Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

18. Januar 2021 [redacted]

Prüfbericht «ISMS.VBS Audit»

IT-Prüfung I 2020-07

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

Frau
Bundesrätin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 18. Januar 2021

Prüfbericht «ISMS.VBS Audit»

Sehr geehrte Frau Bundesrätin

Gerne lassen wir Ihnen unseren Prüfbericht «ISMS.VBS Audit» zukommen. Unsere Prüfarbeiten fanden zwischen Oktober und November 2020 statt. Das vorliegende Dokument haben wir mit unseren Ansprechpersonen abgestimmt. Die Stellungnahmen der Departementsbereiche zu unserem Bericht sind in Kapitel 8 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 jederzeit gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted] [redacted]

Leiter Interne Revision VBS Prüfleiter

Verteiler
– DU Chefin VBS

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

1 ISMS - ein Kurzüberblick

Informationen stellen wesentliche Werte in der öffentlichen Verwaltung sowie in Unternehmen der Privatwirtschaft dar und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage mit Informations- und Kommunikationstechnik (IKT) erstellt, gespeichert, transportiert oder verarbeitet. In Verwaltung und Wirtschaft bestreitet heute niemand mehr die Notwendigkeit, die eigene IKT-Landschaft angemessen zu schützen. Daneben müssen jedoch auch Informationen in allen anderen Phasen von Geschäftsprozessen angemessen gesichert werden. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für eine Institution bedrohend sein kann. Deshalb ist ein vernünftiger Informationsschutz sowie eine angemessene Grundsicherung der IKT mit einem möglichst verhältnismässigen Einsatz von Mitteln sicherzustellen.

Die internationale Norm ISO/IEC 27001 setzt die allgemein anerkannten Rahmenbedingungen für die Implementierung eines Informations-Sicherheits-Management-Systems (kurz ISMS). Die Einrichtung eines ISMS ist eine strategische Entscheidung der obersten Führung einer Organisationseinheit. In Verbindung mit dem Risikomanagementprozess stellt ein ISMS die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicher und signalisiert nach innen und aussen, welche Sicherheitsanforderungen eine Organisationseinheit leben will. In der Bundesverwaltung wird die Anwendung von etablierten Standards im Bereich der Informationssicherheit vom Informatiksteuerungsorgan des Bundes (ISB) empfohlen.

ISO/IEC 27001 besagt folgendes: «*Ein ISMS ist ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen. Es basiert auf einer Risikobeurteilung und dem Risikoakzeptanzniveau der Organisation und dient dazu, die Risiken wirksam zu behandeln und zu handhaben*»[1]. Daraus abgeleitet ergibt sich, dass ein ISMS grundsätzlich als iterativer Prozess über einen PDCA-Zyklus (Plan, Do, Check, Act) organisiert werden sollte. Dabei wird der Ansatz einer kontinuierlichen Verbesserung der Informationssicherheit in den Vordergrund gestellt.

2 Das ISMS im VBS

Verschiedene Vorgänge in der Vergangenheit haben gezeigt, dass im VBS die Aufgaben, Kompetenzen und Verantwortlichkeiten sowie die Verfahren zur wirksamen und systematischen Umsetzung der Informationssicherheit weiterentwickelt und auf einen noch besseren Stand gebracht werden müssen. Im Rahmen eines Projektes wurden daher die diesbezüglichen Vorgaben und Prozesse überarbeitet und erneuert. Dieses Projekt wurde Ende 2017

[1] ISACA Germany Chapter (2016). *Implementierungsleitfaden ISO/IEC 27001:2013*. Heidelberg: dpunkt.verlag. URL: https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf (9.12.2020)

abgeschlossen. Anschliessend ging das ISMS im ganzen VBS in den ordentlichen operativen Betrieb über.

Heute umfasst dieses ISMS zwei Ebenen:

Dezentrale Ebene: Die dezentralen Departementsbereiche tragen die Verantwortung für ihr individuelles ISMS. Dabei werden in einem strukturierten Zyklus Risiken bewirtschaftet und Massnahmen abgeleitet. Einige der dezentralen ISMS sind heute ISO 27001 zertifiziert.

