



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Generalsekretariat VBS
Inspektorat VBS

21. April 2016



Prüfbericht «Vernetzte SAP-Systeme»

Abklärung A 054



Herr
Bundesrat Guy Parmelin
Chef VBS
Schwanengasse 2
3003 Bern



Bern, 21. April 2016

Abklärung «Vernetzte SAP-Systeme»

Sehr geehrter Herr Bundesrat Parmelin

Gerne lassen wir Ihnen unseren Prüfbericht zur Abklärung «Vernetzte SAP-Systeme» zukommen. Dem Auftrag entsprechend haben wir diese Thematik in den Departementsbereichen Verteidigung und armasuisse untersucht. Die Arbeiten sind zwischen September 2015 und Februar 2016 durchgeführt worden.

Sollten Sie Fragen zu diesem Dokument haben, stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

Inspektorat VBS



Verteiler

- GS VBS
- Verteidigung
- armasuisse





1 Einleitung

In Geschäftsbeziehungen zwischen Kunde und Lieferant werden zunehmend gegenseitig elektronische Daten ausgetauscht. Für diese wechselseitige Kommunikation sind die jeweiligen IKT-Systeme über sogenannte Schnittstellen miteinander verbunden. Auch das VBS unterhält solche Schnittstellen zu Lieferanten, damit die geforderten Warenlieferungen und Dienstleistungsbezüge effizient erfolgen können. Schnittstellen zu externen Firmen sind mit verschiedenen Risiken verbunden. Aus diesem Grund beauftragte uns der Chef VBS am 8. Mai 2015 aufzuzeigen, welche SAP-Schnittstellen zu externen Firmen das VBS unterhält und wie die technischen, sicherheitsrelevanten und vertraglichen Aspekte dieser Verbindungen gelöst sind.

An dieser Stelle bedanken wir uns bei all unseren Ansprechpersonen für die angenehme und konstruktive Zusammenarbeit.

2 Abgrenzungen

Im VBS existieren rund [REDACTED] SAP-Systeme, welche [REDACTED] Schnittstellen aufweisen. Im Rahmen dieser Abklärung legten wir den Fokus auf produktive SAP-Systeme im VBS, welche Schnittstellen zu externen Partnern aufweisen. Dabei beschränkten wir uns auf die so genannten Maschine-zu-Maschine Schnittstellen, die eine wechselseitige Interaktion automatisch gewährleisten. Einweg-Datenlieferungen aus VBS-SAP-Systemen an Drittpartner¹ sowie von Drittpartnern² in VBS-SAP-Systeme beurteilten wir in dieser Arbeit nicht. Unsere Prüfung ergab zudem, dass insgesamt zu [REDACTED] externen Partnern Maschine-zu-Maschine Schnittstellen bestehen, nämlich [REDACTED] sowie zum Bundesamt für Informatik und Telekommunikation (BIT). Letztere beurteilten wir als weniger risikobehaftet, da das BIT (wie das VBS) den Sicherheitsvorgaben der Bundesverwaltung unterliegt. Deshalb fokussierten wir nachfolgend ausschliesslich auf die Schnittstellen [REDACTED].

3 Prüfungshandlungen

Wir waren beauftragt, folgende Prüfaktivitäten durchzuführen:

- 1) Einschätzung der technischen und sicherheitsrelevanten Umsetzung sowie deren Kontrollen im Betrieb.
- 2) Beurteilung der vertraglichen Vereinbarungen mit den externen Partnern.
- 3) Aufzeigen von Optimierungsbedarf.

¹

[REDACTED]

²

[REDACTED]



Ergänzend führten wir Einhalteprüfungen durch.

Einleitend erlauben wir uns, eine kurze Übersicht bezüglich dem heutigen Stand zur Dokumentation der Schnittstellen im VBS zu geben.

4 Übersicht zu den Schnittstellen im VBS

Feststellungen: Im Rahmen unserer Arbeit konnten wir die bestehende Schnittstellenliste der FUB mit Stand vom 30. November 2015 einsehen. Dieses Dokument zeigt für SAP-Systeme insgesamt [REDACTED] Schnittstellen auf. Diesen ist in jedem Fall eine dokumentationsverantwortliche Person beim jeweiligen Leistungsbezüger zugewiesen. Befragungen dieser Personen haben jedoch ergeben, dass die Dokumentationsarbeiten in vielen Bereichen noch im Gange sind. Bezüglich SAP-Schnittstellen wurde von der Programmleitung BLSV / ar³ am 1. Mai 2015 der Auftrag erteilt, bis am 31. Dezember 2016 die Dokumentationsarbeiten abzuschliessen. Der Arbeitsfortschritt wird regelmässig durch die Prozessverantwortlichen an den Prozessausschuss rapportiert und von diesem überwacht. Das Reporting zeigt per 26. Februar 2016 folgenden Stand bezüglich den drei wesentlichen produktiven VBS-SAP-Systemen auf:

