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

Audit de la gestion des risques et de la conformité

BGRB Holding SA, RUAG MRO Holding SA, RUAG International Holding SA

CDF-20432 | Prises de position incluses | 12 janvier 2021 | DélFin D2/2021

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Contrôle fédéral des finances (CDF) Monbijoustrasse 45 3003 Berne Suisse
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.20432.997.00536
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
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Sauf indication contraire, les dénominations de fonction dans ce rapport s'entendent aussi bien à la forme masculine que féminine.

Table des matières

Audit de la gestion des risques et de la conformité
BGRB Holding SA, RUAG MRO Holding SA, RUAG International Holding SA

L'essentiel en bref

Au début de l'année 2020, RUAG a été scindé en deux entités, détenues par la Confédération par l'intermédiaire d'une société de participation (BGRB Holding SA). RUAG MRO Holding SA (chiffre d'affaires estimé : 660 millions de francs) doit essentiellement fournir des prestations à l'armée suisse. RUAG International Holding SA (chiffre d'affaires estimé : 1230 millions) a repris les activités dans l'aérospatial et devrait, à terme, être privatisée.

Dans son examen, le Contrôle fédéral des finances (CDF) constate que, contrairement à ce que RUAG a affirmé au Conseil fédéral en décembre 2018, le groupe avant dissociation ne disposait pas d'une gestion des risques globale. Entre 2016 et fin 2019, aucun rapport consolidé sur les risques n'a été présenté au conseil d'administration.

Depuis, les choses ont évolué. Chacune des nouvelles entités élabore un concept de gestion des risques et commence à l'implémenter. RUAG International a déjà établi une solide base normative. Cependant, les étapes de la mise en œuvre ne sont pas encore complètement abouties, ni en termes de contenu ou de granularité. RUAG MRO, qui a dû créer une structure dirigeante encadrant ses unités opérationnelles, comme une « spin-off », n'est pas encore au même niveau que sa société sœur au niveau des directives, mais son plan d'action détaillé et coordonné est convaincant. La mise en œuvre de la gestion de la conformité est également en cours dans les deux entités.

Les conseils d'administration doivent fixer des lignes directrices

Le CDF recommande aux deux entreprises de renforcer la gestion des risques dans une perspective opérationnelle et surtout ascendante *(bottom-up)*. Il leur recommande aussi d'intégrer la gestion des risques comme instrument de gestion et, par conséquent, de permettre l'intégration adéquate du point de vue stratégique dans le sens d'une gestion globale des risques de l'entreprise. Les deux entreprises devraient enfin établir une vue d'ensemble des risques.

L'implication des instances dirigeantes est essentielle. Afin de pouvoir remplir leur fonction de contrôle et de stratégie, le CDF recommande aux deux conseils d'administration de traiter régulièrement de l'organisation de la gestion des risques pour définir leurs besoins en matière d'information et d'en tirer des exigences claires pour la gestion des risques. Ces éléments, très importants dans une phase de démarrage, n'ont jusqu'ici pas été suffisamment pris en compte.

Dans leur concept respectif, RUAG MRO et RUAG International évoquent toutes deux le thème de l'appétit, de la tolérance et de la capacité à supporter les risques. Il manque encore une spécification au sens d'une valeur ou d'un ordre de grandeur pour la tolérance au risque des entreprises. Une fois celle-ci définie, la méthode d'évaluation des risques devra être adaptée en conséquence.

Améliorations préconisées dans l'organisation et les processus

A ce jour, RUAG MRO et RUAG International disposent respectivement de 2 et de 1,9 équivalents plein temps pour la gestion centrale des risques. Bien que l'organisation centrale soit complétée par un réseau de responsables des risques dans les unités, ce ratio semble étonnant dans la mesure où les deux entités diffèrent fondamentalement en termes de taille, de modèle d'entreprise et d'activités internationales. Il est trop tôt pour se prononcer de manière définitive sur l'adéquation des ressources. Dans les deux entreprises, les conditions-cadres doivent être renforcées pour garantir l'indépendance des personnes impliquées dans le système de gestion des risques.

L'identification des risques des deux entités doit avoir lieu à tous les niveaux organisationnels. RUAG International est en train de mettre en place un comité pour consolider les risques identifiés à l'attention de la direction et du conseil d'administration. Pour sa part, RUAG MRO signale un nombre fixe de risques principaux provenant des unités ou des centres. Il n'existe pas encore de spécifications détaillées sur la façon dont l'identification des risques doit être effectuée de manière harmonisée. Par ailleurs, pour les deux entités, les risques stratégiques doivent être ajoutés.

Une gestion des risques est effectuée au niveau des projets. Elle demande toutefois à être davantage formalisée chez RUAG International. Par ailleurs, les deux entreprises doivent clairement définir le lien entre cette gestion au niveau des projets et la gestion centrale des risques.

Le CDF s'est penché, parmi ses études de cas, sur les risques liés au toit de la Halle 3, un hangar à Emmen appartenant à RUAG MRO et où la maintenance des F/A 18 de l'armée suisse est effectuée. Pour lui, le risque d'effondrement du toit connu depuis 2019 n'a pas été géré de manière appropriée. Le CDF recommande à RUAG MRO d'approfondir sans délai l'analyse de la structure du toit et, le cas échéant, d'adapter les mesures prises ou d'en prendre de nouvelles.

La gestion de la conformité n'est pas encore complètement mise en place

En plus de la gestion des risques, l'audit du CDF portait sur la gestion de la conformité. RUAG MRO dispose d'une directive globale à ce sujet émise peu avant la clôture de cet audit. La vérification de sa mise en œuvre est ainsi prématurée. RUAG International dispose aussi d'une directive globale, ainsi que d'une directive portant sur l'alignement des initiatives, des processus et de documents clés. Le système a commencé à se mettre en place. Il manque toutefois un concept réglant l'intégration des filiales.

Prüfung des Risiko- und Compliancemanagements
BGRB Holding AG, RUAG MRO Holding AG, RUAG International Holding AG

Das Wesentliche in Kürze

Anfang 2020 wurde die RUAG in zwei Einheiten aufgespalten, die vom Bund über eine Beteiligungsgesellschaft (BGRB Holding AG) gehalten werden. Die RUAG MRO Holding AG (geschätzter Umsatz: 660 Millionen Franken) erbringt in erster Linie Leistungen für die Schweizer Armee. Die RUAG International Holding AG (geschätzter Umsatz: 1230 Millionen Franken) hat die Geschäftstätigkeit im Raumfahrtbereich übernommen und soll letztendlich privatisiert werden.

Die Eidgenössische Finanzkontrolle (EFK) stellt bei ihrer Prüfung fest, dass die RUAG, anders als vom Konzern im Dezember 2018 gegenüber dem Bundesrat behauptet, vor der Entflechtung über kein umfassendes Risikomanagement verfügte. Zwischen 2016 und Ende 2019 wurde dem Verwaltungsrat kein einziger konsolidierter Risikobericht vorgelegt.

Seither hat sich einiges getan. Alle neuen Einheiten erarbeiten ein eigenes Risikomanagement-Konzept und beginnen mit dessen Umsetzung. Die RUAG International hat bereits eine solide normative Grundlage geschaffen. Die Umsetzungsetappen sind jedoch noch nicht vollständig ausgeführt, weder inhaltlich noch hinsichtlich der Granularität. Die RUAG MRO musste wie ein «Spin-Off» eine Führungsstruktur zur Betreuung ihrer operativen Einheiten aufbauen. Sie ist im Hinblick auf die Richtlinien noch nicht so weit wie ihr Schwesterunternehmen, aber ihr detaillierter und koordinierter Aktionsplan überzeugt. Die Umsetzung des Compliancemanagements ist auch in beiden Einheiten im Gange.

Die Verwaltungsräte müssen Richtlinien festlegen

Die EFK empfiehlt den beiden Unternehmen, das Risikomanagement aus operativer Sicht und vor allem als «Bottom-up-Ansatz» zu stärken. Sie empfiehlt ihnen ausserdem, das Risikomanagement als Führungsinstrument zu integrieren und somit eine strategisch angemessene Integration im Sinne eines umfassenden Risikomanagements zu ermöglichen. Schliesslich sollten beide Unternehmen eine Übersicht über die Risiken erstellen.