Zentrale Ebene: Die Verantwortung für die Konsolidierung aller dezentralen ISMS liegt heute bei der Abteilung Digitalisierung und Cybersicherheit VBS (DCS), die im Generalsekretariat VBS angegliedert ist. Im Rahmen des «ISMS.VBS» sollten die Risiken aus allen Departementsbereichen regelmässig konsolidiert und systematisch bewertet werden (Bottom-up-Methode). Aus dieser Analyse soll schlussendlich ein managementgerechtes Reporting resultierten. Ende 2019 wurde eine Managementbewertung des ISMS.VBS durchgeführt und dieses anfangs 2020 von einer externen akkreditierten Auditstelle ISO 27001 zertifiziert. Dennoch konnten wir vor einem Jahr die Wirksamkeit des zentralen ISMS nicht bestätigten. Damals stellten wir fest, dass in verschiedenen Teilbereichen Lücken bestanden haben. Unsere Prüfung aus dem Vorjahr löste im Departement eine Grundsatzdiskussion zum ISMS.VBS aus und führt dazu, dass dessen Weiterentwicklung mehrheitlich eingestellt wurde.

3 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision VBS am 7. September 2020 den Auftrag, die Existenz und Wirksamkeit des ISMS.VBS auf Stufe Departement zu prüfen. Zudem haben wir den Umsetzungsstand der Massnahmen, aus der Vorjahresprüfung «ISMS.VBS Audit 2019» beurteilt. Dazu haben wir eine strukturierte Befragung bei den Verantwortlichen des zentralen ISMS.VBS sowie bei Fachexperten aus den Departementsbereichen (dezentrale Ebene) durchgeführt. Schliesslich haben wir den Umsetzungsstand der Hauptabweichung aus dem 2019 beurteilt, die zur Einschränkung der Wirksamkeit führte.

Unsere Aufgabe war es nicht, ISMS-Konformitätsaudits in den einzelnen Departementsbereichen des VBS (dezentrale Ebene) durchzuführen. Diese Verantwortung liegt bei der Abteilung DCS[2]. Zudem stellt dieser Audit keine Zertifizierungsprüfung dar. Jedoch verwenden wir in diesem Prüfbericht die gleichen Begriffe, wie sie in einer Zertifizierungsprüfung eingesetzt werden. An dieser Stelle definieren wir die beiden wichtigsten Begriffe wie folgt:

Hauptabweichung: Wird in einem ISMS-Audit eine wesentliche Feststellung aufgezeigt, zum Beispiel die Nichtumsetzung eines Normen-Kapitels, wird von einer Hauptabweichung gesprochen. Diese führt dazu, dass eine allfällige Zertifizierung nicht erfolgen kann.
Nebenabweichung: Wird in einem ISMS-Audit eine Nebenabweichung festgestellt, bedeutet

[2] gemäss Weisungen über die Informationssicherheit im VBS vom 16. Dezember 2016, Ziffer 9, Absatz c

dies, dass ein Normen-Kapitel zwar umgesetzt worden ist, die Umsetzung und Wirksamkeit jedoch noch Lücken aufweist. Mit wenigen Nebenabweichungen kann trotzdem eine Zertifizierung erfolgen. Allerdings müssen diese Nebenabweichungen bis zu einem vereinbarten Termin behoben werden.

4 Würdigung

Während unserer Prüfung trafen wir im ganzen Departement ausnahmslos engagierte Interviewpartner[3], die uns unterstützt und Informationen transparent zur Verfügung gestellt haben. Zudem gewannen wir den Eindruck, dass all unseren Ansprechpersonen die Informationssicherheit und damit auch das ISMS ein wichtiges Anliegen ist. Wir bedanken uns bei allen Beteiligten für die zielführende Zusammenarbeit.

Ergänzend halten wir an dieser Stelle fest, dass sich die Abteilung DCS momentan in einer Phase der Neuausrichtung befindet und dabei auch das ISMS.VBS vor einer grundlegenden Gesamtanalyse steht (siehe dazu auch Kapitel 2). In diese Standortbestimmung sollen sämtliche Departementsbereiche miteinbezogen werden. Der Abschluss dieser Arbeit ist auf Ende 2021 geplant. Wir erachten die Durchführung einer solchen Gesamtanalyse als sinnvoll. Diese soll ermöglichen, das ISMS.VBS auf eine neue Basis zu stellen.