SAP System	Beschreibung	Anzahl identifizierte Schnittstellen	Erledigungsgrad
[REDACTED]	ERP System Verteidigung (V)	[REDACTED]	[REDACTED]
[REDACTED]	ERP System Non-V	[REDACTED]	[REDACTED]
[REDACTED]	ERP System Armeeapotheke	[REDACTED]	[REDACTED]

Beurteilungen: Die laufenden Arbeiten zur schriftlichen Dokumentation aller bestehenden Schnittstellen, unter Leitung der dokumentationsverantwortlichen Personen beim Leistungsbezüger, erachten wir als wichtig und notwendig, um eine abschliessende Übersicht zu erhalten. Die umfassende Dokumentation muss in enger Zusammenarbeit mit dem Leistungserbringer (z.B. der FUB) erfolgen. Dabei sind in jedem Fall der Bezug zum Geschäftsprozess, die technische Umsetzung sowie die relevanten Aspekte zu Risiken und Sicherheit verbindlich festzuhalten. Die zentrale und vollständige Dokumentation aller SAP-Schnittstellen im Solution Manager (SolMan)⁴ erachten wir als zielführend und sinnvoll. Dies ermöglicht zudem, dass nicht mehr produktive Schnittstellen identifiziert und allenfalls aufgehoben werden können.

Aufgrund der noch nicht abgeschlossenen Dokumentation aller Schnittstellen besteht aus unserer Sicht die Möglichkeit, dass heute bislang nicht identifizierte SAP-Schnittstellen zu Dritten existieren. Eine umfassende Dokumentation wird sicherstellen, dass die «Einfallstore» in die SAP-Systeme des VBS identifiziert und deren Risiken bewertet sind.

³ Betriebswirtschaftliche und logistische Systeme Verteidigung und armasuisse

⁴ Standard SAP Plattform für Application Lifecycle Management

5 Schnittstellen

5.1 Technische und sicherheitsrelevante Umsetzung

Feststellungen: Die technische Realisierung der SAP-Schnittstellen vom VBS wurde in den letzten Jahren mehrmals geändert und wird auch in Zukunft Technologiewechseln unterliegen. Heute kommen verschiedene schützenswerte Komponenten, wie zum Beispiel die Middleware⁵-Produkte und «», zum Einsatz. Technische Angaben zu diesen Komponenten können dem Anhang 1 entnommen werden.

Für sämtliche schützenswerte IKT-Komponenten muss gemäss den relevanten Bundesvorgaben⁸ ein gültiger Sicherheitsbericht (z.B. ein ISDS-Konzept) vorliegen. In einem solchen Sicherheitsbericht werden verschiedene Risiken identifiziert und bewertet. Diese werden anschliessend mit technischen, organisatorischen und anderen Massnahmen reduziert oder aber als Restrisiken ausgewiesen. Im Zuge unserer Arbeit haben wir die relevanten Sicherheitsberichte zu -Schnittstellen eingesehen und festgestellt, dass die Mehrheit der Dokumente in einer gültigen Form vorhanden sind. Der Sicherheitsbericht zu «» konnte uns nicht in einer unterzeichneten Version vorgelegt werden (es besteht jedoch eine Ausnahmegewilligung des Ausschusses für Informatiksicherheit des ISB⁹). Uns wurde zugesichert, dass die Unterzeichnung des Dokuments in absehbarer Zeit erfolgen wird.

Beurteilungen: und «» erachten wir als «State of the art»-Technologie, um Schnittstellen zwischen unterschiedlichen IKT-Systemen zu realisieren. Die technische Komplexität der Komponenten sowie der laufende Technologiewandel stellt die beteiligten VBS-Stellen vor gewisse Herausforderungen, die Sicherheitsdokumentation ständig à jour zu halten. Der nicht finalisierte Sicherheitsbericht deutet darauf hin, dass die bestehenden Bundesvorgaben zurzeit nicht vollumfänglich eingehalten werden.