Der Einbezug der leitenden Gremien ist von zentraler Bedeutung. Damit die beiden Verwaltungsräte ihre Kontrollfunktion und ihre strategische Rolle erfüllen können, empfiehlt ihnen die EFK, die Organisation des Risikomanagements regelmässig zu thematisieren, um ihren Informationsbedarf zu definieren und daraus klare Anforderungen an das Risikomanagement ableiten zu können. Diese in einer Aufbauphase sehr wichtigen Aspekte kamen bisher zu kurz.

In ihrem jeweiligen Konzept werden die Themen Appetit, Toleranz und Risikotragfähigkeit angeführt. Es fehlt aber noch eine Spezifizierung im Sinne eines Wertes oder einer Grössenordnung für die Tragfähigkeit gegenüber dem Geschäftsrisiko. Sobald diese Risikotragfähigkeit definiert ist, muss die Methode zur Risikobewertung entsprechend angepasst werden.

Empfohlene Verbesserungen in der Organisation und in den Prozessen

Bisher verfügen die RUAG MRO und die RUAG International über 2 bzw. 1,9 Vollzeitäquivalente für das zentrale Risikomanagement. Obwohl die Zentralorganisation durch ein Netz an Risikobeauftragten in den Verwaltungseinheiten ergänzt werden, erstaunt die Grössenordnung angesichts der Tatsache, dass sich die beiden Unternehmen bezüglich Grösse, Geschäftsmodell und internationalen Aktivitäten grundlegend unterscheiden. Es ist noch zu früh, um sich abschliessend zur Angemessenheit dieser Ressourcen zu äussern. In beiden Unternehmen müssen die Rahmenbedingungen verstärkt werden, um die Unabhängigkeit der in das Risikomanagementsystem beteiligten Personen zu gewährleisten.

In beiden Einheiten müssen die Risiken auf allen organisatorischen Stufen ermittelt werden. Die RUAG International ist dabei, einen Ausschuss einzurichten, der mit der Konsolidierung der ermittelten Risiken zuhanden der Direktion und des Verwaltungsrates beauftragt ist. Die RUAG MRO ihrerseits weist auf eine feste Anzahl an Hauptrisiken hin, die von den Einheiten oder Zentren ausgehen. Es gibt noch keine detaillierten Spezifikationen darüber, wie die Risikoermittlung in harmonisierter Art und Weise durchgeführt werden soll. Ausserdem müssen für beide Unternehmen die strategischen Risiken hinzugefügt werden.

Ein Risikomanagement wird auf Projektebene durchgeführt. Bei der RUAG International muss dieses jedoch noch stärker formalisiert werden. Beide Unternehmen müssen zudem klar definieren, wie dieses Projektrisikomanagement mit dem zentralen Risikomanagement verknüpft ist.

Im Rahmen ihrer Fallstudien hat sich die EFK mit den Risiken im Zusammenhang mit dem Dach der Halle 3, einem Hangar in Emmen im Eigentum der RUAG MRO befasst, in dem die F/A 18 der Schweizer Armee gewartet werden. Aus Sicht der EFK wurde mit dem seit 2019 bekannten Einsturzrisiko des Daches nicht angemessen umgegangen. Die EFK empfiehlt der RUAG MRO, die Dachkonstruktion ohne Verzug eingehender zu untersuchen und die getroffenen Massnahmen nötigenfalls anzupassen oder neue anzuordnen.

Das Compliancemanagement ist noch nicht vollständig umgesetzt

Neben dem Risikomanagement befasste sich die Prüfung der EFK auch mit dem Compliancemanagement. Die RUAG MRO verfügt über eine allgemeine, kurz vor Abschluss dieser Prüfung erlassene Richtlinie zu dieser Frage. Für ihre Überprüfung ist es also noch verfrüht. Auch die RUAG International verfügt über eine umfassende Richtlinie sowie eine zur Ausrichtung der Initiativen, Prozesse und Schlüsseldokumente. Das System steht am Beginn seiner Umsetzung. Allerdings fehlt noch ein Konzept für die Integration der Tochtergesellschaften.

Originaltext auf Französisch

Verifica della gestione dei rischi e della compliance
BGRB Holding SA, RUAG MRO Holding SA, RUAG International Holding SA

L'essenziale in breve

A inizio 2020 RUAG è stata suddivisa in due entità, detenute dalla Confederazione mediante una società di partecipazione (BGRB Holding SA). RUAG MRO Holding SA (cifra d'affari stimata: 660 mio. fr.) deve in primo luogo fornire servizi all'Esercito svizzero. RUAG International Holding SA (cifra d'affari stimata: 1230 mio. fr.) ha rilevato le attività aerospaziali e dovrebbe, a lungo termine, essere privatizzata.

Nella sua verifica, il Controllo federale delle finanze (CDF) constata che, contrariamente a quanto dichiarato da RUAG al Consiglio federale nel dicembre 2018, il gruppo prima dello scorporo non disponeva di una gestione globale dei rischi. Tra il 2016 e la fine del 2019, al consiglio d'amministrazione non è stato presentato alcun rapporto consolidato sui rischi.

Da allora, le cose sono cambiate. Ciascuna delle nuove entità sta sviluppando un piano di gestione dei rischi e sta iniziando a implementarlo. RUAG International ha già definito una solida base normativa. Tuttavia, le fasi di attuazione non sono ancora state integralmente definite, né in termini di contenuto né di granularità. RUAG MRO, che ha dovuto creare una struttura di gestione per supervisionare le proprie unità operative come uno «spin-off», non è ancora allo stesso livello della sua consociata in termini di direttive, ma il suo piano d'azione dettagliato e coordinato è convincente. Anche l'attuazione della gestione della compliance è in corso in entrambe le entità.

I consigli d'amministrazione devono stabilire le linee direttive

Il CDF raccomanda a entrambe le imprese di rafforzare la gestione dei rischi da un punto di vista operativo e, soprattutto, dal basso verso l'alto (bottom-up). Raccomanda inoltre di integrare la gestione dei rischi quale strumento di gestione e quindi di consentire l'integrazione strategicamente appropriata nel senso di una gestione globale dei rischi d'impresa. Infine, entrambe le imprese dovrebbero stabilire una panoramica dei rischi.

Il coinvolgimento degli organi direttivi è essenziale. Per poter svolgere la loro funzione di controllo e di strategia, il CDF raccomanda ai due consigli d'amministrazione di discutere regolarmente l'organizzazione relativa alla gestione dei rischi per definire il loro fabbisogno di informazioni e trarre chiare esigenze per la gestione dei rischi. Questi elementi, molto importanti in una fase iniziale, non sono stati finora presi sufficientemente in considerazione.

Nei loro rispettivi piani, RUAG MRO e RUAG International affrontano entrambi le tematiche dell'aspirazione, della tolleranza e della capacità di gestire i rischi. Manca ancora un'indicazione specifica per quanto riguarda un valore o un ordine di grandezza per la tolleranza ai rischi delle imprese. Una volta definita, occorrerà adeguare di conseguenza il metodo di valutazione dei rischi.

Necessità di miglioramento nell'organizzazione e nei processi

Ad oggi, RUAG MRO e RUAG International dispongono rispettivamente di 2 e di 1,9 equivalenti a tempo pieno per la gestione centralizzata dei rischi. Benché l'organizzazione centrale sia integrata da una rete di responsabili dei rischi nelle unità, questo tasso stupisce, dato che le due entità si differenziano fondamentalmente in termini di dimensioni, modello d'impresa e attività internazionali. È troppo presto per pronunciarsi definitivamente sull'adeguatezza delle risorse. Entrambe le imprese devono rafforzare le condizioni quadro per garantire l'indipendenza delle persone coinvolte nel sistema di gestione dei rischi.

In entrambe le entità i rischi devono essere individuati a tutti i livelli organizzativi. RUAG International sta istituendo un comitato incaricato di consolidare i rischi individuati all'attenzione della direzione e del consiglio d'amministrazione. Da parte sua, RUAG MRO segnala un numero fisso di rischi principali nelle unità o nei centri. Non esistono ancora specifiche dettagliate su come l'individuazione dei rischi debba essere effettuata in modo armonizzato. Inoltre, per entrambe le entità occorre aggiungere rischi strategici.

La gestione dei rischi è effettuata a livello di progetto. Tuttavia, presso RUAG International tale gestione deve essere maggiormente formalizzata. Inoltre, entrambe le imprese devono definire chiaramente il nesso tra questa gestione a livello di progetto e la gestione centrale dei rischi.

