EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung der Informatiksicherheit

RUAG MRO Holding AG

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.20431.997.00443
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Prüfung der Informatiksicherheit
RUAG MRO Holding AG

Das Wesentliche in Kürze

Am 21. März 2018 hat der Bundesrat beschlossen, die fast ausschliesslich für die Schweizer Armee tätigen Geschäftseinheiten der damaligen RUAG in einer neuen Konzerngesellschaft RUAG MRO Holding AG (MRO CH), resp. deren Tochtergesellschaft RUAG AG, zusammenzuführen. Diese Teile sollten von der übrigen RUAG (RUAG International), die international zivile und militärische Geschäfte tätigt, entflochten werden. Der Bundesrat verfolgte mit diesem Entscheid das Ziel, die Informatiksicherheit zu erhöhen und eine robuste, transparente und kostenoptimierte Leistungserbringung für die Armee sicherzustellen. Die MRO CH sollte ihre gesetzlich verankerte Zweckbestimmung – die Sicherstellung der Ausrüstung der Armee – weiterhin erfüllen und gleichzeitig die Möglichkeit haben, sich in den übrigen Geschäftsgebieten weiterzuentwickeln.

Die Entflechtung betraf auch die Informations- und Kommunikationstechnik (IKT) der RUAG. Es wurde entschieden, die IKT für die RUAG AG in die Verantwortung des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport zu geben. Die komplette IKT-Infrastruktur und die -Systeme wurden im Sicherheitsperimeter der Führungsunterstützungsbasis der Armee (FUB) neu aufgebaut und die Daten übernommen. Entsprechend müssen die IKT-Sicherheitsvorgaben des Bundes erfüllt werden. Das Entflechtungsprojekt verursacht Stand September 2020 voraussichtlich Kosten in der Höhe von 81–86 Millionen Franken. Von den bis Ende September aufgelaufenen Gesamtkosten von 57 Millionen sind 34 Millionen Franken der IKT-Entflechtung zuzuordnen Das Projekt betraf rund 2500 Mitarbeitende der MRO CH an über 20 Standorten der Schweiz.

Bei der vorliegenden Prüfung steht die Sicherheit der IKT-Systeme im Fokus und zwar hinsichtlich der kontrollierten Überführung zur RUAG AG und in den Sicherheitsperimeter der FUB.

Die Prüfung hat gezeigt, dass die Überführung der Systeme und Daten, trotz offener Nachfolgeprojekte, weitestgehend erfolgreich abgelaufen ist. Die IKT-Governance und -Sicherheitsorganisation sind zweckmässig aufgestellt, müssen aber noch umfangreiche Nacharbeiten leisten. Die Zusammenarbeit mit der FUB funktioniert, ist aber noch nicht eingeschliffen.

Erfolgreicher Abschluss der IKT-Entflechtung trotz hoher Komplexität und Verzögerungen

Nach der IKT-Entflechtung (erster Arbeitsschritt der Entflechtung) sollten künftig die Standardservices der FUB beansprucht werden. Aus diesem Grund wurden die Mitarbeitenden der RUAG AG mit neuen Büroautomationsgeräten der FUB ausgerüstet. Der für den 1. Januar 2020 geplante Übergang in die neue Umgebung konnte aufgrund verschiedener Umstände nicht eingehalten werden. Die Migration erfolgte daher verspätet an Ostern 2020. Per Ende April 2020 konnte der IT-Cutover abgeschlossen werden und per Ende Juni 2020 wurde der erste Arbeitsschritt der Entflechtung abgeschlossen. Die Projektziele wurden erreicht.

Eine grosse Herausforderung stellte der Datentransfer dar. Um die Verschleppung von Malware auszuschliessen, durften keine Daten direkt von den Systemen der alten RUAG zur FUB kopiert werden. Daher wurden diese über eine eigens dafür eingerichtete Datenleitung

in einen Quarantänebereich der FUB transferiert, dort auf Malware gescannt und danach auf die neuen Systeme übertragen.

Für die Bereinigung der Daten auf den alten Systemen hat die MRO CH im Rahmen des zweiten Arbeitsschritts der Entflechtung ein weiteres Projekt lanciert. Hierbei sollen die militärisch relevanten und vertraulichen Daten auf den Altsystemen gelöscht oder unkenntlich gemacht werden. Dabei ist es von grosser Wichtigkeit, dass auch Archive und Datensicherungen im Fokus der Bereinigung stehen. Das Projekt erfolgt in enger Zusammenarbeit mit der RUAG International. Die RUAG AG ist als Dateninhaberin für die Bereinigung verantwortlich.

Die Technisch Wissenschaftliche Infrastruktur (TWI) wird ebenfalls im Rahmen des zweiten Arbeitsschritts bis Ende 2021 in einen sicheren Zustand überführt. Die Verantwortung und der Betrieb liegen bei der RUAG AG.

Die neue Sicherheitsorganisation der RUAG AG ist zielführend aufgebaut

Die Sicherheitsorganisation der RUAG AG ist zweckmässig aufgestellt. Durch die Einbindung von Sicherheitsbeauftragten in den Fachbereichen ist ein durchgängiger Informationsaustausch gewährleistet. Die unterschiedlichen Teilbereiche sind gut aufeinander abgestimmt und der Austausch mit dem Management ist sichergestellt. Ein regelmässiger Austausch mit der Sicherheitsorganisation der FUB ist etabliert.

Der Aufbau eines Informationssicherheitsmanagementsystems inklusive der Audittätigkeiten tragen zu einer nachhaltigen Informationssicherheit bei. Das Risikomanagement und das betriebliche Kontinuitätsmanagement sind im Aufbau. Letzteres soll erst 2023 operativ werden. Hier sollte die RUAG AG, mindestens für die wichtigsten Geschäftsprozesse, eine raschere Lösung erarbeiten.

Einzelne Aspekte in der Betriebssicherheit müssen verbessert werden

Der Betrieb der Systeme der RUAG AG ist nach der Migration in der Verantwortung der FUB. Die Sicherheitsüberwachung erfolgt durch deren Security Operations Center. Bei der Einbindung der Systeme in die neue Umgebung wurden keine flächendeckenden Sicherheitskonformitätsprüfungen durchgeführt. Dadurch besteht, insbesondere bei Anwendungen mit Zugang zum Internet, ein erhebliches Risiko. Die FUB sollte diese Sicherheitskonformitätsprüfungen konsequent durchführen.

Mit dem Übergang in die Governance der Bundesverwaltung unterliegt die RUAG AG den Vorgaben des Bundes. Daher mussten für gewisse Anwendungsfälle Ausnahmen zum IKT-Grundschutz beantragt werden. Diese gilt es, wo möglich, abzubauen oder andernfalls noch zu formalisieren.

Die Empfehlungen der EFK aus früheren Berichten sind weitgehend umgesetzt

Die Empfehlungen der EFK aus den Berichten 18517 und 19418 wurden, soweit sie die MRO CH betreffen, weitgehend umgesetzt. Für die zum Prüfzeitpunkt noch offenen zwei Empfehlungen wurden Projektorganisationen aufgebaut und die Arbeiten sind am Laufen. Die Bereinigung der Sicherheitsdokumentationen (Empfehlung 19418.002) weist einen Erfüllungsgrad von 60 % auf und soll per Ende 2020 abgeschlossen werden. Bei der Überführung der TWI in einen sicheren Perimeter (Empfehlung 19418.003) wurden die Zielarchitektur und die Serviceleistungen spezifiziert. Das erforderliche Rechenzentrum ist in Betrieb. Das Projekt soll bis Ende 2021 abgeschlossen werden.

Audit de la sécurité informatique
RUAG MRO Holding SA

L'essentiel en bref

Le 21 mars 2018, le Conseil fédéral a décidé de regrouper les unités d'affaires de l'ancienne entreprise RUAG, actives presque exclusivement pour l'armée suisse, dans une nouvelle société du groupe RUAG MRO Holding SA (MRO CH), respectivement sa filiale RUAG SA. Il s'agissait de dissocier ces unités du reste du groupe RUAG (RUAG International) qui réalise des activités tant civiles que militaires au niveau international. Avec cette décision, le Conseil fédéral entendait améliorer la sécurité informatique et assurer à l'armée une fourniture de prestations robuste, transparente et optimisée en termes de coûts. Tout en s'acquittant de sa mission ancrée dans la loi – garantir l'équipement de l'armée – MRO CH devrait avoir la possibilité de poursuivre son développement dans d'autres domaines d'activité.

La scission concernait aussi les technologies de l'information et de la communication (TIC) de RUAG. Le Département fédéral de la défense, de la protection de la population et des sports s'est vu confier la responsabilité des TIC de RUAG SA. Toute l'infrastructure et les systèmes TIC ont été réorganisés et les données reprises dans le périmètre de sécurité de la Base d'aide au commandement de l'armée (BAC). En conséquence, les normes de sécurité informatique de la Confédération doivent être remplies. Le projet de dissociation générera des coûts à hauteur de 81 à 86 millions de francs, selon une estimation de septembre 2020. Sur les 57 millions dépensés jusqu'à fin septembre, 34 millions sont imputables à la scission des TIC. Le projet concerne près de 2500 collaborateurs de MRO CH sur plus de 20 sites en Suisse.

Le présent audit s'est concentré sur la sécurité des systèmes TIC, soit sur le transfert contrôlé au sein de RUAG SA et dans le périmètre de sécurité de la BAC.

L'audit a montré que le transfert des systèmes et des données s'est, dans une large mesure, bien passé, même si les projets subséquents ne sont pas terminés. La gouvernance informatique et l'organisation en matière de sécurité informatique sont adéquates, mais d'importants travaux d'ajustement restent nécessaires. La collaboration avec la BAC fonctionne, mais n'est pas encore bien huilée.

Succès de la scission des TIC malgré la complexité du projet et les retards

Après la scission des TIC (première étape), les services standard de la BAC devraient être utilisés. Par conséquent, les employés de RUAG SA ont reçu de nouveaux appareils de bureautique de la BAC. Prévu pour le 1er janvier 2020, le déploiement n'a pas pu être respecté pour diverses raisons. La migration a été reportée à Pâques 2020. Fin avril 2020, le changement de système *(cut-over)* a pu être finalisé, la première étape de la scission a été achevée à la fin juin 2020. Les objectifs du projet ont été atteints.

Le transfert des données constituait un sérieux défi. Pour exclure toute propagation de maliciels, il n'était pas permis de copier les données directement des systèmes de l'ancienne entreprise RUAG dans ceux de la BAC. Les données ont donc été transférées dans une zone de quarantaine de la BAC via une ligne de données spécialement créée où elles ont fait l'objet d'une analyse antivirus, avant d'être transférées dans les nouveaux systèmes.