5.2 Vertragliche Vereinbarungen

Feststellungen: Im Rahmen der geschäftlichen Tätigkeit werden über die oben erwähnten Schnittstellen wechselseitig geschäftliche Informationen zwischen VBS ausgetauscht und bearbeitet. Das Dokument «IKT-Grundschutz in der Bundesverwaltung»¹⁰ besagt, dass die Bearbeitung von geschäftlichen Informationen ausserhalb der Bundesverwal-

⁵ Vermittlungssoftware unterstützt die Kommunikation zwischen unterschiedlichen Anwendungen.

⁶ Produkt, das Datenaustausch zwischen Systemen ermöglicht.

⁷ ist eine Sicherheits- und Integrationsplattform, um IKT-Zugriffe zu steuern.

⁸ Weisungen über die IKT-Sicherheit in der Bundesverwaltung (WIsB) am 1. Juli 2015

⁹ Informatiksteuerungsorgan des Bundes (ISB)

¹⁰ IKT-Grundschutz in der Bundesverwaltung vom 19. Dezember 2013 (Stand am 1. März 2015)



tung nur aufgrund einer vertraglichen Regelung zulässig ist, welche die sicherheitsrelevanten Belange regelt. Eine solche vertragliche Regelung mit externen Partnern kann in Form einer Schnittstellenvereinbarung abgeschlossen werden. Diese beschreibt unter anderem Rahmenbedingungen, Aspekte zu Technik und Sicherheit sowie organisatorische Massnahmen zu den Schnittstellen.

Im Rahmen unserer Arbeiten konnte uns für die Schnittstellen mit eine Schnittstellenvereinbarung «SAP Logistik» vorgelegt werden. Das Dokument stammt aus dem Jahr 2013 und wurde von sowie unterzeichnet. Diese Schnittstellenvereinbarung basiert jedoch auf der heute nicht mehr verwendeten Technologie des «Lieferantenportals (LIPO)». Uns wurde zugesichert, dass ein überarbeitetes Dokument in absehbarer Zeit finalisiert und von beiden Vertragsparteien neu unterzeichnet wird.

Beurteilungen: Aus unserer Sicht besteht heute keine aktuelle Schnittstellenvereinbarung mit , welche die heute verwendete Technologie beschreibt. Dies deutet darauf hin, dass die bestehenden Bundesvorgaben zurzeit nicht vollumfänglich eingehalten werden.

6 Optimierungsbefund

Zusammenfassend leitend wir folgende Empfehlungen ab:

Wir empfehlen,

1) Zu Kapitel 4: die laufenden Arbeiten zur Dokumentation von SAP-Schnittstellen im Sol-Man fertig zu stellen (Zusammenarbeit von Leistungserbringer und Leistungsbezüger). Diese Dokumentation muss aus unserer Sicht den Bezug zum Geschäftsprozess, die technische Umsetzung sowie die relevanten Aspekte zu Risiken und Sicherheit verbindlich festhalten. Zudem erachten wir es als notwendig, die Dokumentation der Schnittstellen in Zukunft laufend zu bewirtschaften.

2) Zu Kapitel 5.1: für sämtliche schützenswerte Komponenten, welche die SAP-Schnittstelle unterstützen, entsprechende Sicherheitsdokumente (z.B. ISDS-Konzepte) erstellen und unterzeichnen zu lassen. Diese Dokumente sind à jour zu halten.

3) Zu Kapitel 5.2: die bestehende Schnittstellenvereinbarung zwischen VBS der aktuellen Technologie anzupassen und erneut von beiden Vertragsparteien unterzeichnen zu lassen. Das Dokument ist à jour zu halten.




7 **Stellungnahmen**

Empfehlung Nr. 1

Dokumentation der bestehenden Schnittstellen im VBS

Stellungnahme Verteidigung

Wir sind mit der Empfehlung einverstanden. Wie richtig aufgezeigt, wird an der korrekten und vollständigen Dokumentation der Schnittstellen im dafür vorgesehenen Werkzeug (SAP Solution Manager) mit Hochdruck gearbeitet. Bis Ende 2016 wird diese initiale Aufarbeitung der Schnittstellendokumentation aus heutiger Sicht abgeschlossen sein. Alle Schnittstellen basieren auf Schnittstellenvereinbarungen und -beschreibungen, die in der Verantwortung der Prozessverantwortlichen des Leistungsbezüger liegen.

Im täglichen Betrieb werden die Schnittstellendokumentationen jeweils im Rahmen des Change- und Release Management SAP aktuell gehalten und mindestens quartalsmässig durch  auf Vollständigkeit geprüft und evtl. Massnahmen befohlen. Verantwortlich für die vollständige und qualitativ richtige Erfassung der Schnittstellen bleibt die jeweils verantwortliche Prozessgruppe auf Leistungsbezügerseite in enger Zusammenarbeit mit dem Leistungserbringer FUB.