Tra i casi verificati, il CDF ha esaminato i rischi associati al tetto del padiglione 3, un capannone ubicato a Emmen di proprietà della RUAG MRO dove viene effettuata la manutenzione degli aerei da combattimento F/A-18 dell'Esercito svizzero. Secondo il CDF il rischio di crollo del tetto, noto dal 2019, non è stato gestito in modo adeguato. Il CDF raccomanda alla RUAG MRO di effettuare immediatamente un'analisi più dettagliata della struttura del tetto e, se necessario, di adeguare le misure adottate o di ordinarne di nuove.

La gestione della compliance non è ancora completamente attuata

Oltre alla gestione dei rischi, la verifica del CDF si è concentrata sulla gestione della compliance. RUAG MRO dispone di una direttiva globale su questo argomento, emanata poco prima della conclusione della presente verifica. È pertanto prematuro verificare l'attuazione di tale direttiva. RUAG International dispone anche di una direttiva globale nonché di una direttiva concernente l'armonizzazione di iniziative, processi e documenti chiave. Il sistema è stato avviato da poco. Manca tuttavia un piano che disciplini l'integrazione delle filiali.

Testo originale in francese

Audit of the risk and compliance management
BGRB Holding SA, RUAG MRO Holding SA, RUAG International Holding SA

Key facts

At the beginning of 2020, RUAG was split into two entities which are owned by the Confederation through a holding company (BGRB Holding AG). RUAG MRO Holding AG (estimated turnover: CHF 660 million) is primarily intended to provide services to the Swiss Armed Forces. RUAG International Holding AG (estimated turnover: CHF 1.23 billion) has taken over the aerospace business and should eventually be privatised in the long term.

In its audit, the Swiss Federal Audit Office (SFAO) found that, contrary to what RUAG had told the Federal Council in December 2018, the group did not have comprehensive risk management before being split. Between 2016 and the end of 2019, no consolidated risk report was presented to the Board of Directors.

Things have since changed. The new entities have each developed a risk management concept and are beginning to implement them. RUAG International has already established a solid normative basis. However, the implementation stages have not yet been fully completed, either in terms of content or granularity. RUAG MRO, which has had to create a management structure to oversee its business units as a spin-off, is not yet on the same level as its sister company in terms of directives, but its detailed and coordinated action plan is convincing. Compliance management is also being implemented in both entities.

The Boards of Directors should set guidelines

The SFAO recommends that both companies strengthen risk management from an operational and, above all, bottom-up perspective. It also recommends that they integrate risk management as a management instrument and thus allow for strategically appropriate integration in the sense of comprehensive enterprise risk management. Finally, both companies should establish a risk overview.

The involvement of the governing bodies is essential. In order to be able to fulfil its control and strategic function, the SFAO recommends that the two Boards of Directors regularly discuss the organisation of risk management in order to define their information needs and establish clear requirements for risk management. These elements, which are very important in a start-up phase, have not been sufficiently taken into account up to now.

In their respective concepts, RUAG MRO and RUAG International both address the topic of risk appetite, tolerance and capacity. There is still no specification in terms of a value or an order of magnitude for the companies' risk tolerance. Once this has been defined, the risk assessment method will have to be adapted accordingly.

Improvements recommended in terms of organisation and processes

To date, RUAG MRO and RUAG International have 2 and 1.9 FTEs, respectively, for central risk management. Although the central organisation is supplemented by a network of risk managers in the units, this ratio seems surprising in view of the fact that the two entities

differ fundamentally in terms of size, business model and international activities. It is too early to make a definitive statement on resource adequacy. In both companies, the framework conditions must be strengthened to guarantee the independence of those involved in the risk management system.

The identification of risks in both entities must take place at all organisational levels. RUAG International is in the process of appointing a committee to consolidate the identified risks and report them to management and the Board of Directors. For its part, RUAG MRO reports a fixed number of main risks from the units and centres. As yet, there are no detailed specifications on how the identification of risks is to be carried out in a harmonised manner. In addition, strategic risks are to be added for both entities.

Risk management is performed at project level. However, this needs to be formalised more at RUAG International. Furthermore, both companies must clearly define the link between this project-level management and central risk management.

One of the SFAO's case studies examined the risks associated with the roof of Halle 3, a hangar in Emmen belonging to RUAG MRO, where the maintenance of the Swiss Armed Forces' F/A-18s is carried out. In the SFAO's view, the risk of the roof collapsing, which was identified in 2019, has not been adequately managed. The SFAO recommends that RUAG MRO immediately carry out a more detailed analysis of the roof structure and, if necessary, adapt the measures taken or introduce new ones.

Compliance management still not fully established

In addition to risk management, the SFAO's audit focused on compliance management. RUAG MRO issued comprehensive directives on this subject shortly before the audit was completed. It is therefore too early to verify implementation. RUAG International also has comprehensive directives, as well as specific directives on the alignment of key initiatives, processes and documents. Work has started on putting the system in place. However, a concept governing the integration of subsidiaries is lacking.

Original text in French

Prise de position générale des audités

BGRB Holding

Das Begehren der BGRB Holding AG ein Audit des Risikomanagements bzw. der Risikomanagementsysteme der beiden Subholdings durchzuführen, bezweckte eine Analyse des Ist-Zustands, im Hinblick auf die zukünftige Umsetzung des strategischen Ziels des BR wonach die neu geschaffenen Subholdings über ein Unternehmensrisikomanagement verfügen sollen, welches sich an der ISO-Norm 31000 orientiert. Die Zeitspanne, in welcher auditiert wurde, war durch eine doppelte Ausnahmesituation gekennzeichnet: Die Entflechtung der RUAG Holding AG - die zur Schaffung von zwei neuen, sehr unterschiedlichen Subholdings, und insbesondere bei der MRO Holding AG zu einem Aufbau der Risikomanagements quasi von Null, geführt hat, sowie die Pandemie, die zu einer deutlich höheren Arbeitsbelastung der Managements und der Verwaltungsräte beider Subholdings wie auch des Verwaltungsrats der BGRB Holding geführt hat. Diese Tatsachen sind bei der Beurteilung der Risikomanagements entsprechend zu berücksichtigen. Das Ergebnis des Audits betreffend den Umsetzungsstand des Risikomanagements in den Subholdings wie auch die Bestätigung der Feststellung der Schwachstellen des BGRB Governance-Modells ist für die BGRB Holding AG von grossem Stellenwert.

Zu Ziff. 5.1 des Berichts

Art. 3 des Bundesgesetzes über die Rüstungsunternehmen des Bundes (BGRB) sieht vor, dass der Verwaltungsrat der Beteiligungsgesellschaft für die Umsetzung der strategischen Ziele des Bundesrates bei den Rüstungsunternehmen zu sorgen hat. In den strategischen Zielen des Bundesrates für die BGRB Holding AG für die Jahre 2020–2023 geht der Bundesrat jedoch über das Gesetz hinaus, indem er der BGRB die Verantwortung für die Erreichung der strategischen Ziele überträgt. Der Verwaltungsrat der Beteiligungsgesellschaft ist letzteren zufolge verantwortlich für die konzernweite Umsetzung der strategischen Ziele.

In Art. 4 BGRB ist vorgesehen, dass der Bund seinen Interessen entsprechend im Verwaltungsrat der Beteiligungsgesellschaft und die Beteiligungsgesellschaft ihren Interessen entsprechend in den Verwaltungsräten der Rüstungsunternehmen vertreten ist.

Die gesetzlichen Anforderungen sind zurzeit nicht umgesetzt: Die BGRB ist nicht in den Verwaltungsräten der Subholdings vertreten, im Verwaltungsrat der BGRB sitzen hingegen die zwei Präsidenten der Subholdings, und der Bund ist nicht seinen Interessen entsprechend im Verwaltungsrat der BGRB vertreten.

Die Verwaltungsratspräsidenten der Subholdings stehen durch ihren Einsitz im Verwaltungsrat der BGRB in einem Interessenkonflikt, da sie nicht gleichzeitig als Präsidenten des Verwaltungsrates der Subholding die Interessen der jeweiligen Subholding, als auch als Mitglieder des Verwaltungsrates der BGRB die Interessen der BGRB vertreten können.