MRO CH a lancé un autre projet pour nettoyer les données de ses anciens systèmes dans le cadre de la seconde étape du processus de dissociation. Il consiste à effacer les données à caractère militaire et confidentielles des anciens systèmes ou à les rendre illisibles. Il est crucial qu'un tel nettoyage inclue les archives et les copies de sauvegarde. Le projet est mené en étroite collaboration avec RUAG International. Le nettoyage des données est placé sous la responsabilité de RUAG SA, qui en est propriétaire.

Dans cette seconde étape, qui se poursuivra jusqu'à la fin de 2021, il s'agit aussi de mettre en sécurité l'infrastructure scientifique et technique. La responsabilité et l'exploitations incombent à RUAG SA.

La nouvelle organisation de sécurité de RUAG SA est structurée de manière efficace

L'organisation de sécurité de RUAG SA est adéquate. L'implication de responsables de la sécurité dans différents domaines assure un échange constant d'informations. Les divers secteurs sont bien coordonnés et les échanges avec la direction sont garantis. Des échanges réguliers avec l'organisation de sécurité de la BAC sont établis.

La mise en place d'un système de gestion de la sécurité de l'information avec les activités d'audit contribuent à une sécurité de l'information sur le long terme. La gestion des risques et la gestion de la continuité des activités sont en cours de réalisation. La seconde ne deviendra opérationnelle qu'en 2023. RUAG SA devrait trouver ici une solution plus rapide, au moins pour ses principaux processus d'affaires.

Besoins d'amélioration ponctuels au niveau de la sécurité d'exploitation

L'exploitation des systèmes de RUAG SA est du ressort de la BAC depuis la migration. Les contrôles de sécurité sont effectués par le Centre des opérations de sécurité *(Security Operations Center)*. Lors de l'intégration des systèmes dans leur nouvel environnement, aucun contrôle de conformité en matière de sécurité à large échelle n'a été réalisé. Cela représente un risque important, surtout pour les applications reliées à Internet. La BAC devrait effectuer de tels contrôles de conformité en matière de sécurité de manière systématique.

Depuis que sa gouvernance incombe à l'administration fédérale, RUAG SA est soumise aux directives de la Confédération. Ainsi, il a fallu demander pour certaines applications des dérogations à la protection de base des TIC. Ces dernières devraient être supprimées autant que possible ou, à défaut, formalisées.

Les recommandations émises par le CDF dans ses précédents rapports sont pour la plupart mises en œuvre

Les recommandations du CDF des rapports 18517 et 19418 ont été en bonne partie suivies, dans la mesure où elles concernent MRO CH. Des organisations de projet ont été mises en place pour les deux recommandations encore en suspens au moment de l'audit et les travaux sont en cours. La mise à jour des documentations de sécurité (recommandation 19418.002) était réalisée à 60 % et devrait être terminée d'ici fin 2020. Lors du transfert de l'infrastructure scientifique et technique dans un périmètre de sécurité (recommandation 19418.003), l'architecture cible et les prestations ont été définies. Le centre de calcul requis est opérationnel, et le projet devrait être achevé d'ici fin 2021.

Texte original en allemand

Verifica della sicurezza informatica
RUAG MRO Holding SA

L'essenziale in breve

Il 21 marzo 2018 il Consiglio federale ha deciso di riunire le unità operative dell'ex RUAG, attive quasi esclusivamente per l'Esercito svizzero, in una nuova società del gruppo, la RUAG MRO Holding SA (MRO CH), ovvero la società affiliata RUAG SA. Lo scopo era scorporare tali unità dal resto del gruppo RUAG (RUAG International), che svolge attività sia civili che militari a livello internazionale. Con questa decisione, il Consiglio federale ha perseguito l'obiettivo di aumentare la sicurezza informatica e garantire all'esercito una fornitura di prestazioni solida, trasparente e ottimizzata sotto il profilo dei costi. La MRO CH dovrebbe continuare ad adempiere al suo scopo sancito dalla legge, ovvero garantire l'equipaggiamento dell'esercito, e nel contempo avere l'opportunità di svilupparsi ulteriormente negli altri ambiti di attività.

Lo scorporo interessava anche le tecnologie dell'informazione e della comunicazione (TIC) di RUAG. È stato deciso di affidare la responsabilità delle TIC di RUAG SA al Dipartimento federale della difesa, della protezione della popolazione e dello sport. L'intera infrastruttura e i sistemi TIC sono stati riorganizzati e i dati ripresi nel perimetro di sicurezza della Base d'aiuto alla condotta (BAC) dell'esercito. Di conseguenza, i requisiti in materia di sicurezza TIC della Confederazione devono essere soddisfatti. Secondo una stima di settembre 2020, il progetto di scorporo comporta costi dell'ordine di 81–86 milioni di franchi. Dei costi totali pari a 57 milioni di franchi sostenuti fino a fine settembre, 34 milioni sono attribuibili allo scorporo delle TIC. Il progetto ha interessato circa 2500 collaboratori di MRO CH attivi in oltre 20 sedi in Svizzera.

La presente verifica è incentrata sulla sicurezza dei sistemi TIC, ovvero sul trasferimento monitorato in RUAG SA e nel perimetro di sicurezza della BAC.

Dalla verifica è emerso che il trasferimento dei sistemi e dei dati è ampiamente riuscito, nonostante i progetti successivi ancora in sospeso. La governance e l'organizzazione in materia di sicurezza delle TIC sono adeguate, ma necessitano ancora di importanti interventi successivi. La collaborazione con la BAC funziona, ma è ancora in fase di rodaggio.

Lo scorporo delle TIC è stato concluso con successo, malgrado l'elevata complessità del progetto e i ritardi

Dopo lo scorporo delle TIC (prima fase), i servizi standard della BAC dovrebbero essere utilizzati in futuro. Per questo motivo, i collaboratori di RUAG SA sono stati dotati di nuovi apparecchi di burotica della BAC. Il trasferimento nel nuovo ambiente, previsto per il 1° gennaio 2020, non ha potuto essere attuato a causa di diverse circostanze. La migrazione è quindi stata posticipata alla Pasqua 2020. Alla fine di aprile 2020 è stato completato il cambiamento di sistema *(cutover)* e la relativa prima fase è stata conclusa entro fine giugno 2020. Gli obiettivi del progetto sono stati raggiunti.

Il trasferimento dei dati ha rappresentato una grande sfida. Per evitare la diffusione di malware, non era permesso copiare dati direttamente dai sistemi dell'ex RUAG in quelli della BAC. Pertanto, i dati sono stati trasferiti in un'area di quarantena della BAC attraverso un

canale appositamente predisposto, dove vengono sottoposti a un'analisi antivirus prima di essere trasferiti nei nuovi sistemi.

Per ripulire i dati dai vecchi sistemi, MRO CH ha lanciato un altro progetto come parte della seconda fase del processo di scorporo. In questo processo, i dati rilevanti e confidenziali in ambito militare devono essere cancellati dai vecchi sistemi o resi irriconoscibili. È quindi di fondamentale importanza che anche gli archivi e i backup dei dati vengano ripuliti. Il progetto è condotto in stretta collaborazione con RUAG International. In qualità di detentrice dei dati, la loro pulizia spetta a RUAG SA.

Nella seconda fase, che si concluderà entro fine 2021, verrà messa in sicurezza anche l'infrastruttura tecnico–scientifica. In tale ambito, la responsabilità e l'esercizio competono a RUAG SA.

La nuova organizzazione della sicurezza di RUAG SA è strutturata in modo mirato

L'organizzazione della sicurezza di RUAG SA è adeguata. Siccome l'organizzazione include gli incaricati della sicurezza negli ambiti specializzati, lo scambio continuo di informazioni è garantito. I diversi settori parziali sono ben coordinati fra loro e gli scambi con la direzione garantiti. Vi sono inoltre scambi regolari con l'organizzazione della sicurezza della BAC.

La creazione di un sistema di gestione della sicurezza delle informazioni, comprese le attività di verifica, contribuiscono alla sicurezza sostenibile delle informazioni. La gestione dei rischi e quella della continuità operativa sono in fase di realizzazione. La gestione della continuità operativa verrà attuata soltanto nel 2023. Al riguardo, RUAG SA dovrebbe elaborare una soluzione più rapida, perlomeno per i processi aziendali più importanti.

Alcuni aspetti della sicurezza operativa devono essere migliorati

Dopo la migrazione, l'esercizio dei sistemi di RUAG SA spetta alla BAC. La vigilanza sulla sicurezza è garantita dal Centro operativo di sicurezza *(Security Operations Center)*. Tuttavia, all'atto dell'integrazione dei sistemi nel nuovo ambiente, non sono state effettuate verifiche della conformità in materia di sicurezza su ampia scala. Ne consegue un notevole rischio, in particolare per le applicazioni con accesso a Internet. La BAC dovrebbe eseguire sistematicamente verifiche della conformità in materia di sicurezza.

Con il passaggio della sua governance all'Amministrazione federale, RUAG SA soggiace alle direttive della Confederazione. Per determinati casi d'applicazione, è stato quindi necessario chiedere delle deroghe alla protezione di base delle TIC. Laddove possibile, queste deroghe devono essere eliminate o essere almeno ancora formalizzate.

Le raccomandazioni del CDF formulate nei precedenti rapporti sono ampiamente attuate

Le raccomandazioni formulate dal CDF nei rapporti 18517 e 19418 sono state ampiamente attuate, nella misura in cui interessano MRO CH. Per quanto concerne le due raccomandazioni ancora da attuare al momento della verifica, sono state create organizzazioni di progetto e i lavori sono in corso. La pulizia degli incarti della sicurezza (raccomandazione 19418.002) ha raggiunto il 60 per cento e dovrebbe concludersi entro fine 2020. Riguardo al trasferimento dell'infrastruttura tecnico–scientifica in un perimetro di sicurezza (raccomandazione 19418.003), sono state definite l'architettura finale e le prestazioni di servizio. Il necessario centro di calcolo è operativo e il progetto dovrebbe essere concluso entro fine 2021.

Testo originale in tedesco

Audit of information security
RUAG MRO Holding AG

Key facts

On 21 March 2018, the Federal Council decided to reconfigure those business units of RUAG (as it was then known) that work almost exclusively for the Swiss Armed Forces into a new group company, RUAG MRO Holding AG (MRO CH), and a subsidiary, RUAG AG. These units were to be split from the rest of RUAG (RUAG International), which conducts international civil and military business. The Federal Council's decision was aimed at increasing information security and ensuring robust, transparent service provision for the Armed Forces at optimal cost. It was planned that MRO CH would continue performing its statutory mandate – ensuring the provision of equipment to the Armed Forces – while having the opportunity to expand its business in other areas.