Stellungnahme armasuisse

Die Nachdokumentation der SAP Lösungen auf dem Solman inklusive der Schnittstellen, ist geplant per 31.12.2016 abzuschliessen. Gemäss des aktuellen Arbeitsstandes und der verfügbaren Ressourcen kann der Abschlusstermin gehalten werden.

Mit den Richtlinien (Quality Gates) im Bereich des Changemanagements welche letztes Jahr überarbeitet wurden und sich aktuell in der Implementierungsphase befinden, sowie der aktuell laufenden Überarbeitung der Richtlinien zum Projektvorgehen, bestehen ausreichend Vorgaben und Grundlagen zur nachhaltigen SAP Lösungsdokumentation im Solman.



Empfehlung Nr. 2

Sicherheitsdokumente [REDACTED]-Schnittstellen

Stellungnahme Verteidigung

Wir sind mit der Empfehlung einverstanden. Wie richtig aufgezeigt wurde, sind die ISDS Konzepte im Bereich der [REDACTED] grundsätzlich aktuell und gültig. Der Bereich der Maschinen-Maschinen Schnittstellen zu externen Partnern wird im Moment technologisch neu ausgerichtet, damit die Sicherheitswerkzeuge auch in Zukunft dem aktuellen Technologiestand entsprechen. Die Erarbeitung der Sicherheitsdokumente für SAP Schnittstellen zwischen FUB [REDACTED] werden im Rahmen der Entflechtungs- und Optimierungsarbeiten zwischen FUB [REDACTED] sowie im Rahmen der Verbesserungsarbeiten für die Übergänge zwischen [REDACTED] VBS sichergestellt. Diese Verbesserungsarbeiten werden vom GS VBS terminiert. Dies betrifft Sicherheitsdokumente für aktuell notwendige, bewirtschaftete sowie zukünftige SAP Schnittstellen. Für alte, abzulösende Systeme werden keine neuen Sicherheitsdokumente erstellt.

Die FUB baut die SAP Schnittstelle nach Anforderungen (inklusive der abgenommenen Sicherheitskonzepte) der Leistungsbezüger. Sie verantwortet auch die technische Realisierung und somit die Sicherheitsdokumente der eigenen technischen Komponenten.

Um den stetig schnelleren Technologiewandel auch in den Sicherheitsdokumenten zeitnah abzubilden, wird mit dem Projekt [REDACTED] des V eine flächendeckende und breit abgestützte Lösung gesucht.

Stellungnahme armasuisse

Gemäss heutigem Wissensstand weist die armasuisse keine Schnittstellen [REDACTED] aus. In Bezug zu den Vorgaben der ISDS Konzepte, werden diese seitens armasuisse für weitere Lieferanten oder Kunden angewendet.