Aus Governance-Gründen ist der unabhängige Verwaltungsrat der BGRB Holding AG in der heutigen Form weder berechtigt, noch verpflichtet, operativ auf die effektive Umsetzung der strategischen Ziele in den Subholdings Einfluss zu nehmen, weshalb er auch die Verantwortung für die Umsetzung der strategischen Ziele nicht tragen kann.

Es ist eine gesetzkonforme Vertretung des Bundes im Verwaltungsrat der BGRB, mit Einsitz des GS VBS und des Direktors EFV, sowie eine Vertretung der BGRB in den Subholdings (anstatt der heutigen Vertretung der Subholding in der BGRB) anzustreben. Die Vertretung des Bundes im VR der BGRB und in den Subholdings würde dem Bundesrat die Möglichkeit geben, im Falle einer Nicht-Konformität mit seinen Interessen zeitgerecht einzugreifen, was

mit dem heutigen Setup nicht möglich ist. Diese Notwendigkeit der Vertretung des Bundes in der im VR der BGRB zeigt sich aktuell gerade am Fall der RUAG International Holding AG, die sich in einer Devestitionsphase befindet, in der sich die kritische Lage Woche für Woche verändern kann und wofür die quartalsmässig stattfindenden Eignergespräche nicht ausreichen, damit der Eigner seine Interessen zeitgerecht wahren kann.

Zu Ziff. 5.2 des Berichts

Der Bundesrat erwartet von der Beteiligungsgesellschaft dafür zu sorgen, dass die operativ tätigen Konzerngesellschaften über ein Unternehmensrisikomanagementsystem verfügen, das sich an der ISO-Norm 31000 orientiert. Auch wenn der EFK beizupflichten ist, dass auf Stufe BGRB im 2020 zwar noch kein formalisiertes gruppenweites Herangehen an das Risikomanagement bestanden hat, muss doch festgehalten werden, dass das Thema Risikomanagement sowohl im Audit Committee, als auch im Verwaltungsrat ein ständig wiederkehrendes Traktandum war, welches vom Verwaltungsrat der BGRB mit der notwendigen Sorgfalt behandelt wurde bzw. eine Analyse und Beurteilung der konsolidierten Risiken auf Ebene BGRB durchaus vorgenommen wurde. Im Jahr 2020 wurden insgesamt 11 Sitzungen des Audit Committees und 13 Sitzungen des Verwaltungsrates abgehalten.

Der Fokus der BGRB lag im Jahr 2020 im Schaffen einer Risikotransparenz sowie in der Weiterführung und Festigung entsprechender Projekte auf Stufe der Subholdings.

Die BGRB hat aber keine Berechtigung, eine einheitliche Herangehensweise an Risiken zu definieren. Sie kann nur Empfehlungen abgeben.

RUAG MRO

RUAG MRO Holding SA (ci-après RUAG MRO) salue l'opportunité d'avoir été auditée par le CDF peu de temps après la dissociation de RUAG en deux compagnies distinctes et remercie le CDF pour le rapport d'audit ainsi que pour les recommandations formulées.

Depuis la dissociation, RUAG MRO a entrepris des efforts significatifs et convaincants, comme le reconnaît le CDF, pour développer et mettre en place une gestion des risques et de la conformité responsable et pérenne, dotée des ressources nécessaires.

Le développement conceptuel, basé sur le modèle des trois lignes de défense, et le renforcement des mesures opérationnelles progressent parallèlement et sont synchronisés régulièrement. Depuis la dissociation, les organes de direction de RUAG MRO sont informés périodiquement de l'avancée des travaux et des risques majeurs et sur ces bases participent activement au développement de la politique des risques et de la conformité.

L'introduction, actuellement en cours, d'une systématique d'identification, d'évaluation et de traitement des risques à tous les niveaux hiérarchiques de l'entreprise, pour les opérations comme pour les projets, permettra dans un futur proche de disposer d'informations harmonisées et consolidées pour la conduite de l'entreprise.

RUAG MRO reconnaît et soutient l'indépendance des instances responsables de la gestion des risques et de la conformité. Les adaptations nécessaires ont été décidées en automne 2020 et seront effectives dès janvier 2021.

Dans le cadre des échanges concernant la halle 3, RUAG MRO remercie le CDF pour l'expertise complémentaire et ses recommandations qui ont contribué à préciser la marche à suivre définie par RUAG Real Estate SA. RUAG MRO appuie les constatations de la vétusté du parc immobilier faite par le CDF, vétusté résultant de la politique financière du groupe RUAG avant dissociation, ainsi que de la nécessité de disposer d'une vue d'ensemble exhaustive et qualitative du portefeuille immobilier.

Dans le domaine de la conformité, RUAG MRO a fixé, dans un premier temps, la priorité en matière de prévention par la définition de processus et de règles internes. Comme pour la gestion des risques, une systématisation est en cours d'implémentation.

En ce qui concerne le travail du conseil d'administration de RUAG MRO, celui-ci a traité la gestion des risques de manière prioritaire et soutenue tout au long de l'année 2020, en exigeant des instances exécutives le développement et l'amélioration graduelle de son système de gestion des risques. Le comité d'audit a traité à chacune de ses séances les risques et les mesures de mitigation qui ont été régulièrement communiqués au conseil d'administration de BGRB Holding AG. Le conseil d'administration de RUAG MRO est satisfait des avancées faites dans le domaine de la gestion des risques et de la conformité durant cette première année d'exploitation. Au regard de la complexité des structures héritées, 2021 permettra au conseil de consolider ses exigences dans les domaines stratégiques, organisationnels, financiers et réglementaires.

RUAG International

RUAG International begrüsst die zentralen Feststellungen der EFK, dass die Konzeptionierung des ERM-Systems erfolgreich durchgeführt wurde und das Compliance Management System gut definiert ist und funktioniert. RUAG International teilt insbesondere auch die Auffassung der EFK, dass die Risikokultur als organischer Prozess beständig weiter zu entwickeln ist. In den letzten drei Jahren lag gerade auf diesem Aspekt ein wichtiger Fokus des Verwaltungsrats. Er hat den Aufbau des Compliance Management Systems sowie den Wechsel vom lokalen zum globalen Risikomanagement Prozess nicht nur initiiert, sondern auch eng begleitet. Die Feststellung der EFK, dass der «Tone-at-the-top» des Verwaltungsrats verbessert werden muss, ist deshalb – angesichts der zahlreichen persönlichen Gespräche der EFK mit dem Management und dem Verwaltungsrat sowie der vollumfänglichen Einsichtsgewährung in die Unterlagen von RUAG International – nicht nachvollziehbar.

Die meisten Empfehlungen der EFK zur weiteren Verbesserung von Compliance und Risikomanagement sind fachlich verständlich und die Initiativen zur Umsetzung der einzelnen Punkte laufen bereits. Es ist indes zu beachten, dass die tatsächliche Risikosituation sowie die Risikotragfähigkeit einer Unternehmung bei der Definierung der Compliance und Risikomanagement Prozesse sowie der Ressourcenaufstellung zentral sind. Bei RUAG International ist die risikoadäquate Priorisierung bei der Umsetzung unter effizientem Einsatz der Ressourcen aufgrund der gut strukturierten Organisation dieser Bereiche sowie der vorhandenen Expertise sichergestellt. RUAG International kann den grossen Teil der inhaltlichen Feststellungen der EFK bestätigen. Falsch ist jedoch die Behauptung, dass in der Entflechtung nicht alle Transformationsrisiken in einem formalisierten Risikomanagementprozess behandelt wurden. Risikomanagement war integraler Bestandteil jedes Workstream und wurde durch das Project Management Office regelmässig überprüft und im Lenkungssauschuss mit den Repräsentanten von VBS und EFD besprochen. Während des Entflechtungsprozesses waren die Transformationsrisiken zudem ein wichtiger Teil der Quartalsberichterstattung an den Eigner. Inhaltlich nicht korrekt ist überdies die Feststellung, dass die COVID-19-bezogenen Risiken in dem Group Risk Report für das erste Halbjahr 2020 gegenüber anderen Risiken ein zu starkes Übergewicht hätten. In diesem Risikobericht werden insgesamt 98 Risiken dargestellt, wovon nur ein kleiner Teil COVID-19-bezogen ist. Es liegt aber in der Natur dieser Krise, dass die COVID-19-bezogenen Risiken am höchsten zu bewerten waren und deshalb die Gegenmassnahmen ein Schwergewicht einnahmen.

Les prises de position ont été intégrées dans le rapport telles quelles et sans commentaires.

