Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

12. November 2019 [redacted]

Prüfbericht «ISMS.VBS – Konformitätsaudit 2019»

IKT-Prüfung I 2019-06

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, 12. November 2019

IKT-Prüfung «ISMS.VBS – Konformitätsaudit 2019»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «ISMS.VBS – Konformitätsaudit 2019» zukommen. Unsere Prüfarbeiten fanden zwischen Juli und September 2019 statt. Den vorliegenden Bericht haben wir mit dem Chef IOS am 6. September 2019 besprochen. Die Stellungnahmen der Departementsbereiche sind in Kapitel 8 ersichtlich.

Diese Prüfung wurde in Übereinstimmung mit den internationalen Standards für die berufliche Praxis der internen Revision durchgeführt. Der Prüfleiter ist zertifizierter ISMS Lead Auditor.

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

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
– DU Chefin VBS
– Chef IOS

Interne Revision VBS
Schauplatzgasse 11, 3003 Bern
Tel. +41 58 464 30 53

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 weiterverarbeitet. 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 adäquat 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*». 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 Vorfälle im VBS haben gezeigt, dass 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 des Projekts «ISMS.VBS» wurden daher die diesbezüglichen Vorgaben und Prozesse überarbeitet und erneuert. Dieses Projekt wurde Ende 2017 abgeschlossen, und das ISMS ging anschliessend in den ordentlichen Betrieb über.

Heute wird im VBS ein ISMS betrieben, welches auf einem «bottom up»-Prozess basiert. Dabei tragen die dezentralen Departementsbereiche die Verantwortung für ihr eigenes ISMS. Auf zentraler Ebene fasst die Abteilung Informations- und Objektsicherheit (kurz IOS) die Informationssicherheitsrisiken im «ISMS.VBS» zusammen und konsolidiert diese ein einer angemessenen Form. Seit dem 1. Januar 2018 wird dieses Managementsystem in allen Verwaltungseinheiten des VBS angewendet und ist in die ordentlichen Geschäftsprozesse eingebettet.

3 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision VBS am 3. Mai 2019 den Auftrag, die Existenz und Wirksamkeit des ISMS.VBS auf Stufe Departement zu prüfen. In erster Linie haben wir dazu eine strukturierte schriftliche Befragung bei insgesamt 19 Fachexperten aus allen Departementsbereichen des VBS durchgeführt. Zudem haben wir die für das ISMS.VBS verantwortlichen Personen in der IOS befragt und eine umfassende Dokumentenanalyse durchgeführt. Schliesslich haben wir den Umsetzungsstand unserer Empfehlungen vom Vorjahr beurteilt.

Unsere Aufgabe war es nicht, ISMS-Konformitätsaudits in den einzelnen Departementsbereichen des VBS (d.h. auf dezentraler Ebene) durchzuführen. Diese Verantwortung liegt gemäss WIns VBS[1] bei der IOS. 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 (Muss-Massnahme): 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 (Muss-Massnahme): Wird in einem ISMS-Audit eine Nebenabweichung festgestellt, bedeutet 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 abgearbeitet werden.

1 Weisungen über die Informationssicherheit im VBS vom 16. Dezember 2016, siehe Ziffer 9, Absatz c

4 Würdigung

Während unserer Prüfung trafen wir im ganzen Departement ausnahmslos engagierte Interviewpartner[2], 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.

5 Hauptabweichung

Unsere Prüfhandlungen ergaben, dass das ISMS.VBS in der IOS eingerichtet und angemessen dokumentiert ist und damit dessen **Existenz** bestätigt werden kann. Jedoch ergab sich aus unserer Befragung der VBS-Fachexperten (mehrheitlich die Sicherheitsbeauftragten in den Departementsbereichen), dass bezüglich der heute bestehenden Konsolidierung der Informationen aus den dezentralen ISMS in das ISMS.VBS eine gewisse Unzufriedenheit besteht. Die Umfrage ergab folgendes Bild:

– Der Nutzen des ISMS.VBS wird in Frage gestellt.
– Die Ziele und der Zweck des ISMS.VBS sind unklar.
– Ein gemeinsames Verständnis für das ISMS.VBS fehlt.
– Eine Schnittstelle des ISMS.VBS zum Risikomanagement VBS ist kaum ersichtlich.