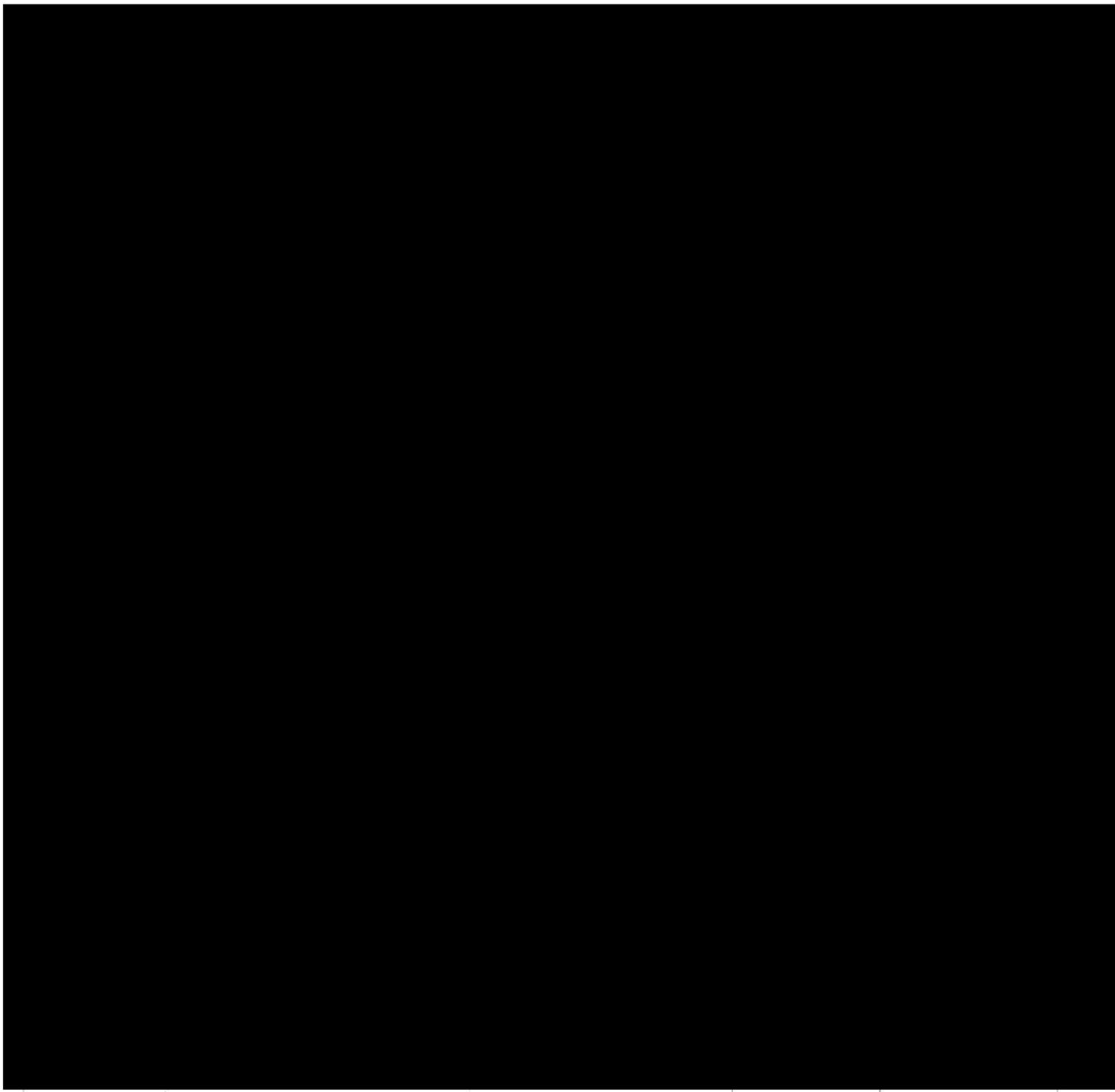
Empfehlung Nr. 3 Schnittstellenvereinbarung mit

Stellungnahme Verteidigung

Wir sind mit der Empfehlung einverstanden. Die SAP Schnittstellen werden aus technischen Gründen neu aufgesetzt. Entsprechende Vorarbeiten wie Inventarisierung der Schnittstellen, Analyse und Grobplanung sind initialisiert. Die Schnittstellenvereinbarungen mit sind auf Grund dieser diversen Änderungen in der Technologie aber auch im Prozess im Moment in Überarbeitung. Die Verantwortung im V liegt hier bei der LBA, da die LBA die vertraglichen Vereinbarungen mit getroffen hat und die Prozessverantwortung für die Logistikprozesse im V trägt. Ziel ist es, die Vereinbarungen nach Finalisierung der technischen Grundlagen durch die FUB bis spätestens Ende 2016 in unterschriebener Form (LBA) vorliegen zu haben.

Stellungnahme armasuisse

Gemäss heutigem Wissensstand weist die armasuisse keine Schnittstellen aus. In Bezug zu den Vorgaben der "Aktualität der Dokumentation" bspw. Schnittstellenvereinbarung, ISDS Konzepte, etc. werden diese seitens armasuisse für weitere Lieferanten oder Kunden angewendet.





A-Priority CH-3003 Bern

Herr Korpskommandant André Blattmann
Chef der Armee

Herr Martin Sonderegger
Rüstungschef

Referenz/Aktenzeichen:
Bern, 09.06.2016

Umsetzung der Empfehlungen aus der Abklärung «Vernetzte SAP-Systeme» (A 054)

Sehr geehrter Herr Korpskommandant
Sehr geehrter Herr Rüstungschef

Mit Mail vom 27. April 2016 stellte Ihnen die Interne Revision VBS den Prüfbericht zur oben erwähnten Abklärung zu. Wie Sie daraus entnehmen können, besteht bei der Dokumentation der SAP-Schnittstellen noch ein gewisser Handlungsbedarf.

Ich bitte Sie, die im Bericht aufgeführten Empfehlungen gemäss Ihren Stellungnahmen bis Ende 2016 umzusetzen.

Der jeweilige Stand der Umsetzung wird im Rahmen des Massnahmencontrollings erhoben.

Für Ihre Bemühungen bedanke ich mich.

Mit freundlichen Grüssen

Guy Parmelin
Bundesrat

z K an
GS
C IR VBS