und standardisiertem Beschaffungsprozess erreicht werden.

### 6.2 Standardbestimmungen für Beschaffungsverträge

Der Bundesrat beschloss am 1. Mai 2024 Massnahmen zur Vermeidung von Datenabflüssen bei Lieferanten des Bundes. Das Massnahmenpaket hält u. a. fest, dass die AGB des Bundes und die Standardklauseln zu Cybersicherheitsbedrohungen<sup>14</sup> in der Praxis oft zu unspezifisch sind, um mit den Lieferanten die konkreten, auftragsbezogenen Sicherheitsbedürfnisse zu stipulieren. Die Gestaltung von standardisierten Vertragsklauseln hat sich als schwierig erwiesen, weil gewisse dafür nötige technische Sicherheitsvorgaben heute entweder fehlen oder für Externe teilweise schwierig umzusetzen sind (z. B. IKT-Grundschutz des Bundes<sup>15</sup>). Das SEPOS wurde beauftragt, standardisierte Vertragsklauseln zur Informationssicherheit nach Artikel 10 Absatz 3 ISV sowie Sicherheitsvorgaben zur Zusammenarbeit mit Lieferanten bis Ende 2024 zu erarbeiten. Am 13. Oktober 2025 legte das SEPOS eine Sammlung von Standardbestimmungen vor, welche die Informationssicherheit in Beschaffungsverträgen des Bundes besser verankern soll. Im Sinne eines vertraglichen Grundschutzes sollen diese die Informationssicherheit des Bundes erhöhen und Datenabflüsse bei Lieferanten verhindern.

Die IR VBS hat bereits in einer früheren Prüfung<sup>16</sup> darauf hingewiesen, dass die Verträge mit Lieferanten des Bundes einer kritischen Prüfung unterzogen und bei Bedarf durch Nachträge ergänzt werden sollen. Dabei sollten insbesondere Aspekte wie Datenschutz und Datensicherheit, Klauseln zum Schutz der Informatikmittel vor Cyberangriffen, Meldepflichten sowie das Auditrecht zur Überprüfung der Einhaltung von Informationssicherheits- und Datenschutzerfordernissen bei externen Lieferanten berücksichtigt werden.

---

<sup>14</sup> Beschaffungskonferenz des Bundes BKB, [Mustervertragsklausel der BKB betreffend Cyberangriffen \(admin.ch\)](#) (Stand 22.11.2024)

<sup>15</sup> Bundesamt für Cybersicherheit BACS, [Grundschutz \(admin.ch\)](#) (Stand 20.10.2025)

<sup>16</sup> Interne Revision VBS: [Prüfbericht «Schutz der sensitiven Daten bei externen IT-Partnern des VBS in deren Entwicklungs- und Testumgebungen \(I 2024-03\)»](#) vom 4. Februar 2025

Im Rahmen der Überarbeitung der Vertragsvorlagen (vgl. Abschnitt 6.1) sind die Themen zur Informationssicherheit inzwischen eingeflossen. Zudem kommt bereits seit Längerem die «Vereinbarung betreffend Umgang mit schutzwürdigen Informationen und Cyberrisiken» als Vertragszusatz zur Anwendung.

### **Beurteilung**

Da die neuen Standardbestimmungen des SEPOS für Beschaffungsvorhaben unterhalb der Sicherheitsempfindlichkeit und ohne Datenschutz geschaffen wurden («Massengeschäft») und die Vertragsvorlagen von armasuisse diese Minimalanforderungen bereits erfüllen, müssen weder die aktuellen Vertragsvorlagen noch die «Vereinbarung betreffend Umgang mit schutzwürdigen Informationen und Cyberrisiken» angepasst werden. Eine regelmässige kritische Überprüfung der Vertragsklauseln hinsichtlich Informationssicherheit wird dennoch empfohlen.

## 7 Stellungnahme

### **Bundesamt für Rüstung (armasuisse)**

armasuisse ist mit der Empfehlung einverstanden. Insbesondere muss die Checkliste Sicherheit bei jeder Beschaffung ausgefüllt werden und dient als Nachweis für die Relevanzbeurteilung von notwendigen Sicherheitsmassnahmen. In dieser Checkliste wird auch die Relevanz des Themas Informationssicherheit abgefragt. Falls ja ist der ISBO/CISO mit einzubeziehen.

armasuisse wird in Zukunft besorgt sein, dass diese Checkliste bei Beschaffungen auch ausgefüllt wird.