Dies führt dazu, dass auch die Wirksamkeit des ISMS.VBS von den Fachexperten in Frage gestellt wird. Basierend auf unseren Prüfhandlungen kommen wir zu folgendem Schluss: Eine systematische und risikobasierte Erfassung der relevanten Risiken auf Stufe Departement findet derzeit kaum statt. Heute werden bei der IOS vorwiegend Querschnittsrisiken erfasst. Damit ist jedoch die VBS-weite Sicht auf die Informatiksicherheits-Risiken nicht gegeben. Dazu kommt, dass seit 2017 keine Managementbewertung des ISMS.VBS durchgeführt wurde, wie dies die Norm verlangt. Insgesamt beurteilen wir daher den heutigen Nutzen des ISMS.VBS als Führungsinstrument als gering. Aus all diesen Gründen können wir die **Wirksamkeit** des ISMS.VBS nicht bestätigen.

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

Wir formulieren daher folgende Hauptabweichung:

HA-Nr.	Hauptabweichung	Status der Umsetzung
2019-1	**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

6 Nebenabweichungen aus den Vorjahren

Von den sechs im Vorjahr entstandenen Nebenabweichungen konnten aus unserer Sicht bis heute keine erledigt werden. Nachfolgend zeigen wir auf, welche Nebenabweichungen im «ISMS.VBS» zum Berichtszeitpunkt noch bestehen. Unsere Feststellungen halten wir absichtlich kurz und geben dabei nur die wesentlichsten Punkte wieder.

NA-Nr.	Nebenabweichung	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. Termin: 31. Dezember 2019.	Offen; Termin noch nicht überschritten Stand per Ende August 2019: Knapp 70% der 200 Schutzobjekte sind erfasst und bewertet.
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; Termin noch nicht überschritten Stand per Ende August 2019: Die relevanten Parteien sind in den Lösungsprozess eingebunden. Die Arbeiten sind am Laufen.
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	Offen; Termin noch nicht überschritten

	einzubauen und regelmässig zu überwachen. Termin: 31. Januar 2020	Stand per Ende August 2019: Die relevanten Parteien sind in den Lösungsprozess eingebunden. Die Arbeiten sind am Laufen.
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	Offen; Termin überschritten Stand per Ende August 2019: Die IOS ist bei der Umsetzung dieses Punktes auf die Inkraftsetzung des neue ISG angewiesen.
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; Termin überschritten Stand per Ende August 2019: Im Rahmen der Umstrukturierung der IOS wird dieser Punkt neu beurteilt.
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; Termin noch nicht überschritten Stand per Ende August 2019: Im Rahmen der Umstrukturierung der IOS wird die Bewirtschaftung der Sicherheit neu überdacht.

7 Empfehlungen

Wir empfehlen der IOS die Hauptabweichung sowie die offenen Nebenabweichungen möglichst zielgerichtet zu bearbeiten und die diesbezüglichen Empfehlungen termingerecht umzusetzen. Im Konformitätsaudit 2020 werden wir sämtliche offenen Punkte erneut beurteilen.

8 Stellungnahmen

Generalsekretariat VBS

Das GS VBS dankt der Internen Revision VBS für die Prüfung des ISMS.VBS und für die Gelegenheit zur Stellungnahme zum Prüfbericht «ISMS.VBS – Konformitätsaudit 2019». Die Informationssicherheit ist ein sehr wichtiges Anliegen. Das Ergebnis der Prüfung zeigt Handlungsbedarf im Umfeld des ISMS.VBS. Das GS-VBS ist mit den Empfehlungen der Internen Revision grundsätzlich einverstanden. In der Folge werden zu einigen Sachverhalten Bemerkungen gemacht:

Zu Kapitel 5 Hauptabweichung: Das ISMS.VBS ist insbesondere das Instrument für die Informationssicherheitsverantwortlichen des VBS. Es liefert jeweils die Inhalte für die Konferenz der Sicherheitsverantwortlichen VBS, welche seit Mitte 2017 regelmässig durchgeführt wird. In der Umfrage wurden scheinbar die Informationssicherheitsverantwortlichen des VBS nicht einbezogen. Das BASPO, die FUB, die swisstopo und die armasuisse haben ihr ISMS bereits durch die Firma SQS ISO 27001 zertifizieren lassen. Das zeigt, dass viele Verantwortliche des VBS einen Nutzen im ISMS sehen. Ziel und Zweck des ISMS.VBS sowie die Rollen und Aufgaben der Informationssicherheitsverantwortlichen, sind seit dem 1.3.2017 in den Weisungen über die Informationssicherheit im VBS klar geregelt. Die bessere Abstimmung im Risikomanagement bildete im 2019 einen Schwerpunkt. In mehreren Sitzungen mit den Risiko-Coaches der Gruppen und Ämter und Risiko-Manager VBS wurden Verbesserungen erreicht. Die Wirksamkeit des ISMS.VBS, wurde durch die Firma SQS im Auditbericht vom 24. August 2019, als genügend beurteilt. Per Dezember 2019 ist die Zertifizierung des ISMS.VBS geplant.