5 Hauptabweichung

Unsere Prüfhandlungen haben ergeben, dass die Prozesse und Strukturen für die Bewirtschaftung des ISMS.VBS in der Abteilung DCS angemessen dokumentiert sind. Daher bestätigen wir die Existenz des ISMS.VBS. Jedoch ergab unsere Arbeit, dass bezüglich der von uns im Vorjahr formulierten Hauptabweichung kaum Fortschritte erzielt wurden. Nach wie vor findet auf zentraler Ebene keine systematische und risikobasierte Konsolidierung der relevanten Risiken statt. Daher resultiert auch kein managementgerechtes Reporting, welches eine VBS-weite Sicht auf wesentliche Informatiksicherheits-Risiken aufzeigt. Da auch die Schnittstelle zum Risikomanagement VBS wenig ersichtlich ist, beurteilen wir den heutigen Nutzen des ISMS.VBS als Führungsinstrument als gering. Aus all diesen Gründen können wir die Wirksamkeit des ISMS.VBS nicht bestätigen.

6 Nebenabweichungen

Von den sechs Nebenabweichungen, die wir im Vorjahr aufgezeigt haben, wurde bis heute eine behoben. Die Zusammenstellung der Nebenabweichungen und deren Stand der Umsetzung haben wir im Anhang dieses Berichts dokumentiert.

[3] Aus Gründen der Lesbarkeit wird bei Personenbezeichnungen die männliche Form gewählt; es ist jedoch immer die weibliche Form mitgemeint.

7 Empfehlung

Wir empfehlen dem Generalsekretariat VBS die bestehenden Abweichungen im Rahmen der laufenden Standortbestimmung des ISMS.VBS zu beheben.

8 Stellungnahmen

GS VBS
Das Generalsekretariat VBS ist mit der Empfehlung einverstanden.

Gruppe Verteidigung
Die Gruppe Verteidigung bedankt sich für die Gelegenheit einer Stellungnahme zum Prüfbericht "ISMS.VBS Audit". Wir unterstützen die im Bericht erwähnten Empfehlungen vollumfänglich. Es ist aus unserer Sicht wichtig, dass mit der Standortbestimmung die Aufgaben und Ziele des zentralen ISMS.VBS überprüft werden. Die Definition der fehlenden Schnittstelle zum Risikomanagement VBS ist sehr zu begrüssen, es muss aber zwingend der bestehende Risikomanagementprozess beigezogen werden, damit keine Doppelspurigkeiten entstehen und Risiken nicht mehrfach rapportiert und behandelt werden.

Nachrichtendienst des Bundes
Der NDB nimmt den Bericht zur Kenntnis und unterstützt die resultierende Empfehlung. Mit einer Überprüfung der Ziele des ISMS.VBS und einer möglichen Reduktion des Ambitionsniveaus kann unter Umständen dessen Nutzen als Führungsinstrument erhöht werden.

armasuisse
Die Verantwortlichen der Informationssicherheit armasuisse unterstützen den Bericht und dessen Erkenntnisse vollumfänglich. Durch die lang andauernde Restrukturierung des GS-VBS ist es nicht erstaunlich, dass bezüglich der im Vorjahr formulierten Hauptabweichung und Nebenabweichungen kaum Fortschritte erzielt wurden. Wir erachten es als sehr wichtig, dass die Punkte im 2021 unverzüglich umgesetzt werden, damit die erwartete Glaubwürdigkeit wiederhergestellt wird. Die armasuisse hat im September 2020 das erste Aufrechterhaltungsaudit ISO 27001:2013 erfolgreich bestanden.

BABS
Das BABS unterstützt die Empfehlung der Internen Revision vollumfänglich. Mit der Einführung des ISMS-Tools im GS-VBS und den Ämtern/Bereichen bietet sich erneut die Chance, die Informationssicherheit weiter zu optimieren. Dabei scheint uns wichtig, dass der Aufwand für die Erstellung und den Unterhalt von Sicherheitsdokumenten reduziert und der Fokus umso mehr auf gezielte Überprüfungen/Audits gelegt wird. Wir sind überzeugt, dass sich dadurch auch die Akzeptanz des ISMS und dessen Wirkung merklich verbessern wird.