1 Mission et déroulement

1.1 Contexte

En 2018, le Conseil fédéral a pris la décision de scinder RUAG en deux. Les modalités de cette dissociation ont été fixées en mars 2019 par le gouvernement. D'un côté, RUAG MRO Holding SA (ci-après « RUAG MRO ») doit essentiellement fournir des prestations à l'armée suisse. De l'autre, RUAG International Holding SA (ci-après « RUAG International ») reprend les activités dans le domaine de l'aérospatial et devrait, à terme, être privatisée. En attendant, une société de participation financière (BGRB Holding SA, ci-après BGRB Holding), constituée uniquement d'un conseil d'administration, chapeaute les deux entités. Selon le calendrier fixé par le Conseil fédéral, la dissociation a officiellement eu lieu le 1er janvier 2020. Dans les faits, l'essentiel de la dissociation opérationnelle a été effectuée le 1er avril 2020.

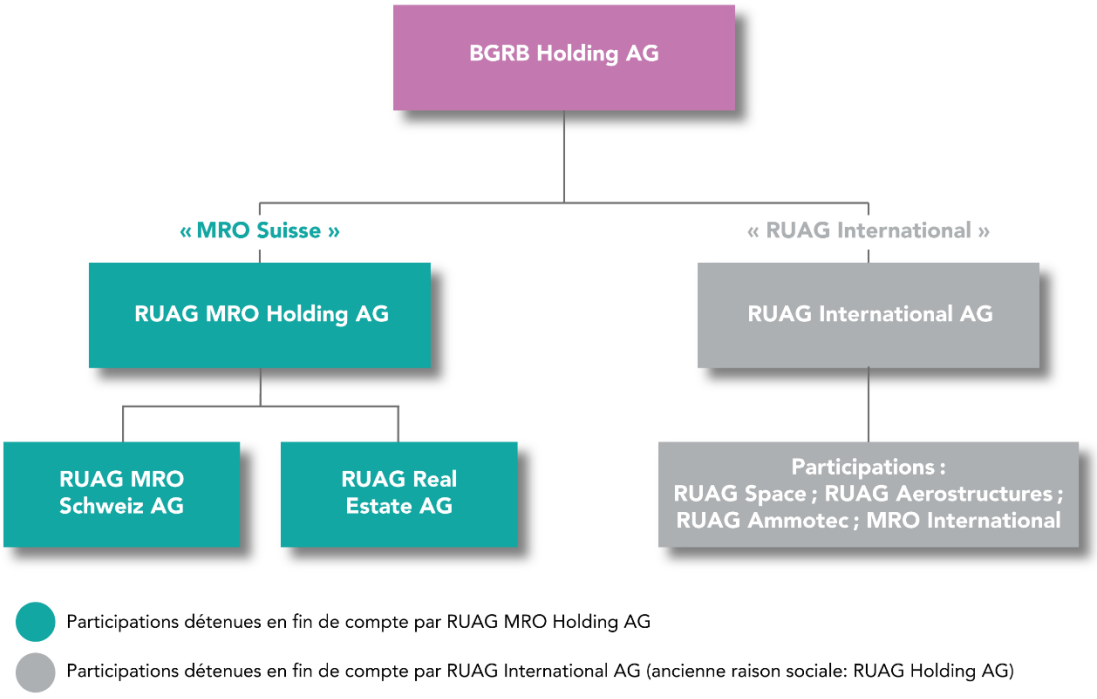

Illustration 1 : Nouvelle structure au 1er janvier 2020 (source : RUAG rapport de gestion 2019).

En octobre 2019, le Conseil fédéral a fixé des objectifs stratégiques à la société de participation ainsi qu'à RUAG MRO et RUAG International pour la période 2020–2023. Le propriétaire y précise que la gestion des risques doit s'appuyer sur la norme ISO 31000[1], ce qui n'était pas mentionné dans les objectifs stratégiques pour la période précédente.

[1] ISO 31000 guide les entreprises sur la manière d'intégrer la prise de décision fondée sur le risque aux processus de gouvernance, de planification, de management, de rapport, ainsi qu'aux politiques, aux valeurs et à la culture d'ensemble de l'organisme, source : www.iso.org.

1.2 Objectif et questions d'audit

L'audit vise à évaluer l'organisation et l'efficacité des systèmes de gestion des risques et de la conformité de BGRB Holding et des deux sous-groupes RUAG MRO et RUAG International. Les questions d'audits sont les suivantes :

1. L'organisation des trois sociétés permet-elle une gestion adéquate du risque et de la conformité ?
2. La gestion du risque a-t-elle été efficace durant la dissociation ?
3. La gestion du risque et de la conformité est-elle efficace dans les nouvelles structures ?
4. La gestion du risque est-elle efficace au niveau des projets ?

Le CDF s'est basé sur plusieurs études de cas couvrant différentes entités et projets, sélectionnés en fonction de critères de risques, pour répondre aux questions 3 et 4.

Dans son approche, le CDF a considéré le système de gestion des risques de chacune des sociétés dans sa globalité, comme illustré dans le schéma ci-dessous. Dans cette vision, le système de gestion de la compliance tend à être inclus dans celui de la gestion des risques. Ce qui ne signifie toutefois pas que cette subordination conceptuelle doit se refléter dans l'organisation.

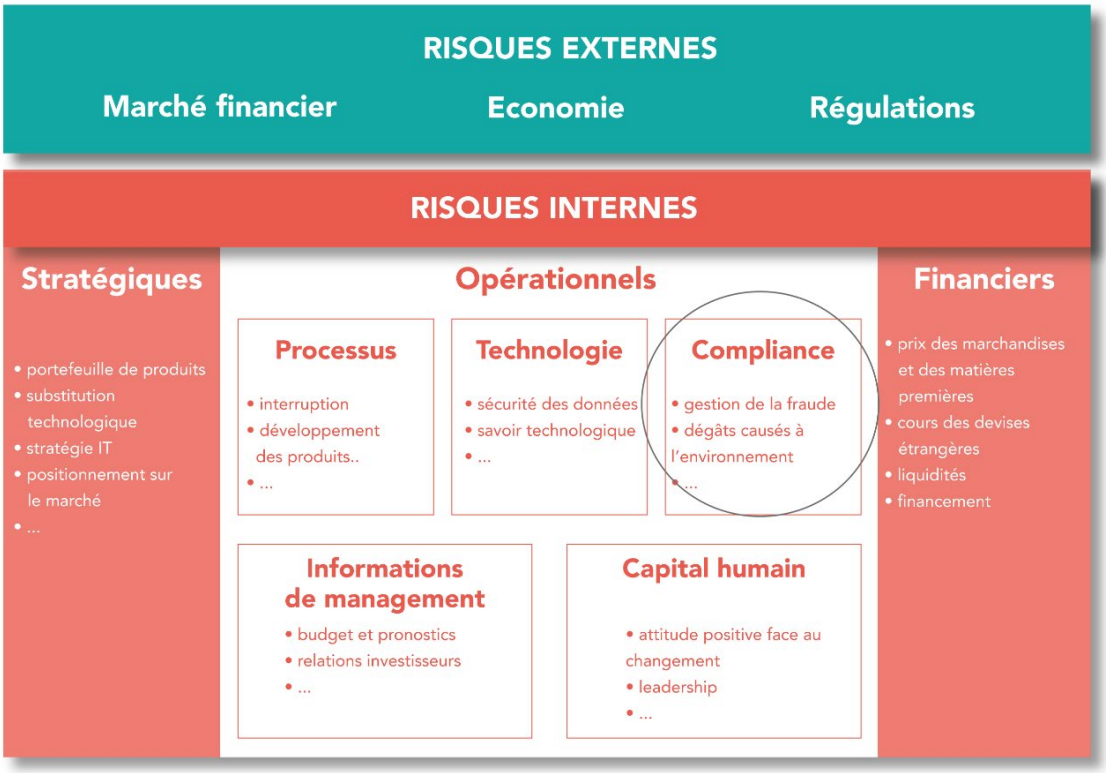

Illustration 2 : Schéma du système de gestion des risques (source : SECO, portail pour les PME).