The split also involved RUAG's information and communications technology (ICT). It was decided to transfer responsibility for RUAG AG's ICT to the Federal Department of Defence, Civil Protection and Sport. The complete ICT infrastructure and systems were recreated within the security perimeter of the Armed Forces Command Support Organisation (AFCSO) and the data was migrated. Accordingly, the federal ICT security requirements have to be observed. As at September 2020, the cost of the splitting project is estimated at CHF 81–86 million. Of the CHF 57 million in total costs incurred up to the end of September, CHF 34 million was attributable to the ICT split. The project involved around 2,500 MRO CH employees at over 20 locations across Switzerland.

This audit focuses on the security of the ICT systems, specifically on the controlled migration to RUAG AG and into the AFCSO security perimeter.

The audit showed that the migration of systems and data has been largely successful, despite a number of pending legacy projects. The ICT governance and security organisation are appropriately structured, but substantial corrective actions are still necessary. Collaboration with the AFCSO is working but is not yet running completely smoothly.

ICT split successfully completed, despite complexity and delays

Following the ICT split (first stage of the overall demerger), AFCSO's standard services are to be used in future. RUAG AG's employees were therefore equipped with new office automation devices from the AFCSO. For various reasons, the migration to the new environment could not take place on 1 January 2020 as planned, but was instead delayed until Easter 2020. At the end of April 2020, the IT cutover was finished, and the first stage in the split was completed at the end of June 2020. The project objectives were achieved.

The data migration presented a major challenge. To prevent the carry-over of malware, it was not permitted to copy any data directly from the old RUAG AG systems to the AFCSO. The data was therefore transferred via a dedicated data line to a quarantined zone of the AFCSO, where it was scanned for malware before being migrated to the new systems.

In the second stage, MRO CH launched another project to clean up the data on the old systems. The strategic and confidential military data was to be deleted or rendered

unintelligible. In this regard, it was very important that archives and data backups were also included in the cleanup. The project is being carried out in close collaboration with RUAG International. RUAG AG, as the data owner, is responsible for the cleanup.

The technical scientific infrastructure (TSI) will also be migrated to a secure status by the end of 2021 as part of stage two. Responsibility for this, and for operation, lies with RUAG AG.

RUAG AG's new security organisation is appropriately structured

The structure of RUAG AG's security organisation is appropriate. Through the involvement of IT security officers from the specialist areas, the end-to-end exchange of information was ensured. The various sub-areas work well together and liaison with management is ensured. A regular exchange with the AFCSO's security organisation has been established.

Setting up an information security management system, including audit activities, contributes to sustainable information security. The risk management and business continuity management are in the process of being set up, with the latter not due to become operational until 2023. In this regard, RUAG AG should find a faster solution, at least for the most important business processes.

Individual aspects of operational security need to be improved

After the migration, the AFCSO will be responsible for operating RUAG AG's systems. Security monitoring is performed by its Security Operations Centre. No comprehensive security compliance testing was performed when the systems were integrated into the new environment. This poses a significant risk, especially for applications with internet access. The AFCSO should consistently perform these security compliance tests.

Having become part of the Federal Administration's governance, RUAG AG is now subject to federal requirements. As a result, exceptions to ICT basic protection have had to be requested for certain application scenarios. Where possible, these should be removed; otherwise, they should be formalised.

The SFAO's recommendations from earlier reports have largely been implemented

The SFAO's recommendations from mandates 18517 and 19418, insofar as they apply to MRO CH, have largely been implemented. Project organisations have been set up to address the two recommendations that were outstanding at the time of the audit, and work is under way. The cleanup of security documentation (recommendation 19418.002) is 60% complete and should be fully complete by end-2020. As regards the migration of the TSI to a secure perimeter (recommendation 19418.003), the target architecture and the service activities have been defined. The requisite data centre has entered operation. The project is due to be completed by the end of 2021.

Original text in German

Generelle Stellungnahme der Geprüften

RUAG MRO Holding AG

Die RUAG MRO Holding AG begrüsst die von der EFK kurz nach der Entflechtung durchgeführte Prüfung der Informatiksicherheit und bedankt sich bei der EFK für den detaillierten Prüfbericht. RUAG MRO ist mit den darin enthaltenen Empfehlungen einverstanden und wird diese umsetzen.

Ein wesentliches Ziel der Entflechtung bestand in der Trennung der IKT, wobei RUAG MRO in den Sicherheitsperimeter der FUB zu integrieren war. RUAG MRO hat grosse Anstrengungen unternommen, um dieses Ziel mitzutragen und zu erreichen. Trotz der hohen Anforderungen konnte der IT-Cutover per Ende April 2020 und der IKT-Transfer (sog. erster Arbeitsschritt der Entflechtung) Ende Juni 2020 erfolgreich abgeschlossen werden. Die Projektziele wurden, wie von der EFK festgehalten, erreicht und die geplanten Folgeprojekte (sog. zweiter Arbeitsschritt der Entflechtung) nahtlos lanciert. RUAG MRO weist übereinstimmend mit der EFK darauf hin, dass im Rahmen dieses zweiten Arbeitsschrittes anspruchsvolle Folgearbeiten zu leisten sind, namentlich die Datenbereinigung auf den alten Systemen und die Migration der TWI.

Die Entflechtung machte im Zuge der Neugründung der RUAG MRO Holding AG einen «Neustart» erforderlich. Parallel zur Entflechtung war RUAG MRO im vergangenen Jahr daher intensiv mit dem Aufbau einer Sicherheitsorganisation und der Implementierung eines eigenen ISMS befasst. Die Sicherheitsorganisation steht und RUAG MRO fühlt sich durch die Feststellungen der EFK im eingeschlagenen Weg bekräftigt. Im ISMS-Projekt konnten bis Mitte Februar 2021 die Schutzbedarfsanalysen zu allen Schutzobjekten vollständig erstellt werden, die Weiterentwicklung der Richtlinien ist im Gang. Das gesamte Projekt soll bis Ende 2022 umgesetzt und operativ sein.

Führungsunterstützungsbasis (FUB)

Wir danken für den detaillierten Prüfbericht und für die Möglichkeit der Stellungnahme und sind mit der enthaltenen Empfehlung für die FUB einverstanden. Durch die Entflechtung der RUAG AG und dem kompletten Neuaufbau der IKT-Infrastruktur und -Systeme im Sicherheitsperimeter der Führungsunterstützungsbasis der Armee (FUB) sowie der Datenübernahme nach kompletter Überprüfung auf Malware sind die RUAG MRO Holding AG und die FUB partnerschaftlich sehr eng miteinander verbunden. Die Sicherheit in der Informatik ist eines der höchsten Güter für die Sicherheitsorganisationen der Schweiz in der heutigen Zeit. Die FUB wird deshalb alles daran setzten, dass die Sicherheit der Informatik generell und in der partnerschaftlichen Zusammenarbeit mit der RUAG MRO Holding AG im Speziellen gewährt werden kann.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Am 21. März 2018 hat der Bundesrat beschlossen, die fast ausschliesslich für die Schweizer Armee tätigen Geschäftseinheiten der alten RUAG Holding AG in einer neuen Konzerngesellschaft zusammenzuführen und von den übrigen Teilen, welche weltweit zivile und internationale militärische Geschäfte tätigen, zu entflechten. Der Bundesrat verfolgte mit diesem Entscheid das Ziel, die Informatiksicherheit zu erhöhen und eine robuste, transparente und kostenoptimierte Leistungserbringung für die Armee sicherzustellen.

Am 15. November 2019 wurden die dazu nötigen neuen Gesellschaften gegründet: die BRGB Holding AG als Dachgesellschaft und die Subholding RUAG MRO Holding AG [1] mit der RUAG AG sowie die Subholding RUAG International Holding AG. Die neue Subholdingstruktur wurde ab dem 1. Januar 2020 operativ.

Die Entflechtung erforderte auch die Aufteilung der Informatiksysteme. Es wurde entschieden, den Aufbau einer eigenen IKT für die RUAG AG, innerhalb des Sicherheitsperimeters des VBS weiter zu verfolgen. Die komplette Infrastruktur und die Systeme wurden daher in den Sicherheitsperimeter der FUB verschoben. Entsprechend müssen die Sicherheitsvorgaben des Bundes, d. h. die Bundesinformatikverordnung (BinfV) und alle damit verbundenen Weisungen bzw. Standards von der RUAG AG erfüllt werden.

Vom Transfer in den Perimeter der FUB ist einzig die RUAG AG betroffen (siehe Abbildung 1: Organisation der BGRB Holding AG, rote Darstellung). RUAG Real Estate, RUAG GmbH sowie RUAG Inc. sind indirekt betroffen, da sie teilweise Zugriff auf Informationen der RUAG AG benötigen. Der Austausch dieser Informationen erfolgte zum Prüfzeitpunkt über E-Mail, Secure File Transfer Service oder ein Sharepoint Portal des VBS. Es existieren keine direkten Zugriffe auf Applikationen oder Verbindungen auf Systeme der RUAG AG. Die übrigen Unternehmen sind vom Transfer nicht betroffen.

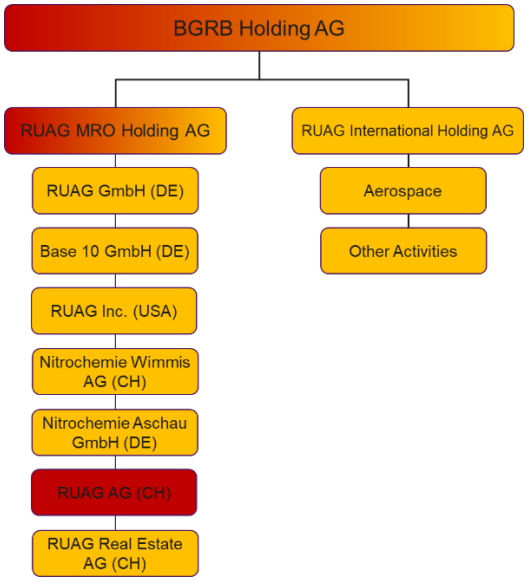


Abbildung 1: Organisation der BGRB Holding AG

[1] MRO = Maintenance Repair Overhaul, damaliger Arbeitstitel

Die EFK führte die Prüfung im Auftrag der Finanzdelegation durch. Der Bericht untersteht nicht dem Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung, sondern dem Parlamentsgesetz.

1.2 Prüfungsziel und -fragen

Die Prüfung soll der RUAG MRO CH aufzeigen, wie sie hinsichtlich der Umsetzung der Sicherheitsanforderungen im Perimeter der FUB positioniert ist und wo es Verbesserungsbedarf gibt. Ziel der Prüfung ist die Beurteilung der Informationssicherheit bei RUAG MRO Holding AG nach der Migration in den Sicherheitsperimeter der FUB.

