Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

18. Mai 2022

Prüfbericht «ISMS.VBS Audit 2021»

IT-Prüfung I 2021-09

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. Mai 2022

Prüfbericht «ISMS.VBS Audit 2021»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «ISMS.VBS Audit 2021» zukommen. Unsere Prüfungsarbeiten fanden zwischen Januar und März 2022 statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern besprochen. Die Stellungnahmen der Departementsbereiche zu unserem Bericht sind 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 jederzeit gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
– DU Chefin VBS

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

1 Das Informationssicherheits-Managementsystem (ISMS)

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 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 sollte jede Organisation einen vernünftigen Informationsschutz sowie eine angemessene Grundsicherung der IKT mit einem möglichst verhältnismässigen Einsatz von Mitteln sicherstellen.

Die internationale Norm ISO/IEC 27001 setzt die allgemein anerkannten Rahmenbedingungen für die Implementierung eines Informationssicherheits-Managementsystems (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.

ISO/IEC 27001 beschreibt ein ISMS als systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die kontinuierliche 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 handzuhaben.[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

In der Vergangenheit haben verschiedene Vorgänge gezeigt, dass im VBS die Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) sowie die Verfahren zur wirksamen und systematischen Umsetzung der Informationssicherheit weiterentwickelt und auf einen besseren Stand gebracht werden müssen. Im Rahmen des ISMS-Projektes wurden daher die diesbezüglichen Vorgaben und Prozesse überarbeitet und erneuert. Dieses Projekt wurde Ende 2017 abgeschlossen. Anschliessend ging das ISMS im ganzen VBS in den ordentlichen operativen Betrieb über.

[1] ISO - ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements (17.5.2022)

Heute wird das ISMS im VBS primär aus den dezentralen ISMS der Departementsbereiche betrieben. Dabei werden in einem strukturierten Zyklus die Risiken der jeweiligen Departementsbereiche bewirtschaftet und Massnahmen abgeleitet. Einige der dezentralen ISMS sind bereits heute ISO/IEC 27001 zertifiziert.

Das zentrale ISMS.VBS auf Departementsebene soll neu ausgerichtet und nicht mehr in der ursprünglich angedachten Form weitergeführt werden. Welche Aufgaben auf zentraler Ebene zukünftig noch wahrgenommen werden sollen, wird im Rahmen einer Standortbestimmung durch die Abteilung Digitalisierung und Cybersicherheit VBS (DCS) in Zusammenarbeit mit allen Departementsbereichen zurzeit erarbeitet.

3 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision VBS am 3. November 2021 den Auftrag, die Existenz und Wirksamkeit des ISMS.VBS auf Stufe Departement zu prüfen. Zudem soll der Umsetzungsstand der Massnahmen aus der Vorjahresprüfung «ISMS.VBS Audit 2020» beurteilt werden. Dazu haben wir eine strukturierte Befragung bei den Verantwortlichen des zentralen ISMS.VBS sowie bei Fachexperten aus den Departementsbereichen (dezentrale Ebene) durchgeführt.

Unsere Aufgabe war es nicht, ISMS-Konformitätsaudits in den einzelnen Departementsbereichen des VBS auf dezentraler Ebene durchzuführen. Auch stellt dieser Audit keine Zertifizierungsprüfung dar.

Aufgrund der geplanten Neuausrichtung im zentralen ISMS.VBS sehen wir davon ab, den Umsetzungsstand der offenen Massnahmen aus dem Jahr 2020 erneut zu überprüfen. Dieser Bericht fokussiert daher auf die aktuelle Situation.

4 Würdigung

Während unserer Prüfung trafen wir im ganzen Departement ausnahmslos engagierte Ansprechpersonen, 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 Feststellung und Beurteilung

5.1 Regelung der Verantwortung für die Sicherheit

Feststellung: Per 1. Januar 2020 wurden die «Weisungen über die Führung und Organisation der Sicherheit im VBS (WeFOS)»[2] in Kraft gesetzt. Die AKV für das Sicherheitsmanagement liegen in denjenigen Departementsbereichen, wo das entsprechende ISMS betrieben wird.

Beurteilung: Mit diesen Weisungen wurden die AKV im Bereich Sicherheit festgelegt und die Verantwortung für das Sicherheitsmanagement konsequent an die Departementsbereiche übertragen.

5.2 Standortbestimmung zum zentralen ISMS.VBS

Feststellung: Seit 2020 wird über eine Neuausrichtung des ISMS.VBS debattiert. Bis heute wurden allerdings kaum Fortschritte erzielt.

Die für das Jahr 2021 geplante Standortbestimmung zum zentralen ISMS.VBS durch die Abteilung DCS in Zusammenarbeit mit den Departementsbereichen ist immer noch in Erarbeitung. Darin wird festgehalten, welche Aufgaben und Rollen auf zentraler Ebene zukünftig wahrgenommen werden sollen. Zwischen Februar und Oktober 2021 haben dazu mit allen Sicherheitsverantwortlichen und Informationssicherheitsbeauftragten der Departementsbereiche des VBS sowie dem Risikomanagement VBS entsprechende Einzelgespräche und Workshops stattgefunden. Aufgrund der hohen Priorität des Informationssicherheitsgesetzes (ISG)[3] – u. a. mussten vier Ausführungsverordnungen[4] erarbeitet werden, welche bis Mitte 2023 in Kraft zu setzen sind – konnten die Arbeiten zur Standortbestimmung nicht wie geplant bis Ende Jahr fertiggestellt werden.