Avant la dissociation, le système de compliance de RUAG avait été audité par le CDF. En 2016, un audit[2] relevait le fait qu'il n'était pas assez utilisé comme un outil de conduite par le conseil d'administration. Les risques étaient identifiés, mais pas suffisamment pris en compte. Une visite dans une usine d'Ammotec en Hongrie montrait que la gestion de la

[2] « Prüfung des Compliance Management Systems – RUAG » (PA 16532), 13 octobre 2016.

compliance n'avait pas été implémentée dans toutes les filiales. Le CDF avait alors recommandé de combler ces lacunes pour atteindre un meilleur niveau de maturité du système.

En 2018, le CDF a aussi procédé, à la demande des Délégation des finances du Parlement, à un audit sur l'exportation du matériel de guerre[3]. Aucune violation de la loi n'a été constatée dans les divisions auditées (Ammotec et Defence). Le CDF a cependant recommandé à RUAG de contrôler périodiquement ces questions d'exportations, aussi bien en Suisse que dans ses filiales à l'étranger.

Dans cet audit, une attention particulière a été apportée à la vérification de la mise en œuvre de ces recommandations de 2016 et 2018, bien qu'elles ont été adressées à RUAG avant la dissociation.

1.3 Etendue de l'audit et principe

L'audit du CDF s'est déroulé durant la phase de mise en œuvre de la gestion du risque et de la conformité dans les deux sous-groupes. De ce fait, il est trop tôt pour se prononcer sur l'efficacité de ces systèmes. Le CDF n'a pas audité les aspects de conformité sur la base de cas concrets, mais s'est concentré sur les concepts et leur degré d'implémentation. Il en va de même pour le risque: le CDF n'a pas audité de cas particulier, l'exhaustivité de l'inventaire, ni l'efficacité des mesures prises. Dans cette phase d'implémentation, ce rapport décrit la conception des systèmes et l'état de leur mise en œuvre pour identifier des améliorations. Il ne constitue donc pas une attestation sur la conformité.

Au niveau des recommandations, le CDF a également tenu compte du fait que les deux systèmes sont en phase d'implémentation. Il renonce ainsi à émettre systématiquement des recommandations pour chacun de ses constats et appréciations. Les recommandations sont regroupées à la fin de chaque chapitre.

Par ailleurs, en raison de la situation sanitaire liée au COVID-19, l'audit des filiales à l'étranger n'a pas pu se faire dans le cadre de visites sur place. Ces dernières ont dû être remplacées par des entretiens en vidéoconférence. Si ces discussions à distance ont permis de se faire une bonne impression générale de la situation, elles n'apportent pas la même assurance quant aux constats et appréciations qu'une visite sur place.

L'audit a été mené du 17 août au 6 novembre par Alexandre Bläuer, Peter König, Nicolas Marty, Benedikt Schlegel, Daniel Wyniger (experts en audit) et Alexandre Haederli (responsable de révision). Il a été conduit sous la responsabilité d'Oliver Sifrig. Les présentations des constats ont eu lieu les 3, 5 et 11 novembre 2020. Le présent rapport ne prend pas en compte le développement ultérieur à ces discussions.

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de manière exhaustive et compétente par les sociétés auditées. Les documents (ainsi que l'infrastructure) requis ont été mis à disposition de l'équipe d'audit sans restriction.

[3] « Prüfung der Compliance beim Transfer von Kriegsmaterial – RUAG» (PA 17658), 7 mai 2018.

1.5 Discussion finale

La discussion finale a eu lieu le 1er décembre 2020. Les participants étaient:

Pour BGRB Holding : la présidente et deux membres du conseil d'administration, le secrétaire.

Pour RUAG MRO : la présidente du comité d'audit et des risques, le CEO, le secrétaire général, le responsable de la gestion des risques.

Pour RUAG International : le président du conseil d'administration, le CEO, la secrétaire générale, le responsable des finances, le responsable de la gestion des risques et de la conformité, le responsable de l'audit interne.

Pour le CDF : le directeur, le responsable de centre de compétence, le responsable de révision et l'équipe d'audit.

Le CDF remercie l'attitude coopérative et rappelle qu'il appartient aux conseils d'administration, respectivement aux directions, des entités auditées de surveiller la mise en œuvre des recommandations.

CONTRÔLE FÉDÉRAL DES FINANCES

2 La dissociation de RUAG est synonyme de risques et d'opportunités

2.1 Une gestion globale et institutionnalisée du risque a longtemps été inexistante

Aucun rapport consolidé des risques entre 2016 et fin 2019

Dans les années précédant la dissociation, les risques chez RUAG n'étaient pas consolidés au niveau du groupe. Les risques étaient identifiés au sein des unités. Le comité stratégique du conseil d'administration discutait en outre des projets importants. Ce fonctionnement en silos, sans vue d'ensemble sur les risques, a duré de 2016 à 2019 et, durant cette période, aucun rapport global sur les risques n'a été présenté au conseil d'administration. En septembre 2019, le comité d'audit constate lui-même que « la gestion des risques a été négligée durant les deux ou trois dernières années »[4]. La priorité, durant cette période, a apparemment été donnée au développement de la conformité au sens large, en particulier à la conformité des exportations (Trade Compliance).

En août 2019, quelques mois avant la dissociation, RUAG a créé un poste de gestionnaire des risques au niveau du groupe avec un taux d'occupation de 60 %. Sa mission : créer un système de gestion des risques. En novembre 2019, un premier rapport des risques global est établi. Les cinq principaux risques au niveau du groupe sont recensés ainsi que les principaux risques pour chacune des divisions d'alors (Space, Aerostructures, MRO International, Ammotec et MRO Suisse). En revanche, ce document ne contenait aucun risque lié aux fonctions de support (ressources humaines, achats, informatique, sécurité de l'information, etc.). Il s'agit du dernier rapport sous cette forme. A partir de 2020, les nouvelles entités, RUAG International et RUAG MRO, ont chacune produite leur propre rapport sur les risques.

Parmi les dix-neuf risques figurant dans le rapport du mois de novembre 2019, deux se retrouvent dans le rapport des risques de RUAG International et quatre dans celui de RUAG MRO en mai 2020. Pour RUAG International, l'analyse des registres détaillés des risques sur lesquels sont basés ces rapports montre que des risques ont été repris, mais d'autres pas. Pour RUAG MRO, l'analyse des risques a recommencé de zéro avec la création de la société. Dans les deux cas, il y a une absence de traçabilité des risques avant et après dissociation. Les derniers rapports sont marqués de manière prégnante par l'apparition de risques liés au COVID-19: quatre sur les cinq principaux risques chez RUAG International et un sur huit du côté de RUAG MRO. Seul un risque lié à la transformation apparaît en lien avec une division dans ces rapports.

RUAG International hérite de l'organisation avant dissociation, RUAG MRO en mode spin-off

Du point de vue de l'organisation, RUAG International a repris le concept de gestion des risques élaboré en 2019 et le gestionnaire des risques engagé en novembre 2019. RUAG MRO a tout d'abord dû former une nouvelle structure encadrant ses unités opérationnelles, un peu comme une « spin-off ».

[4] Procès-verbal de la séance de direction de RUAG, 1 septembre 2019.

Dans le cadre de la dissociation, les modèles opérationnels des deux sous-groupes ont fait l'objet de réflexions, notamment sur la question des fonctions transversales comprenant notamment la gestion des risques et de la conformité. Une analyse quantitative et qualitative, avec l'étude de plusieurs variantes organisationnelles, a été effectuée pour le domaine de la Trade Compliance, qui constitue l'un des principaux risques en matière de conformité. Selon les entretiens, l'organisation générale de ces domaines de la gestion des risques et de la conformité a été thématisée, mais plutôt de manière marginale et sans être documentée. Des réflexions et des ajustements sont toujours en cours en 2020.

Appréciation

La gestion des risques est un élément crucial pour la conduite d'une société. D'autant plus quand celle-ci emploie plusieurs milliers d'employés, est active au niveau international et dans des secteurs aussi sensibles que le matériel de guerre ou l'aérospatial. Le fait que la gestion globale des risques a été négligée durant plusieurs années n'en est que plus problématique. Le rapport sur les risques publié en 2019, peu avant la dissociation doit être considéré comme une première étape importante et constitue notamment une contribution à la mise en place d'une culture du risque.