1. Sind die Informationssicherheitsmassnahmen gemäss den Vorgaben des Bundes, des VBS und auch gegenüber internationalen Vorschriften (z. B. ITAR) umgesetzt?
2. Ist die Governance im Bereich der Informationssicherheit zweckmässig und wirksam?
3. Sind die für die RUAG MRO Holding AG relevanten Empfehlungen aus den Berichten 18517 und 19418 umgesetzt oder auf Kurs?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Roland Gafner (Revisionsleiter) und Christian Brunner vom 19. Oktober bis 20. November 2020 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Die RUAG AG hat entschieden, die Security Governance des VBS als Basis für die eigenen Sicherheitsrichtlinien zu verwenden. Die Beurteilungen orientieren sich daher an der Informationsschutzverordnung (IschV) und den Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB) sowie am Standard ISO/IEC 27001 und 27002.

Die RUAG Real Estate AG betreibt das umfassende Gebäudemanagement für die Infrastruktur und Technik der Räumlichkeiten der RUAG AG. In diesen Bereich fallen unter anderem die Systeme für die Zutrittsregelung in die verschiedenen geschützten Bereiche. Die physische Zutrittskontrolle stellt einen wichtigen Aspekt der Informationssicherheit dar. Da die RUAG Real Estate AG nicht im Fokus der Prüfung stand, kann im Bericht kein abschliessendes Urteil bezüglich der physischen und umgebungsbezogenen Sicherheit wiedergegeben werden.

Die Ergebnisbesprechung hat am 18. Dezember 2020 stattgefunden. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von der RUAG AG, der FUB und vom Bundesamt für Informatik und Telekommunikation (BIT) umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 3. Februar 2021 statt. Teilgenommen haben seitens RUAG der Vizepräsident des Verwaltungsrates, ein Verwaltungsratsmitglied, der Chief Executive Officer, der Chief Information Security Officer und die Information Security Auditorin. Die FUB wurde durch den Chief Information Security Officer vertreten. Für das GS-VBS hat die Chefin Eignerpolitik teilgenommen. Seitens der EFK haben der zuständige Mandatsleiter, der Federführende und der Revisionsleiter teilgenommen.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung der Geschäftsleitung (GL) bzw. dem Verwaltungsrat der RUAG AG und für die FUB der Amtsleitung bzw. dem Generalsekretariat obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Entflechtung der Informatik der RUAG AG

2.1 Die Projektziele wurden qualitativ und quantitativ erreicht

Im Oktober 2018 ist die Programmorganisation zur Steuerung und Umsetzung der vom Bundesrat beschlossenen Entflechtung MRO CH definiert worden. Das übergeordnete Ziel war das Separieren der damaligen RUAG Corporate IKT-Umgebung in zwei vollständig physisch getrennte IKT-Umgebungen für RUAG International und MRO CH. Letztere sollte in den Netzwerkperimeter der FUB integriert werden und nach der Migration auch die Dienstleistungen der FUB beanspruchen.

Im Dezember 2018 wurde in der FUB das Projekt «MRO in der FUB» lanciert mit dem Ziel, per Ende 2019 sämtliche benötigten IKT-Leistungen zugunsten der RUAG AG bereitgestellt zu haben. Das Projekt wurde in drei Teilprojekte unterteilt, Organisation und Basisdienste, Fachanwendungen, Standorterschliessung und Rollout. Als FUB internes Führungsorgan wurde ein interner Projektausschuss gebildet. Oberstes Entscheidungsgremium des Projektes bildete der Steuerungsausschuss Entflechtung RUAG unter der Leitung des Generalsekretariats VBS. Die wesentlichen Projektziele waren:

- Die Integration der Fachapplikationen auf die IKT-Infrastruktur der FUB;
- der Bezug von Standarddiensten für den Büroarbeitsplatz;
- die Netzerschliessung sämtlicher Standorte der RUAG AG sowie
- der sichere und nachvollziehbare Transfer der Daten in die IKT-Infrastruktur der FUB.

Das Programm erwies sich als sehr komplex und erforderte von allen Beteiligten überdurchschnittliche Leistungen. Die Zusammenarbeit wurde von allen Seiten als konstruktiv beurteilt. Hinsichtlich des Termins für den operativen Übergang auf den 1. Januar 2020 lastete auch ein erheblicher Zeitdruck auf den Projektorganisationen. Der geplante Termin konnte dann aus verschiedenen Gründen nicht eingehalten werden und die Migration erfolgte daher erst im April 2020. Der erste Schritt der Entflechtung konnte Ende Juni 2020 formell abgeschlossen werden. Die Projektziele wurden gemäss den Statusberichten erreicht und die geplanten Folgeprojekte (Phase 2) initialisiert.

Beurteilung

Die Projektteams haben alles unternommen, damit die Ziele der Entflechtung realisiert werden konnten. Es wurde mit Hochdruck und allen verfügbaren Ressourcen gearbeitet, um die Migration erfolgreich zu beenden. Die Verzögerung ist auf Grund der Komplexität und des erheblichen Umfangs des Vorhabens durchaus nachvollziehbar. Entscheidend ist, dass die Ziele erreicht wurden und die Infrastruktur und Anwendungen der RUAG AG vollumfänglich in den Netzperimeter der FUB transferiert werden konnten. Mit den Nachfolgeprojekten werden noch weitere wichtige Aspekte zur Erhöhung der Informationssicherheit erarbeitet und dadurch ein nachhaltiger Sicherheitsgewinn erzielt.

2.2 Der sichere Datentransfer stellte die Projektteams vor grosse Herausforderungen

Nach dem Cybervorfall im Jahr 2016 konnte nicht ausgeschlossen werden, dass weiterhin kontaminierte Daten auf den Systemen der RUAG vorhanden sind. Um die Verschleppung von Malware auszuschliessen, durften keine Daten direkt von der RUAG zur FUB kopiert werden. Daher wurden diese über eine eigens dafür eingerichtete Datenleitung in einen Quarantänebereich der FUB transferiert, dort auf Malware gescannt und danach auf die neuen Systeme der RUAG AG übertragen. [redacted]

Für den Transfer wurden detaillierte Konzepte und Prozesse erarbeitet. Daten welche unter die Bestimmungen der International Traffic in Arms Regulations (ITAR) fallen, wurden einem gesonderten Prozess unterzogen. Hierfür haben die Business- und Share-Verantwortlichen im Vorfeld zum Datentransfer bestimmt, ob es sich um ITAR-Daten handelt. Nach dem Abschluss des Datentransfers wurde die physische Verbindung zwischen der FUB und RUAG AG wieder deaktiviert. Die Löschung der Daten auf den Ausgangssystemen wird im Rahmen des zweiten Arbeitsschritts der Entflechtung) in einem Folgeprojekt der RUAG AG abgehandelt (siehe Kapitel 2.3).

Beurteilung

Die Projektteams beider Seiten waren sich der Wichtigkeit der engmaschigen Reinigung der Daten bewusst und haben diese auch in verschiedenen Konzepten detailliert ausgearbeitet. Der Transfer der Daten wurde überwacht und die Ergebnisse akribisch protokolliert. Das Vorgehen und die Umsetzung erachtet die EFK als geeignet.

Angesichts der noch bestehenden Technisch Wissenschaftlichen Infrastrukturen (TWI) [redacted] Aus diesem Grund verzichtet die EFK hier auf eine weitere Empfehlung.

2.3 Den weiterführenden Projekten aus der Entflechtung muss eine grosse Beachtung geschenkt werden

Der Bereinigung von Archiven und Datensicherungen muss mehr Beachtung geschenkt werden

Nach der erfolgten Migration muss die RUAG AG sicherstellen, dass alle kritischen Daten bei der RUAG International Holding AG gelöscht werden. Hierfür wurde im Rahmen des zweiten Arbeitsschritts der Entflechtung ein Projekt zur Datenbereinigung initialisiert. Das Ziel ist, alle militärischen oder als vertraulich klassifizierten Daten aus den Systemen der RUAG International Holding AG unwiderruflich zu löschen oder unleserlich zu machen. Einzelne Dokumente sind aus Sicht RUAG AG als unkritisch zu betrachten, in ihrer Gesamtheit könnten sie jedoch einen Nachbau von Teilen oder Systemen ermöglichen. Das Projekt geht davon aus, dass zirka ein Promille der Daten nicht erfasst werden kann, dies wären dann jedoch einzelne Dokumente und keine zusammenhängenden Daten und somit wäre ein Rückschluss auf Gesamtsysteme kaum möglich.

Bestehende Enterprise-Resource-Planning-Systeme bei der RUAG International Holding AG sollen erhalten bleiben, damit historische Daten (z. B. Finanzdaten) auch nach der IKT-Entflechtung dokumentiert verfügbar bleiben. Dies erfolgt insbesondere aufgrund der gesetzlichen Bestimmungen wie bspw. der Aufbewahrungspflichten.

Die RUAG AG ist als Dateneigner für die Bereinigung verantwortlich. Die RUAG International Holding AG verpflichtet sich, Zugriff auf die Daten zu gewähren und das Projektteam bei der Bereinigung zu unterstützen. Die zu löschenden Daten werden in verschiedenen Tranchen zusammengefasst. Nach der Freigabe durch das Kernteam werden die Daten gelöscht und das finale Abnahmeprotokoll durch den Lenkungsausschuss abgenommen. Alle gelöschten Daten werden detailliert dokumentiert. Dafür wurde eine Datenbank aufgebaut. Die Löschmengen und der Arbeitsfortschritt können über ein Dashboard eingesehen werden.

Gemäss Projektauftrag sollen alle vorhandenen Archive und Backups ebenfalls im Rahmen dieses Projekts gelöscht werden. Im Besonderen ist zu untersuchen, ob ausgelagerte Backups oder Archive existieren. [redacted]

Das Projekt hat zum Prüfzeitpunkt eine Verzögerung von zirka vier Wochen. Diese ist auf organisatorische und ressourcenbedingte Gründe zurückzuführen. Für das Löschen der Daten wurde ein Team von Experten aufgebaut, was eine gewisse Zeit in Anspruch genommen hat.

Beurteilung

Das Konzept für die Löschung der Daten auf den Systemen der RUAG International Holding AG ist aus der Sicht der EFK zweckmässig aufgebaut. Ein mehrstufiger Kontrollmechanismus stellt die Qualität der Umsetzung sicher. Die Abnahme durch den Lenkungsausschuss stellt eine weitere unabhängige Kontrolle dar. Dennoch kann nicht ausgeschlossen werden, dass vereinzelte militärische oder vertrauliche Daten nicht gefunden und somit auch nicht bereinigt werden.