Der finale Bericht zur Standortbestimmung des ISMS.VBS lag zum Prüfungszeitpunkt noch nicht vor. DCS plant den Bericht zur Standortbestimmung des ISMS.VBS bis Ende Juni 2022 fertigzustellen.

Beurteilung: Aus Sicht der Internen Revision VBS muss diese Standortbestimmung des ISMS.VBS rasch abgeschlossen werden, damit die erforderliche Neuausrichtung zeitnah umgesetzt werden kann.

---

[2] Weisungen über die Führung und Organisation der Sicherheit im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport VBS vom 18.12.2019

[3] Die Bundesversammlung - Das Schweizer Parlament: 17.028 | Informationssicherheitsgesetz | Geschäft | Das Schweizer Parlament (17.5.2022)

[4] Informationssicherheitsverordnung (ISV), Identity & Access Management Verordnung (IAMV), Verordnung über die Personensicherheitsprüfungen und sinngemässe Prüfungen (VPSP) sowie Verordnung über das Betriebssicherheitsverfahren (VBSV)

5.3 ISO/IEC 27001-Zertifizierung

Feststellung: Der Auftrag der Chefin VBS zur Abklärung des Zeitbedarfs für eine Zertifizierung des ganzen VBS nach der Norm ISO/IEC 27001 wurde durchgeführt. Ende Mai 2021 wurde die Thematik im Rahmen der Konferenz der Sicherheitsverantwortlichen VBS behandelt. Dabei wurde festgehalten, dass eine Zertifizierung aus Sicht der Departementsbereiche frühestens per Ende 2024 möglich ist.

Beurteilung: Die beauftragte Abklärung zur Zertifizierung des gesamten Departementes nach der Norm ISO/IEC 27001 hat stattgefunden. Die Art und Weise der Umsetzung soll im Rahmen der Standortbestimmungen ISMS.VBS festgelegt werden.

6 Empfehlung

Aufgrund unserer Feststellungen empfehlen wir dem Generalsekretariat VBS,

Zu 5.2 den Bericht zur Standortbestimmung des zentralen ISMS.VBS bis Ende Juni 2022 abzuschliessen und die daraus abgeleiteten Massnahmen entsprechend umzusetzen.

7 Stellungnahmen

Generalsekretariat VBS
Das Generalsekretariat dankt der Internen Revision für die Gelegenheit zur Stellungnahme. Das zukünftige Tool muss die Neuausrichtung des ISMS unterstützen.

Nachrichtendienst des Bundes
Der NDB ist mit der Empfehlung des Prüfberichts einverstanden und hat keine weiteren Bemerkungen.

Gruppe Verteidigung
Die Gruppe Verteidigung bedankt sich für die Gelegenheit einer Stellungnahme zum Prüfbericht «ISMS.VBS Audit 2021». Wir unterstützen die im Bericht erwähnte Empfehlung vollumfänglich. Es ist aus unserer Sicht wichtig, dass geklärt wird, welche Aufgaben und Rollen auf zentraler Ebene wahrgenommen werden und wie das Reporting erfolgen soll. Dies insbesondere unter dem Aspekt der neu in Kraft gesetzten Informatik- & Digitalisierungs-Governance VBS (IKT-D GOV VBS) sowie den in der Ämterkonsultation stehenden Ausführungsverordnungen aus dem Informationssicherheitsgesetz (ISG).

armasuisse
Seitens armasuisse unterstützt man die im Prüfbericht angemerkten Themen. Vor allem ist es auch durch die aktuelle Bedrohungslage umso wichtiger, Informationssicherheit und die ISMS der einzelnen VE und des VBS durch einen Top-Down Ansatz zu betrachten. Weiterhin sollte die Kooperation in der Informationssicherheit erhöht werden.

swisstopo
swisstopo ist mit den Aussagen des Berichts einverstanden und hat keine ergänzenden Bemerkungen. Den Bericht zur Standortbestimmung des ISMS.VBS und dessen Weiterentwicklung werden wir mit Interesse lesen, insbesondere im Hinblick auf einen allfälligen Einsatz eines departementsweiten ISMS-Tools.

Bundesamt für Bevölkerungsschutz
Das BABS nimmt den Bericht zur Kenntnis und unterstützt die Empfehlungen der Internen Revision. Auf Grund der andauernden Restrukturierung des GS-VBS erstaunt es nicht, dass gegenüber dem Vorjahr kaum Fortschritte erzielt werden konnten. Da die Komplexität der Systeme stetig steigt ist es für uns unerlässlich, dass uns dafür rasch ein ISMS-Tool zur Verfügung gestellt wird.

Bundesamt für Sport
Das BASPO ist seit Jahren ISMS-zertifiziert, hat damit gute Erfahrungen gemacht und entwickelt das System kontinuierlich weiter. Am Grundsatz der dezentralen Zuständigkeit, wie sie die WeFOS vorsieht, ist festzuhalten. Das BASPO ist insofern mit der Empfehlung einverstanden, als dass die Standortbestimmung möglichst bald abgeschlossen werden soll. Bezüglich der Massnahmen erwartet das BASPO, dass die Verwaltungseinheiten in deren Erarbeitung bzw. Festlegung einbezogen werden.