Dans les rapports des sous-groupes de mai 2020, la traçabilité des risques n'est pas toujours garantie et la fiabilité ne peut dès lors pas être assurée. Les éléments liés au COVID-19 sont prédominants et risquent de monopoliser l'attention. L'absence presque complète de risques en 2020 liés à la transformation parmi les risques principaux est difficilement compréhensible, alors qu'au moment de la publication de ces rapports les deux entités étaient en pleine réorganisation, et que des défis importants se posaient comme la fluctuation de personnel, le départ de personnes clés et le maintien du savoir-faire.

La conception et le développement d'une gestion des risques aurait dû être mûrement réfléchie avant la dissociation, notamment parce que la culture du risque avait été négligée depuis des années et qu'il y avait un important besoin de rattrapage.

2.2 Absence d'un cadre global institutionnel de gestion des risques durant la dissociation

Tous les risques liés à la transformation n'ont pas fait l'objet d'une gestion formalisée

En 2018, la transformation est organisée dans un programme baptisé « RUAG 2020 ». Ce dernier est subdivisé en trois sous-programmes : Dissociation, Maelstrom et Orion. Le premier se concentre sur la séparation juridique et opérationnelle, le second sur la définition du développement des différentes unités du futur RUAG International et le troisième sur les options de privatisation de RUAG International.

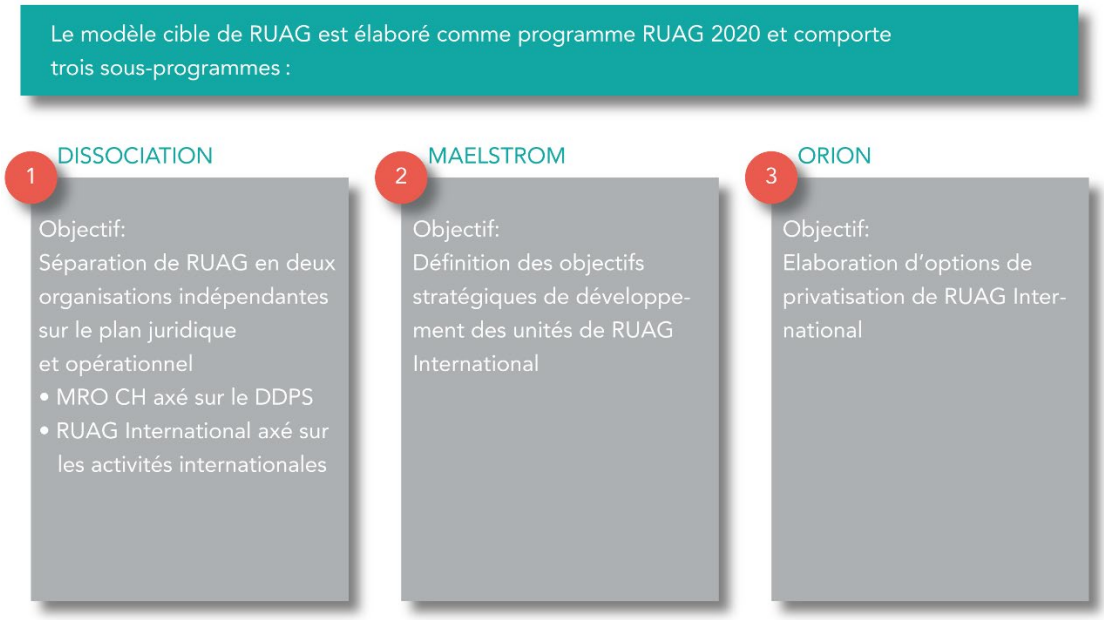

Illustration 3 : Organisation du programme « RUAG 2020 » (source : présentation interne de RUAG, 16.10.2018).

Les programmes « Maelstrom » et « Orion » ont abouti début novembre 2018 à la rédaction d'un livre blanc sur la stratégie et les options de privatisation de RUAG International. Ce document a été soumis au Conseil fédéral qui a choisi, en mars 2019, l'option de développer un groupe actif dans le domaine aérospatial. Les 53 pages de ce livre blanc ne contiennent aucune analyse des risques des différentes options. A la demande du propriétaire, RUAG comblera cette lacune en décembre 2018 avec une analyse de neuf pages sur les risques liés à la transformation ainsi qu'aux différentes options stratégiques. Ceux-ci sont organisés en trois catégories : risques externes (marché), risques internes (mise en œuvre) et risques liés à la gouvernance et à la politique.

Au-delà des risques pour RUAG International, le document transmis au Conseil fédéral affirme que RUAG avant dissociation dispose d'une gestion du risque couvrant « l'ensemble de l'entreprise », basée notamment sur la norme ISO 31000. Pour minimiser les risques liés à la transformation, RUAG annonce notamment vouloir élargir ce système existant de gestion des risques et accroître la rapidité de gestion grâce à un « Transformation Office » dédié. La documentation obtenue ne permet pas d'identifier qui s'est chargé de la gestion active des risques stratégiques évoqué dans ce document.

Les risques du programme « Dissociation » font l'objet d'une grande attention

Le programme « Dissociation » a pour sa part été subdivisé en plusieurs projets. Les risques ont été identifiés par chacun des responsables de projet puis agrégés par le responsable de programme. Il s'agit essentiellement de risques opérationnels liés au programme lui-même. Durant la première phase du programme, le responsable a régulièrement rappelé dans ses rapports ou ses échanges avec le comité d'audit que les risques liés à la transformation des deux nouvelles entités n'entraient pas dans la gestion des risques du programme « Dissociation ». Malgré cette communication transparente, aucune analyse approfondie sur la manière dont les risques liés à ces transformations pouvaient être traités n'a pu être fournie au CDF.

Lors de l'audit, le programme « Dissociation » se poursuit en vue de finaliser la dissociation. Pour cette deuxième phase, qui porte principalement sur les questions informatiques, la responsabilité de la gestion des risques est définie dans un mandat des conseils d'administration de RUAG MRO et de RUAG International. L'évaluation des risques est attribuée à un gestionnaire des risques indépendant qui a été intégré au *Program Management Office*.

Désinvestissements et informatiques sont sur le radar

Les désinvestissements passés ou à venir, découlant de la dissociation, sont gérés par RUAG International sous la forme de projets. Bien qu'il n'existe pas de gestion des risques *ad-hoc* pour chacun des projets, les risques sont pris en compte au moment d'envisager les différentes options ou acquéreurs. Dans les rapports globaux sur les risques de RUAG International, le cas d'un désinvestissement est évoqué. S'y ajoute, dans la dernière mouture du rapport, l'impact possible du COVID-19 sur tous les projets de désinvestissement. Ces risques concernent plutôt l'aspect financier.

Les risques informatiques dans le cadre de « Dissociation » font quant à eux l'objet d'une attention particulière et sont rapportés à un comité de pilotage spécialement dédié à l'informatique, instauré au cours du projet. Dans les rapports globaux des sous-groupes, aucun risque directement lié à la dissociation informatique n'est explicitement mentionné.

Appréciation

Les risques globaux liés à la transformation n'ont pas fait l'objet d'une gestion adéquate. L'absence d'un cadre institutionnel pour cette catégorie des risques qui aurait également permis d'assurer la transparence de leur traitement est problématique.

Selon l'analyse des risques qui complète le livre blanc, RUAG disposait en 2018 d'une gestion des risques à l'échelle du groupe qui répondait à la norme ISO 31000. Le CDF constate rétrospectivement qu'il ne s'agit en réalité que d'une déclaration d'intention. Un tel système n'existait pas à l'époque, comme relevé au chapitre précédant.

Les risques opérationnels liés à la dissociation, y compris dans le domaine informatique et les désinvestissements, ont été thématisés de façon adéquate. L'absence presque complète de ces risques dans les rapports globaux des sous-groupes n'est toutefois pas compréhensible.

Pour les désinvestissements, une formalisation de la gestion des risques serait souhaitable.

3 RUAG MRO

Si les unités opérationnelles qui composent RUAG MRO existaient avant la dissociation, la structure qui les encadre, du conseil d'administration aux fonctions de support, sont pour la plupart nouvelles. RUAG MRO est actuellement composée de quatre unités opérationnelles ainsi que des unités de services (finances, ressources humaines, marketing et ventes par exemple). Chaque unité opérationnelle regroupe plusieurs centres, eux-mêmes subdivisés en filiales ou actifs sur plusieurs sites. La conception et la mise en œuvre des systèmes de gestion des risques et de la conformité étaient en cours au moment de l'audit.