[redacted]

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt der RUAG AG, im Rahmen des Projektes die Erarbeitung einer Übersicht über die Backup- und Archivierungslandschaft der RUAG zu erstellen. Die Löschung der vorhandenen Sicherungen muss mit hoher Priorität angegangen werden.

Stellungnahme RUAG MRO Holding AG

RUAG MRO ist mit der Empfehlung einverstanden. Die Empfehlung wird innerhalb des zweiten Arbeitsschrittes der Entflechtung umgesetzt. RUAG MRO fasst eine organisatorische Lösung ins Auge, welche die Inventare und Zugangsprozesse regelt.

Die Migration der Technisch Wissenschaftlichen Infrastruktur ist auf Kurs

Bei den TWI handelt es sich um Infrastrukturen, Applikationen und Kommunikationspfade in der alten IKT-Umgebung, die auf Grund ihrer Geschäftsanforderung vom IKT-Standard der RUAG AG abweichen. An verschiedenen Standorten wurden für die Anbindung von Spezialsystemen (z. B. Messgeräte) daher separate Netzbereiche geschaffen. Da diese Systeme nicht unter der Kontrolle der IKT-Verantwortlichen der RUAG AG stehen, haben diese auch keine Kontrolle darüber, welche Technologien im Einsatz stehen. Die TWI wurden mindestens teilweise auch dazu verwendet, von der RUAG nicht zugelassene Software zu betreiben oder eigene Netzwerkübergänge zu schaffen. Es ist jedoch aus Sicherheitsgründen unabdingbar, dass die festgestellten Netzübergänge und auch die allfälligen Eigenentwicklungen zeitnah unter Kontrolle der IKT der RUAG AG kommen.

Die Programmleitung hat sich auf Grund der Komplexität entschieden, die TWI erst nach erfolgreicher IKT-Entflechtung abzulösen. Die Verschiebung in den zweiten Arbeitsschritt der Entflechtung beinhaltet sowohl die Analyse der aktuellen Situation in jedem TWI, wie auch das Erstellen von Zielbild und Lösungsarchitektur. Die Integration in den Perimeter der FUB wurde geprüft. Es wurde jedoch festgestellt, dass die für den Betrieb der TWI notwendigen IKT-Services nicht durch die standardisierten FUB-Services erbracht werden können. Deshalb wurde im Rahmen des Projektauftrags entschieden, eine separate neue IKT-Infrastruktur für die TWI aufzubauen. Die zentrale IKT-Infrastruktur wird in einem externen Rechenzentrum aufgebaut. Der Aufbau und die Betreuung der Systeme wird durch den Bereich zentrale TWI Services erfolgen. Die entsprechenden Fähigkeiten und Ressourcen müssen erst noch aufgebaut werden. Sie werden entsprechend auch durch externe Berater unterstützt werden. Der Aufbau der Infrastruktur soll bis Ende Februar 2021 und das Projekt «Entflechtung TWI» bis Ende 2021 abgeschlossen werden.

Beurteilung

Der Entscheid, die TWI erst in einem zweiten Schritt der Entflechtung zu migrieren, macht Sinn. Es ist wichtig erst eine Bestandsaufnahme zu erhalten, damit Klarheit über die im Einsatz stehenden Komponenten und Software geschaffen werden kann. Somit kann auch sichergestellt werden, dass die RUAG AG eine Übersicht über mögliche Sicherheitslücken erhält und diese entsprechend behandeln kann.

Durch den Aufbau einer separaten IKT-Infrastruktur kann sichergestellt werden, dass die TWI vom übrigen Netz der RUAG getrennt sind. Da die Infrastruktur durch die RUAG AG selber aufgebaut und betrieben wird, muss sichergestellt werden, dass die entsprechenden Ressourcen und Fähigkeiten vorhanden sind.

3 Sicherheitsorganisation und Governance

3.1 Die Sicherheitsorganisation ist zweckmässig aufgestellt

Die Information Security Organisation der RUAG arbeitet auf drei Ebenen. Auf Konzernebene ist der Chief Information Security Officer (CISO) für das konzernweite Information Security Management verantwortlich. Unterstützt wird dieser durch die Information Security Officer (ISO), einen Information Security Auditor und zukünftig einen Security Incident Manager. Die ISO stellen die Verbindung zu den Informationssicherheitsverantwortlichen der Fachabteilungen und der Tochtergesellschaften sicher. Innerhalb der Fachabteilungen sind die Informationssicherheitsverantwortlichen für das Management, die Implementierung und den Betrieb der Sicherheitskontrollen verantwortlich.

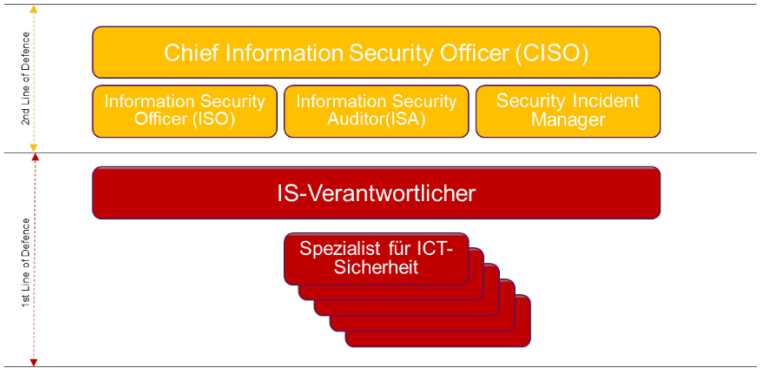


Abbildung 2: Sicherheitsorganisation der RUAG AG (Quelle: RUAG AG)

Der CISO der RUAG AG ist seit 1. Januar 2020 operativ. Er ist im Generalsekretariat angegliedert und rapportiert direkt an den General Counsel. Grundsätzlich werden die Anliegen des CISO über den General Counsel in die GL getragen. Der Chief Information Officer (CIO) und CISO haben alle drei Monate ein Zeitfenster in der Geschäftsleitung (GL), um ihre Themen vorzubringen. Im Moment ist der CISO wegen des Aufbaus des Informationssicherheitsmanagementsystems (ISMS) jeden Monat in der GL. Zudem kann er auch spontan einen Termin bei der GL oder dem Chief Executive Officer (CEO) beantragen. Der Leiter «Business Services und IT» hat einen regelmässigen Austausch mit dem CISO und entsprechend können Themen auch forciert werden.

Der Security Incident Manager wird sich hauptsächlich auf die Bearbeitung von Vorfällen im Bereich Information Security, inklusive Problemmanagement fokussieren. Er wird das zentrale Bindeglied zwischen dem Security Operations Center (SOC) der FUB und den Fachabteilungen. Die Rolle wurde ausgeschrieben und konnte auf Januar 2021 besetzt werden.

Jede Fachabteilung verfügt über einen Informatiksicherheitsverantwortlichen (IS-Verantwortlichen), welcher die Bereitstellung von RUAG-Services unterstützt. Fachabteilungen sind explizit auch Teile einer Geschäftseinheit, die selbstständig IKT-Services implementieren und betreiben. Hierbei handelt es sich um spezielle Dienste ausserhalb der Grundversorgung durch die FUB (z. B. TWI und oder Dienste zu Gunsten der Real Estate AG).

Der Fachausschuss Information Security setzt sich aus dem CISO, allen ISO der RUAG MRO Holding AG, dem Datenschutzbeauftragten, dem Geheimschutzbeauftragten, sowie einem Vertreter des Bereichs «Quality & Safety» (Physische Sicherheit) zusammen. Der Fachausschuss wird durch den CISO geleitet. Der Fachausschuss berät und koordiniert die Anliegen

der RUAG MRO Holding AG in allen Fragen der Information Security. Er sorgt für eine ausreichende Regelungsdichte im Bereich der Information Security auf Stufe RUAG MRO Holding AG und unterstützt die CIO, die IS-Verantwortlichen und ICT-Spezialisten bei ihren Regelungsaufgaben.

Die Schnittstellen zum Leistungserbringer sind institutionalisiert

Der CISO der RUAG AG und der CISO der FUB treffen sich monatlich zu einem bilateralen Austausch. Die Traktanden und Inhalte werden zuvor gemeinsam definiert. Weitere Schnittstellen sind der Austausch zwischen dem Security Incident Manager und dem SOC der FUB. Hierfür wurde eine Kommunikationsmatrix definiert und der Security Incident Prozess wird laufend überarbeitet. Weiter besteht ein direkter Kontakt mit dem Audit- und Risikomanagement (RM) der FUB.

Beurteilung

Damit die Information Security bei der RUAG AG angemessen und auf die Bedürfnisse des Unternehmens abgestimmt ist, muss die Information Security Organisation nicht nur auf Konzernebene präsent, sondern auch in allen Geschäftsbereichen verankert sein. Die Organisation ist zielführend aufgebaut und deckt die Bedürfnisse einer klassischen IKT-Sicherheitsorganisation ab. Durch die Rollen der Informationssicherheitsverantwortlichen ist die IKT-Sicherheit auch in den verschiedenen Fachbereichen verankert. Dies begünstigt nachhaltig die konsolidierte Erfassung von Bedrohungen und Vorfällen und dient einer verbesserten Erstellung des Lagebildes. Der Fachausschuss Information Security stellt sicher, dass die Belange der IKT-Sicherheit und des Datenschutzes mit den übrigen relevanten Stellen in der Organisation koordiniert werden.

Der regelmässige und institutionalisierte Austausch zwischen dem CISO der FUB und dem CISO der RUAG AG ist ein wichtiges Instrument zum gemeinsamen Verständnis.

3.2 Die erforderlichen Sicherheitsdokumente müssen noch erarbeitet werden

Grundsätzlich wurden die Richtlinien und Konzepte der RUAG Holding übernommen und an die Bedürfnisse der RUAG AG angepasst. Im Rahmen des Projekts «Aufbau ISMS» sollen die Richtlinien überarbeitet werden. Dies wurde als ein Meilenstein definiert und soll bis Ende 2020 fertiggestellt werden. Zum Prüfzeitpunkt liegen jedoch kaum adaptierte und formalisierte Versionen vor.