Zu Kapitel 6 Nebenabweichungen: Aufgrund der verschiedenen Reorganisationen in der IOS und den diversen Abhängigkeiten zum Informationssicherheitsgesetz, konnten die bisherigen Empfehlungen nicht so rasch wie geplant umgesetzt werden.

Nachrichtendienst des Bundes

Der Bericht gibt die Aussagen des NDB wieder, insbesondere die Aussagen zur Risikoerfassung und -konsolidierung auf Stufe Departement und zur Schnittstelle zwischen dem ISMS.VBS und dem Risikomanagement VBS/Bund.

Gruppe Verteidigung

Die Gruppe Verteidigung bedankt sich für die Gelegenheit einer Stellungnahme zum "ISMS.VBS - Konformitätsaudit 2019". Wir sind dem Prüfbericht sowie den Empfehlungen einverstanden und unterstützen das GS-VBS bei der Umsetzung der Massnahmen und bringen unsere Erfahrungen gerne ein. Wir danken für die stets konstruktive und angenehme Zusammenarbeit. Speziell unterstützen wir die Fokussierung der Kräfte auf den Risikomanagementprozess, dessen Nachvollziehbarkeit in der Konsolidierung der Risiken und damit der erwarteten Verbesserung der Glaubwürdigkeit des ISMS.VBS.

armasuisse

Die Verantwortlichen der Informationssicherheit armasuisse unterstützen den Bericht und dessen Erkenntnisse vollumfänglich. Die armasuisse unterstützt insbesondere das Engagement und Zusammenarbeit im Bereich Reporting der Risiken und KPIs, dessen Nachvollziehbarkeiten in der Konsolidierung und damit der erwarteten Verbesserung der Glaubwürdigkeit des ISMS.VBS. Die armasuisse hat Ende August 2019 die Zertifizierung ISO 27001:2013 erfolgreich bestanden.

swisstopo

Die Implementierung eines übergeordneten ISMS auf Stufe Departement ist eine komplexe Aufgabe, die offensichtlich noch nicht zufriedenstellend gelöst werden konnte. Die Formulierung einer Hauptabweichung ist nachvollziehbar. Auf Stufe VE (z.B. für das ISMS.VBS.swisstopo) hat das ISMS sehr grosse Fortschritte bei der systematischen Risikobeurteilung im Informationssicherheitsbereich und bezüglich der Einhaltung der «Weisungen über die Informationssicherheit im VBS» gebracht. Von den aufgelisteten Nebenabweichungen ist zu beachten, dass viele Anforderungen auf Stufe der VE zu erfüllen sind. Hier hat das IOS keine direkte Ergebnisverantwortung, diese liegt beim Direktor der VE.

Bundesamt für Bevölkerungsschutz

Die dezentralen Departementsbereiche, so auch das BABS, tragen die Verantwortung für ihr eignes ISMS. Das BABS kommt dem nach. Das BABS braucht kein ISMS-VBS. Eine ungenügende Konsolidierung der Risiken im ISMS-VBS wäre auf Stufe GS VBS zu bereinigen. Allfällige Massnahmen sollen aber bei den dezentralen Departementsbereichen nicht zu einem Mehraufwand führen.

Bundesamt für Sport

Das BASPO teilt die Befunde wie auch das dargestellte Bild gemäss dem vorliegenden Prüfbericht. Die Aussage in Ziffer 3, dass die IOS für die Durchführung von Konformitätsaudits in den einzelnen Departementsbereichen des VBS (d.h. auf dezentraler Ebene) zuständig ist, ist zu streichen. Das ISMS BASPO ist ISO-zertifiziert. Somit ist durch das GS-VBS (IOS) allein zu prüfen, ob die aus den externen Audits hervorgehenden Empfehlungen im BASPO umgesetzt werden. Das BASPO hat alle Abweichungen ausgewiesen und die entsprechend notwendigen Massnahmen werden umgesetzt.