BASPO
Das BASPO unterstützt die Empfehlung der Internen Revision. Wir erachten es zudem als zielführend, dass die Aufgaben und Ziele des zentralen ISMS.VBS grundsätzlich zu überprüfen sind. Wichtig scheint uns, Redundanzen zu vermeiden und den administrativen Aufwand weiterhin so gering wie möglich zu halten.

swisstopo
Den relativ ernüchternden Bericht, wonach der Nutzen des ISMS VBS als Führungsinstrument als «gering» eingestuft wird, hat swisstopo zur Kenntnis genommen. Diese Schlussfolgerung ist nachvollziehbar, ist doch nach dem departementsweiten Projektabschluss eine Art Vakuum entstanden, zurückzuführen auf diverse organisatorische und personelle Veränderungen sowie neue Zuständigkeiten für ISMS im GS VBS. Während auf zentraler Stufe die Wirksamkeit eines ISMS in Frage gestellt werden darf, ist darauf hinzuweisen, dass auf Stufe VE ein nach ISO 27'001 geprüftes ISMS durchaus den erwarteten Nutzen bringt und auf dezentraler Stufe die Wirksamkeit für die Amtsführung nachgewiesen werden kann.

Anhang

Nachfolgend fassen wir die bestehenden Haupt- und Nebenabweichungen zusammen:

HA-Nr.	Hauptabweichung	Status der Umsetzung
2020-1	**Wirksamkeit des ISMS.VBS** Eine unzureichende Konsolidierung der Risiken im ISMS.VBS führt zu einer hohen Unzufriedenheit bei dessen Anspruchsgruppen. Vor allem führt ein nicht zielführender Konsolidierungsprozess dazu, dass die Glaubwürdigkeit des ISMS.VBS leidet und dieses von der Departementsleitung kaum als Führungsinstrument genutzt wird. Wir erachten es als sinnvoll, eine Neubeurteilung zum ISMS.VBS vorzunehmen. Dabei sind u.a. dessen Ziele, die managementgerechte Form des Reportings sowie die Rolle des Sicherheitsverantwortlichen VBS festzulegen. Termin: 31. Dezember 2020	**Offen**

NA-Nr.	Nebenabweichungen	Status der Umsetzung
2018-1	**Erfassung der Schutzobjekte** Aktuell sind noch nicht alle Schutzobjekte im «ISMS.VBS» erfasst und bewertet. Gemäss Zielvorgaben der Generalsekretärin VBS sollen bis Ende 2018 50%, bis Ende 2019 100% der Schutzobjekte erfasst und bewertet sein. Die Verantwortung für die Erfassung der Schutzobjekte liegt bei den Verwaltungseinheiten, jedoch muss DCS diese Arbeiten zielführend überwachen. Termin: 31. Dezember 2019	Offen
2018-2	**Schnittstelle «Risikomanagement VBS» zu «ISMS.VBS»** Zurzeit verlaufen die beiden Prozesse noch parallel. Es ist geplant, diese mittels einer Schnittstelle zu verbinden und zu synchronisieren. Termin: 31. Januar 2020	Offen

NA-Nr.	Nebenabweichungen	Status der Umsetzung
2018-3	**Reporting von Kennzahlen zum «ISMS.VBS»** Um dem «ISMS.VBS» auch in Zukunft die notwendige Management-Attention zu geben, erachten wir es als sinnvoll, ausgewählte Kennzahlen in das Cockpit VBS einzubauen und regelmässig zu überwachen. Termin: 31. Januar 2020	Offen
2017-4	**Geheimschutzverfahren auf Datenschutz ausweiten / Sicherheitsrelevante Verträge** Es ist zu prüfen, ob die Anforderungen an den Datenschutz ebenfalls in das Geheimschutzverfahren einbezogen werden können. Insbesondere sind bei Überprüfungen von Lieferanten alle drei Themen der Informationssicherheit zu prüfen. Termin: 30. Juni 2019	Erledigt. Analyse ist erfolgt. Die Anforderungen an den Datenschutz werden nicht in das Geheimschutzverfahren einbezogen.
2017-6	**Zusammenarbeit Vertragswesen – Lieferantenaudits (ISMS.VBS)** Hinsichtlich der Durchführung von Lieferantenaudits sind die genannten Listen aus dem Vertragswesen einzubeziehen. Die Verträge sind regelmässig mit dem «ISMS.VBS» abzustimmen. Termin: 30. Juni 2019	Offen
2017-10	**Gemeinsamer Prozess für Meldung von Informationssicherheitsvorfällen und weiteren Sicherheitsvorfällen** Es ist zu prüfen, wo der Mehrwert dieser Regelung liegt und ob dadurch nicht «gefährliche» Schnittstellen geschaffen werden, welche zu unnötigen Koordinationstätigkeiten führen. Das bestehende Dokument «Sicherheitsmeldung» muss hierzu überarbeitet werden. Termin: 31. Januar 2020	Offen