Die von der Bundesverwaltung geforderten Sicherheitsdokumente[2] sollen ebenfalls im Projekt «Aufbau ISMS» erarbeitet werden. Die Schutzbedarfsanalysen (Schuban) zu allen Schutzobjekten sollen erstellt und in einer Datenbank erfasst werden (siehe Kapitel 3.5). Die Dokumente werden durch interne Stellen und durch den CISO der FUB überprüft und freigegeben. Anschliessend sollen die Informationssicherheits- und Datenschutzkonzepte (ISDS) der Anwendungen mit erhöhtem Schutzbedarf erstellt und verabschiedet werden. Die Dokumentationen der Sicherheitsanforderungen sollen bis Ende 2020 erstellt werden. Zum Prüfzeitpunkt sind gemäss Statusbericht 60 % der Schuban erstellt und in der Datenbank abgelegt. Die Verantwortung für die termingerechte Umsetzung

[2] P041 - Schutzbedarfsanalyse (Schuban), Si001 - IKT-Grundschutz in der Bundesverwaltung und P042 - Informationssicherheits- und Datenschutzkonzept (ISDS)

liegt bei der RUAG AG. Die FUB nimmt hier nur die Rolle der Kontrollinstanz wahr. Aus Sicht des CISO FUB ist die geplante Umsetzung bis Ende Jahr gefährdet.

Beurteilung

Die Dokumentation der Sicherheitsanforderungen von Anwendungen und Systemen ist ein zentraler Punkt für die Definition der erforderlichen Sicherheitsmassnahmen. Die RUAG AG erarbeitet die erforderlichen Dokumentationen im Rahmen des Projektes «Aufbau ISMS» und hat hierfür einen Meilenstein definiert. Dies verdeutlicht, dass das Bewusstsein für die Wichtigkeit der Thematik auf Seiten RUAG AG vorhanden ist. Der Umsetzungsstand ist inzwischen bei rund 60 % und die Ziele konnten nicht erreicht werden. Ein Abschluss der Arbeiten bis Ende Jahr erachtet die EFK als unrealistisch. Durch die regelmässige Berichterstattung an das Management der RUAG AG und die Überwachung durch die FUB, ist aus Sicht der EFK ein genügendes Controlling installiert. Aus diesem Grund verzichtet die EFK hierzu auf eine Empfehlung.

3.3 Ein Information Security Management System schafft eine Grundlage zur Erhöhung der IKT-Sicherheit

Das Projekt «Aufbau ISMS» ist für die RUAG AG von strategischer Bedeutung. Das bestehende ISMS soll an die Anforderungen der neuen Unternehmung angepasst werden. In einer ersten Phase möchte die RUAG AG deshalb eine Analyse durchführen. Ziel dieser Analyse ist die Definition und Dokumentation des weiteren Projektvorgehens. Das Lieferobjekt dient der Geschäftsleitung als Entscheidungsgrundlage für das weitere Vorgehen. In einer ersten Phase wurde eine Gap-Analyse durchgeführt, welche die Basis für die Definition des weiteren Projektvorgehens und die Arbeitspakete lieferte. Die Gap-Analyse diente der Überprüfung der derzeitigen Fähigkeiten, bereits vorhandener Vorgaben und Prozesse und der Definition eines Fahrplans zur Schliessung der identifizierten Lücken. Die resultierenden Arbeitspakete wurden priorisiert und in die Meilensteinplanung integriert. Das ISMS soll bis Ende 2022 vollständig umgesetzt und operativ sein.

Beurteilung

Die Anpassung bzw. Implementierung eines ISMS in der RUAG AG ist ein wesentlicher Bestandteil zur Erhöhung der Informationssicherheit. Das Projekt zur Einführung ist zweckmässig aufgestellt und die Planung und Meilensteine sind nachvollziehbar. Mit den einzelnen Meilensteinen deckt die RUAG AG auch verschiedene Anforderungen des IKT-Grundschutzes ab und stellt sicher, dass diese längerfristig erfüllt und laufend kontrolliert werden.

3.4 Periodische Audits stellen die Wirksamkeit der umgesetzten Massnahmen sicher

Interne Audits sind ein Bestandteil des geplanten ISMS der RUAG AG. Die Audits sollen prüfen, inwieweit die Anforderungen, Vorgaben und Massnahmen wirksam umgesetzt wurden. Damit werden in geplanten Abständen jährlich zwei bis drei Audits und vier Follow-Up durchgeführt. Die Audittätigkeiten der RUAG AG werden durch die interne Auditorin oder extern beauftragte Dritte durchgeführt. Der interne Auditprozess wendet systematische Prozesse zur Planung, Durchführung und Massnahmenüberprüfung an und orientiert sich

grundsätzlich am ISO/IEC 19011:2018. Die Prüfungsplanung wird basierend auf Schwachstellen oder Risiken jeweils für die kommenden drei Jahre erstellt. Alle drei Monate erfolgt ein Statusbericht an das Management. Das Audit-Management ist in einem Risikomanagement-Werkzeug abgebildet.

Die RUAG AG hat das Recht, die Systeme und Prozesse der FUB zu prüfen. Zum Prüfzeitpunkt organisierte sie mit externer Unterstützung die Durchführung eines Audits bei der FUB. Dieses soll die korrekte Umsetzung der Netzwerkarchitektur und der Sicherheitsvorgaben im Perimeter der FUB für die RUAG AG prüfen. Parallel dazu prüft die RUAG AG im selben Zeitraum bei der FUB den Incident Response Prozess. Die Resultate der beiden Prüfungen sind zum Berichtszeitpunkt noch offen.

Beurteilung

Die Organisation des Bereichs Audit bei der IKT-Sicherheit der RUAG AG ist aus Sicht der EFK zielführend aufgestellt. Durch die risikobasierte und längerfristige Planung, können die verschiedenen Bereiche des ISMS adressiert und allfällige Schwachstellen aufgedeckt und korrigiert werden.

Die EFK begrüsst insbesondere, dass die RUAG im FUB Perimeter Audits durchführen, bzw. beauftragen kann.

3.5 Das Risikomanagement und das betriebliche Kontinuitätsmanagement sind im Aufbau

Das Unternehmens-Risikomanagement (RM) soll im Rahmen eines Projektes bis Ende 2021 in den wesentlichen Punkten aufgebaut und operativ werden. Zum Prüfzeitpunkt ist es organisatorisch bei der Service Unit «Business Services & IT» angesiedelt. Mit der Reorganisation wird es per Januar 2021 im Generealsekretariat und somit bei den Bereichen Informationssicherheit, Compliance und Legal angesiedelt. Zum Prüfzeitpunkt ist eine Vollzeitstelle für das RM und das Business Continuity Management (BCM) zuständig, geplant ist jedoch die Erweiterung um eine weitere Vollzeitstelle. Zusätzlich verfügt jeder Geschäftsbereich über einen Risikocoach, welcher die Risiken auf Stufe Geschäftsbereich aufnimmt und mit dem RM abspricht. Das RM ist in regelmässigem Kontakt mit dem CISO und die Behandlung der Toprisiken erfolgt gemeinsam. Absprachen mit der FUB gibt es noch keine. Dies soll jedoch ab 2021 Jahr erfolgen.

Ein BCM ist bei der RUAG AG zum Prüfzeitpunkt nicht operativ implementiert. Auch dies soll in den nächsten Jahren definiert werden. Der eigentliche Aufbau steht in Abhängigkeit zum Abschluss des Projektes zum RM. Somit erfolgen die konzeptionellen Arbeiten voraussichtlich ab Mitte 2021 und der operative Betrieb eines ganzheitlichen BCM ist für 2023 geplant. Im Bereich der IKT und Information Security sind jedoch bereits Aktivitäten hinsichtlich des Aufbaus eines BCM am Laufen. So wurde beispielsweise die Richtlinie «Kontinuität von Informationssicherheit» erarbeitet. Auch werden hinsichtlich der BCM Massnahmen, Schutzbedarfsanalysen für Applikationen und Datenbanken erarbeitet und diese Schutzobjekte in einer Datenbank gemäss den Schutzbedarfsanalysen klassifiziert. Auf Basis dieser Daten werden die Risiken ermittelt und sollen in den sukzessiven risikobasierten Aufbau des BCM einfliessen.

Beurteilung

Als Teil der Governance, Risk und Compliance-Organisation hilft das RM, die Werte der RUAG AG zu schützen. Die Implementierung und Aufrechterhaltung eines Risikomanagement-Systems bei der RUAG AG ist erforderlich. Die EFK erachtet die Projektziele und Umsetzungsplanung als angemessen und zielführend.

Die Notwendigkeit eines funktionierenden BCM über die gesamte Organisation wurde durch die RUAG AG erkannt und im Rahmen des Projektes zum RM adressiert. Durch die zeitliche Abhängigkeit wird das operative BCM jedoch frühestens ab 2023 vollständig in Betrieb sein. Für die Zeit des sukzessiven risikobasierten Aufbaus bis zur effektiven Wirksamkeit des gesamten BCM stehen die Notfallpläne daher noch nicht vollständig zur Verfügung. Die EFK sieht das Risiko, dass dadurch Geschäftsprozesse nicht genügend geschützt sind. Sie erachtet es daher als wichtig, dass für alle kritischen Geschäftsprozesse die Einführung angemessener Notfall-Massnahmen priorisiert behandelt und umgesetzt werden.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt der RUAG AG, die kritischen Geschäftsprozesse zu definieren und für diese (allenfalls in Absprache mit der FUB) geeignete Massnahmen zur Betriebsweiterführung im Störungsfall vorzusehen.

Stellungnahme RUAG MRO Holding AG

RUAG MRO ist mit der Empfehlung einverstanden. Eine weiter voranzutreibende Roadmap für das BCM steht, die konzeptuellen Arbeiten sind ab Mitte 2021 vorgesehen. Die Planung beinhaltet die Massnahmen für den Aufbau eines BCM, welches die wesentlichen Geschäftsprozesse (inkl. Infrastruktur) sowie die spezifischen IT-gestützten Prozesse (inkl. IT-Infrastruktur) umfasst. Die kritischsten Elemente, die einen Notfall-Planung erfordern, sollen dabei identifiziert und prioritär bereits ab 2021 sukzessive gesichert werden.

Vorgehen:

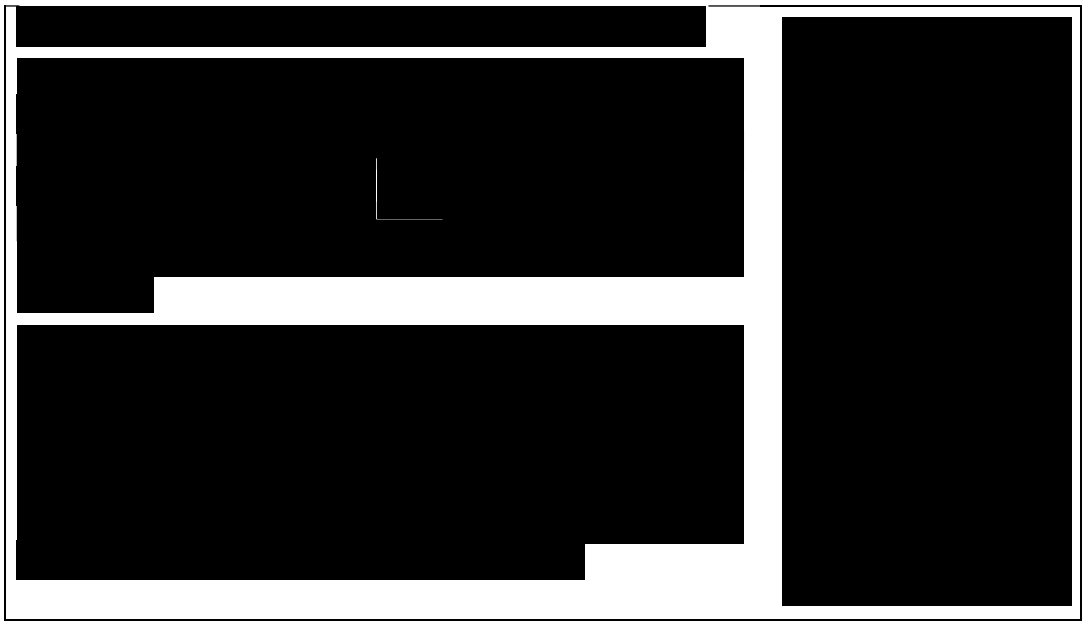
- Erstellung Planung «Konzeption/Implementierung BCM-System»
- Identifizierung der kritischen Geschäftsprozesse *
- Erstellung der Notfall-Planungen für kritische Geschäftsprozesse *
- Umsetzung Planung «Konzeption/Implementierung BCM-System»

*) iteratives, paralleles Vorgehen

4 Sicherheit im Betrieb

4.1 Die Führungsunterstützungsbasis als Provider

Die RUAG AG hat den Betrieb der Informatik-Infrastruktur an die FUB ausgelagert. Diese betreibt die Systeme bis und mit der Ebene Betriebssystem. Die RUAG AG ist für die Applikationen zuständig.



Damit wurde auch ein wesentlicher Teil des Server-Managements an die FUB übergeben. Die ersten Betriebserfahrungen in der neuen Konstellation haben gezeigt, dass auch innerhalb der RUAG AG die Aufgabenabgrenzung zwischen den jeweiligen Applikationsverantwortlichen und den Systemadministratoren geschärft werden muss. Die RUAG hat die Probleme und die potentiellen betrieblichen Risiken erkannt und beabsichtigt, im Rahmen eines Projektes, das Server-Management und den Betrieb der Datenbanken und Applikationen zu professionalisieren.

Beurteilung

Die FUB bietet ihre IKT-Serviceleistungen primär den Verwaltungseinheiten des VBS an. Die RUAG AG als Technologiekonzern hat stark unterschiedliche Anforderungen an IKT-Services, als dies das VBS hat. Dennoch konnten die Ansprüche der RUAG AG weitgehend in den Betrieb der FUB eingebunden werden. Mit dem IaaS-Modell stellt die FUB der RUAG eine solide Infrastruktur in einem geschützten Perimeter zur Verfügung. Die Überwachung der Systeme und Anwendungen der RUAG AG ist in den operativen Betrieb eingebunden. Dadurch ist die FUB in der Lage, frühzeitig mögliche Gefahren zu erkennen und abzuwenden. Die im Betrieb erkannten prozessualen Schwachstellen werden im Rahmen eines Projektes angegangen. Die EFK erachtet die Form der Zusammenarbeit als zweckmässig.

[redacted]

4.2 Das Störungsmanagement muss durchgängiger werden

Die Mitarbeitenden der RUAG AG melden Störungen an den IKT-Systemen dem Service-Desk der FUB. Die Anfragen werden in einem Ticketing-System bearbeitet. Dabei kann die RUAG AG nicht feststellen, ob die Ursache einer Störung bei der FUB liegt oder ob der Bereich Netzwerk des BIT betroffen ist. Umgekehrt kann das BIT bei einem Netzausfall nicht erkennen, ob es sich um einen Standort der RUAG AG handelt. Entsprechend muss die FUB als Provider mögliche Ausfälle und Unterbrüche bei Änderungen an Systemen des BIT, auch entsprechend an die RUAG AG kommunizieren. Dies ist zum Prüfzeitpunkt noch nicht lückenlos und zufriedenstellend umgesetzt. Von Seiten RUAG AG wurde mehrfach bemängelt, dass auf Grund von Ausfällen die Servicevereinbarungen nicht eingehalten würden. [redacted]

Beurteilung

[redacted] Entsprechend besteht die Gefahr, dass sich die Fehlersuche und Störungsbehebung verzögert. Die Schaffung durchgängiger Prozesse für die Störungsbehebung und die Kommunikation sind daher von hoher Wichtigkeit. Es muss zudem sichergestellt werden, dass die FUB die RUAG AG bei geplanten Änderungen an den Systemen zweckmässig informiert.

Gemäss Definition der Vereinbarung zum Service «IaaS» kann die EFK keine Verletzung der Serviceleistungen feststellen. Aufgrund der aktuellen Verfügbarkeiten und Kapazitäten der FUB bestehen momentan Standardverträge zu Hilfeleistung während der Bürozeiten. Sofern der RUAG AG die aktuellen Störungsbehebungszeiten und Leistungen nicht genügen, sollte geklärt werden, ob die Servicevereinbarungen allenfalls angepasst werden sollten.

Die RUAG AG führt zum Prüfzeitpunkt ein internes Audit zum Incident Response Prozess durch. Die Feststellungen der EFK waren Gegenstand der internen Prüfung, aus diesem Grund verzichtet die EFK auf eine zusätzliche Empfehlung.

4.3 Ausnahmen zum IKT-Grundschutz müssen bearbeitet oder formalisiert werden

Mit der Einbindung der Systeme in den Perimeter der FUB unterliegt die RUAG AG den Sicherheitsvorgaben des Bundes. Einige im Betrieb stehende Anwendungen und Systeme verfügen über Ausnahmen zum IKT-Grundschutz. Diese werden durch den CISO der FUB entsprechend gelistet und behandelt. Ausnahmen werden im ISMS erfasst und alle zwölf Monate geprüft. Die Prozesse für das Genehmigungsverfahren sind definiert und werden

laufend überwacht. Auch für nicht Standardprodukte sind Ausnahmeanträge erforderlich. Für diese gibt es den Ausnahmeprozess der FUB. Dort werden die Ausnahmen beurteilt und bei Bedarf über den P035-Prozess über den ISBD des VBS an das Nationale Zentrum für Cybersicherheit (NCSC) zur weiteren Behandlung weitergeleitet.

Beurteilung

Die RUAG AG kann im Einzelfall aus organisatorischen, technischen oder wirtschaftlichen Gründen vom IKT-Grundschutz abweichen. Jede Abweichung muss jedoch im entsprechenden ISDS-Konzept beschrieben und die Risiken ausgewiesen werden. Zudem müssen solche Grundschutzunterschreitungen vom ISBD des VBS oder vom NCSC genehmigt werden. Bei Nichteinhalten dieser Vorgaben besteht die Gefahr, dass eine VE Risiken nicht ausreichend behandelt, oder dass sich Risiken unerkannt kumulieren.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt der RUAG AG, sämtliche Ausnahmen zu den IKT-Grundschutzanforderungen zu erfassen und zu prüfen. Primär sollen Grundschutzunterschreitungen vermieden werden. Wo dies nicht umsetzbar ist, müssen diese entsprechend dem IKT-Grundschutz Kapitel 1.2 formalisiert werden.

Stellungnahme RUAG MRO Holding AG

RUAG MRO ist mit der Empfehlung einverstanden. Ausnahmen zu den IKT-Grundschutzanforderungen werden zukünftig elektronisch verwaltet, dazu werden diese im Confluence-System der RUAG AG erfasst. Ein entsprechender Prozess wird derzeit aufgebaut mit dem Zweck, die laufenden und neuen Ausnahmen zu erfassen.

4.4 [redacted]

5 Umsetzung der Empfehlungen aus früheren Prüfungen

Die Prüfungen 18517 und 19418 wurden vor der Entflechtung der RUAG durchgeführt. Die Umsetzung der Empfehlungen wurden im Rahmen dieses Audits nur überprüft, soweit sie sinngemäss die RUAG AG betrafen. Daher bezieht sich der Erfüllungsstand ausschliesslich auf die RUAG AG.

Die RUAG AG hat die meisten Empfehlungen der EFK zweckmässig adressiert

Sieben von neun Empfehlungen der EFK sind bei der RUAG AG umgesetzt. Die verbleibenden zwei Empfehlungen befinden sich in der Umsetzung.

Für die Erstellung der Sicherheitsdokumente (Empfehlung 19418.002) wurden im Rahmen der Einführung des ISMS konkrete Umsetzungsziele definiert. Das Projekt rapportiert zum Prüfzeitpunkt einen Erfüllungsgrad von zirka 60 % und soll bis Ende 2020 abgeschlossen werden. Die Planung erscheint der EFK als unrealistisch.

Der Transfer der TWI in ein gesichertes Umfeld (Empfehlung 19418.003) ist ebenfalls im Rahmen eines Projektes des zweiten Arbeitsschritts adressiert (siehe Kapitel 2.3). Wichtige Grundlagen wie die Zielarchitektur und das Service-Portfolio sind definiert und das Rechenzentrum ist betriebsbereit. Die Umsetzung ist aber gemäss aktueller Planung erst auf Ende 2021 zu erwarten und damit gegenüber dem ursprünglich an die EFK gemeldeten Umsetzungstermin acht Monate verspätet.

Eine tabellarische Darstellung der Empfehlungen und deren Umsetzungsstand befinden sich in den Anhängen 4 und 5.

Beurteilung

Mit der Migration der IKT-Infrastruktur der RUAG AG konnten die meisten Empfehlungen im Rahmen der Entflechtung adressiert werden. Die Empfehlungen wurden durch die RUAG AG mehrheitlich umgesetzt. Die beiden offenen Empfehlungen sind adressiert und es liegen nachvollziehbare Projektpläne und Meilensteinplanungen vor. Die EFK erachtet die getroffenen Massnahmen und das weitere Vorgehen der RUAG AG als angemessen.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Bundesgesetz über die Rüstungsunternehmen des Bundes (BGRB) vom 10. Oktober 1997 (Stand am 1. Januar 2012), SR 934.21
Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV) vom 9. Dezember 2011 (Stand am 1. November 2016), SR 172.010.58
Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (Stand am 1. Januar 2018), SR 510.411
Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. Januar 2014) SR 235.1
Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 (Stand am 16. Oktober 2012) SR 235.11
Verordnung über das Geheimschutzverfahren bei Aufträgen mit militärisch klassifiziertem Inhalt (Geheimschutzverordnung) vom 29. August 1990 (Stand am 1. Januar 1991) SR 510.413
Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB) vom 1. Juli 2015 (Stand am 16. Januar 2019) W002
Weisungen über die Klassifizierung und Behandlung von US-COMSEC Material (US-COMSEC Weisungen) vom 1. Januar 2014 (Stand am 31.12.2019) 90.070 d
Beschlüsse des Bundesrates
BRB vom 28. Juni 2017, Portfolioanalyse der RUAG und Teilprivatisierungsstrategie
BRB vom 21. März 2018, Entflechtung VBS – RUAG
BRB vom 15. März 2019, Entflechtung und Weiterentwicklung der RUAG
BRB vom 23. Oktober 2019, Strategische Ziele des Bundesrats für die BGRB Holding AG 2020–2023

Anhang 2: Abkürzungen

BCM	Business Continuity Management (Betriebliches Kontinuitätsmanagement)
[redacted]	[redacted]
BIT	Bundesamt für Informatik und Telekommunikation
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNO	Computer Network Operations
EFK	Eidgenössische Finanzkontrolle
FUB	Führungsunterstützungsbasis
GL	Geschäftsleitung
IKT	Informations- und Kommunikationstechnik
IaaS	Infrastructure as a Service
ISA	Information Security Auditor
ISDS	Informationssicherheits- und Datenschutzkonzept
ISO	Information Security Officer
ISO/IEC	International Organization for Standardization
ITAR	International Traffic in Arms Regulation (siehe Glossar)
milCERT	Military Computer Emergency Response Team
MRO	Maintenance Repair Overhaul
NCSC	Nationales Zentrum für Cybersicherheit
RM	Unternehmens-Risikomanagement
Schuban	Schutzbedarfsanalyse
SOC	Security Operations Center

TWI	Technisch wissenschaftliche Infrastruktur
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

Anhang 3: Glossar

International Traffic in Arms Regulation	Export-Regelungen der US-Regierung, welche zum Tragen kommen, wenn potentiell gefährliche Systeme über Landesgrenzen hinweg transportiert oder gehandelt werden. Die Regelungen gelten vor allem für Systeme im militärischen Bereich. Eine Verletzung dieser Regelungen kann schwere Sanktionen seitens der USA zur Folge haben.
ISO/IEC 19011:2018	Leitfaden zur Auditierung von Managementsystemen
ISO/IEC 27001:2013	Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen
ISO/IEC 27002:2013	Informationstechnologie – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheits-Massnahmen
Secure File Transfer Service	Der Secure File Transfer Service kann zum sicheren Austausch von grossen Dateien innerhalb von Unternehmen, aber auch mit externen Stellen (Lieferanten, Partner etc.) verwendet werden.
P035 – Prozess	Die IKT-Vorgabe regelt den Umgang mit Anforderungen und Vorgaben zur Bundesinformatik gemäss Ziffer 4 der Weisungen des EFD vom 19. Februar 2013 zur Umsetzung der Bundesinformatikverordnung (WUBinfV) sowie gemäss P000 - Informatikprozesse in der Bundesverwaltung.
Terabyte	1 Terabyte = 1.024 Gigabyte = 10^{12} Byte

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).

Anhang 4: Follow-up Empfehlungen 18517

Nr.	Empfehlung	Feststellungen	Termin
001	Die EFK empfiehlt der Geschäftsleitung der RUAG, ein Gesamtinventar ihrer wertvollen oder sensitiven Informationen (Information Assets) über alle Divisionen erstellen zu lassen und aktuell zu halten. Das Inventar muss jederzeit aufzeigen, wo heikle Daten in elektronischer Weise gelagert werden und wer für den Schutz dieser Daten verantwortlich ist.	Mit dem Transfer Daten und der damit verbundenen Zuordnung an «Besitzer» konnte die RUAG AG ihre Informationen sichten und entsprechend klassifizieren. Diese, aber auch sämtliche Anwendungen, wurden erfasst und werden im Rahmen des ISMS in einer Datenbank geführt. Diese Informationen sind unter anderem Grundlage für den Aufbau des RM und des BCM (siehe Kapitel 3.5).	Umgesetzt (für RUAG AG)
002	Die EFK empfiehlt der Geschäftsleitung der RUAG, die Sicherheitsorganisation in allen Bereichen mit geeigneten Spezialisten weiter zu verstärken. Insbesondere in den überprüften Divisionen, aber auch zentral, sind zu wenig Ressourcen vorhanden, um die zahlreichen wichtigen Sicherheitsaufgaben wahrzunehmen.	Die Sicherheitsorganisation der RUAG AG wurde, wie in Kapitel 3.1 beschrieben, neu definiert und erscheint angemessen. Die Information Security Organisation der RUAG AG arbeitet auf drei Ebenen. Auf Konzernebene ist die Funktion des CISO für das konzernweite Information Security Management verantwortlich. Unterstützt wird der CISO von den ISO, dem ISA und dem Security Incident Manager. Die ISO verbinden die Information Security Organisation mit den Fachabteilungen. Innerhalb der Fachabteilungen sind die Informationssicherheitsverantwortlichen für das Management, die Implementierung und den Betrieb der Sicherheitskontrollen verantwortlich.	Umgesetzt (für RUAG AG)
003	Die EFK empfiehlt der Geschäftsleitung der RUAG, die Umsetzung ihrer Vorgaben zum Information Security Management System konzernweit durch regelmässige und systematische Audits überprüfen zu lassen.	Die periodischen IT-Audits werden im Rahmen des ISMS geplant und durchgeführt. Die Organisation des Bereichs Audit bei der IKT-Sicherheit der RUAG ist aus Sicht der EFK zielführend aufgestellt. Durch die risikobasierte und längerfristige Planung, können die verschiedenen Bereiche des ISMS adressiert werden und allfällige Schwachstellen aufgedeckt und korrigiert werden (siehe Kapitel 3.4).	Umgesetzt (für RUAG AG)

004	Die EFK empfiehlt der Geschäftsleitung der RUAG, die in die Firma Clearswift übernommenen Cyberspezialisten aus dem Bereich Materialkompetenzzentrum rasch wieder in einen Bereich einzugliedern, welcher später in die MRO CH überführt wird.	Die Mitarbeitenden, welche für Tranalyzer sowie das IKZ arbeiteten, wurden per 1. Oktober 2018 der Business Unit NEO unterstellt. Aufgrund dieser Massnahme und der daraus resultierenden Synergieverluste, hat die RUAG entschieden, das internationale Service-Geschäft aufzugeben und den betroffenen zehn Mitarbeitern andere Stellen anzubieten oder abzubauen. Die Empfehlung wurde umgesetzt und durch die EFK mit dem Bericht 19418 validiert.	Umgesetzt

Anhang 5: Follow-up Empfehlungen 19418

Nr.	Empfehlung	Feststellungen	Termin
001	Die EFK empfiehlt der Führungsunterstützungsbasis, einen unkontrollierten Datentransfer über die Arbeitsplatzsysteme mit geeigneten technischen Massnahmen zu verhindern.	Es wurden keine technischen Massnahmen implementiert. Jedoch gab es umfangreiche Vorgaben an die Mitarbeitenden. Diese wurden von der RUAG AG erlassen.	Umgesetzt
002	Die EFK empfiehlt der RUAG MRO CH, eine verbindliche Roadmap zur Aktualisierung der Sicherheitsdokumente gemäss Bundesvorgaben zu erstellen inklusive der sich daraus ergebenden und umzusetzenden zusätzlichen Sicherheitsmassnahmen.	Eine Schuban ist Grundlage für die Erstellung der ISDS-Konzepte. In einem ersten Schritt werden die fehlenden Schuban für die zur FUB transferierten Applikationen erarbeitet. Danach werden für Applikationen mit erhöhtem Schutzbedarf zusätzlich ein ISDS-Konzept erstellt. Für eine kontinuierliche Betriebserlaubnis der Applikationen per 1.1.2021 ist eine vorliegende Schuban Voraussetzung (Vorgabe FUB). Zum Prüfzeitpunkt rapportiert die RUAG AG einen Erfüllungsgrad bei 60 % (siehe 3.2). Eine Umsetzung bis Ende 2020 erschient der EFK als unrealistisch. Eine Verlängerung der Umsetzungsfrist sollte **bei der EFK** beantragt werden.	In Arbeit 31.12.2020
003	Die EFK empfiehlt der RUAG, für die technisch wissenschaftliche Infrastruktur zeitnah eine Lösung zu suchen, damit diese in einem gesicherten Umfeld betrieben und überwacht wird.	Im Rahmen eins Folgeprojekts werden die TWI in ein gesichertes Umfeld transferiert. Dieser Arbeitsschritt beinhaltet sowohl die Analyse der aktuellen Situation in jedem TWI, wie auch das Erstellen von Zielbild und Lösungsarchitektur. Inzwischen wurden erste Services definiert und ein Rechenzentrum in Betrieb genommen. Das Projekt ist gemäss Planung der RUAG AG auf Kurs und soll bis Ende 2021 abgeschlossen werden (siehe Kapitel 2.2). Der Termin vom 30. April 2021 kann daher nicht eingehalten werden, eine Verlängerung der Umsetzungsfrist sollte bei der EFK beantragt werden.	In Arbeit 30.04.2021

004	Die EFK empfiehlt der Führungsunterstützungsbasis und RUAG MRO CH, die Verantwortlichkeiten und die Zusammenarbeit der beiden Sicherheitsorganisationen zu regeln. Die Regelungen sollten insbesondere auch das Vorgehen bei Sicherheitsvorfällen (Meldung, Eskalation, Alarmierung) beinhalten.	Die Verantwortlichkeiten und Prozesse zwischen den Sicherheitsorganisationen der RUAG AG und der FUB sind geregelt (siehe Kapitel 3.1). Die Leistungserbringung des SOC der FUB ist in der Servicebeschreibung «Infrastructure as a Service (IaaS)» implizit enthalten. Nach einer ersten Anwendungsphase bis 31.12.2020 werden die Eckwerte der SOC-Leistungserbringung überprüft und wo nötig verfeinert.	Umgesetzt
005	Die EFK empfiehlt der RUAG, für die verbleibende Laufzeit des Entflechtungsprogramms einen von der Programmorganisation unabhängigen Risikomanager einzusetzen.	Das Projekt ist abgeschlossen, die Empfehlung somit obsolet. Das RM im Projekt wurde durch das RM der RUAG Holding übernommen.	Umgesetzt