Ce chapitre est basé sur l'analyse de documents et d'entretiens dans l'organisation centrale de RUAG MRO, ainsi que sur différentes études de cas :

- Unité « Subsystems & Products » à Emmen, environ 510 collaborateurs et 169 millions de francs de chiffres d'affaires en 2019
- Filiale RUAG GmbH à Cassel (D), rattachée à l'unité « Landsystems », environ 17 collaborateurs et 19,3 millions de francs de chiffres d'affaires en 2019
- Projets Cobra (lance-mine), Detect & Avoid (système de détection automatique pour drones) et Halle 3 (sécurisation du toit d'un hangar à Emmen).

3.1 La conception de la gestion des risques avance, mais elle n'est pas encore aboutie

Des exigences détaillées pour la mise en place du système de gestion des risques font défaut

Une série de documents décrit le concept de gestion des risques telle qu'elle est prévue. Il existe aussi une feuille de route avec des éléments de concept qui sont encore à réaliser. Plusieurs documents ne sont toutefois pas encore définitifs et n'ont pas été approuvés par les instances dirigeantes.

La définition et la réalisation d'une gestion des risques se fonde uniquement sur l'objectif stratégique fixé par le Conseil fédéral. Il n'existe pas de document qui précise ces objectifs ou qui spécifie les attentes du conseil d'administration de RUAG MRO. La conception se fait essentiellement sur propositions des collaborateurs spécialisés, discutées puis validées par la direction ou le conseil d'administration. Les différentes options envisagées pour la conception de la gestion des risques, y compris les décisions prises, n'ont pas été documentées.

L'ancrage dans l'organisation doit être revu

La gestion des risques est conduite par l'unité « Business Services & IT ». Un gestionnaire des risques est subordonné au responsable de cette unité. Ce dernier siège à la direction et dispose d'un accès direct au conseil d'administration de RUAG MRO. Selon RUAG MRO, un changement organisationnel est prévu au 1er janvier 2021. La gestion des risques devrait être rattachée au Secrétariat général dans le but de réduire le risque de conflit d'intérêts. Cette modification de l'organigramme doit encore être validée par le conseil d'administration. Au total, deux équivalents plein temps (EPT) devraient être consacrés à la gestion centrale des risques. Un outil informatique de gestion centralisée des risques est en cours de déploiement.

La gestion décentralisée des risques se fait quant à elle par un Risk Coach désigné dans chaque unité et dans chaque centre. Il ne s'agit pas d'une fonction à plein temps, elle est intégrée à des postes existants. Par exemple : le Risk Coach de l'unité « Subsystems & Products » à Emmen est en même temps le responsable de la gestion de la qualité. Neuf Risk Coaches devraient être désignés ce qui représenterait un total de 0,9 EPT. Les Risk Coaches au niveau des unités ont été définis, mais les études de cas montrent qu'en octobre 2020, ils n'avaient pas encore été désignés dans les centres, les filiales et les sites. Par ailleurs, les descriptions de poste des Risk Coaches nommés n'ont pas encore été adaptées. Ils rapportent *(dotted reporting line)* au gestionnaire central des risques.

Appréciation

Les exigences spécifiques pour le développement et la mise en place du système de gestion des risques, venant du conseil d'administration de RUAG MRO font défaut. Celui-ci porte pourtant la responsabilité dans ce domaine. Pour le CDF, relayer l'exigence, fixée dans les objectifs stratégiques du Conseil fédéral, de la mise en place d'un système répondant à la norme ISO 31000 n'est pas suffisant. Le conseil d'administration devrait spécifier concrètement ses attentes, par exemple en terme d'organisation, de périodicité des rapports ou de leur niveau de détail. Les personnes responsables de la gestion des risques devraient ensuite proposer différentes variantes à même de remplir ces exigences. Cela permettrait au conseil d'administration de s'assurer que la mise en place correspond à ce qu'il a voulu d'une part et d'autre part de mieux exercer ses fonctions de pilotage et de contrôle. Il permettrait en outre d'éviter qu'il n'intervienne après-coup, ce qui est inefficace. De plus, il soulignerait ainsi l'importance de ce domaine.

Le concept de gestion des risques prévu par RUAG MRO a – s'il est réalisé comme prévu – de bonnes chances d'aboutir à un système adéquat. L'implémentation dans toute l'organisation, notamment la désignation de tous les Risk Coaches, doit se poursuivre.

La position du responsable de l'unité « Business Services et IT » ne permet pas d'exclure un conflit d'intérêt entre ses fonctions opérationnelles et celles de Chief Risk Officer. Cette question doit impérativement être réglée comme prévu. Le CDF s'attend à ce que l'accès direct au conseil d'administration soit préservé, quelle que soit la solution retenue. L'organisation décentralisée est aussi susceptible de créer des conflits d'intérêts pour les Risk Coaches, qui n'ont pas suffisamment été thématisés.

Engagement visible des instances supérieures

Les procès-verbaux des séances du conseil d'administration et du comité d'audit (Audit & Risk Committee) montrent que la thématique des risques est régulièrement abordée. L'engagement des instances supérieures est visible de ce point de vue.

La capacité à supporter les risques ainsi que la tolérance dans ce domaine n'a pas été définie au niveau du groupe. Selon la feuille de route, cet élément était prévu pour le mois d'août 2020. Il n'a pas encore été concrétisé. Actuellement, le choix de la cartographie des risques s'appuie sur celle utilisée dans l'administration fédérale avec une matrice où chaque axe compte six niveaux.

L'importance de la gestion des risques a été communiquée par la direction à l'ensemble des collaborateurs de RUAG MRO dans un courriel d'avril 2020. Par ailleurs, la gestion des risques fait partie des objectifs collectifs fixés aux cadres de l'entreprise pour 2020. Malgré ces éléments, les entretiens menés dans le cadre des études de cas font ressortir le besoin de clarification de la plus-value d'un système performant de gestion des risques.

Appréciation

La sensibilité des instances dirigeantes à la thématique des risques est démontrée, mais les attentes et limites devraient être fixées de manière chiffrée. En quantifiant la capacité à supporter les risques ainsi que sa tolérance dans ce domaine, le conseil d'administration fixerait un cadre pour la prise de décision.

Le choix de s'appuyer d'abord sur la cartographie des risques utilisée par l'administration fédérale est compréhensible. Mais il ne doit pas exclure une réflexion sur l'adéquation de cette cartographie aux besoins spécifiques à RUAG MRO, notamment vu la taille de la société et de son appétence aux risques, une fois que cette dernière aura été définie.

L'ajout de la gestion des risques dans les objectifs annuels des cadres, qui peut avoir une influence sur leur revenu, devrait faciliter la mise en œuvre du projet. Des incitations pour favoriser une gestion proactive et une identification précoce des risques manquent.

Afin que la gestion des risques ne soit pas considérée comme un « tigre de papier », le travail de communication doit continuer auprès de l'ensemble des collaborateurs. L'utilité dans les processus opérationnels et la plus-value du nouveau système pour les collaborateurs eux-mêmes doivent clairement être démontrées pour faciliter son adoption.

3.2 Le concept global de gestion de la conformité vient d'être approuvé

La gestion de la conformité est coordonnée par le Senior Compliance Manager, actuellement subordonné au service juridique, lui-même rattaché au secrétariat général. Au total, 6,8 EPT devraient être dédiés à la conformité, avec un fort accent sur la thématique des exportations (Trade Compliance avec quatre EPT). En septembre 2020, le recrutement pour deux postes nouvellement créés (Compliance Officer et Data Protection & Compliance Officer) étaient en cours. Selon RUAG MRO, il est prévu, à partir du 1er janvier 2021, que le Senior Compliance Manager rapporte directement au secrétaire général. Le gestionnaire de la conformité « monterait » ainsi d'un niveau dans l'organigramme, tout en disposant d'un accès direct au conseil d'administration. Ce dernier doit encore valider ce changement dans l'organigramme.

Les activités en matière de conformité se focalisent sur la prévention, notamment par l'élaboration de directives et l'organisation de formation, d'actions concrètes définies dans les processus opérationnels, ainsi que sur les mitigations de violations de la conformité.

Une directive globale sur le système de gestion de la conformité a été approuvée juste avant la clôture de l'audit du CDF. Elle décrit les domaines qui relèvent de la conformité : éthique des affaires (code de conduite, conflits d'intérêts), conformité des exportations (Trade Compliance), conformité commerciale (corruption, relation avec des tiers) et protection des données. Chacun de ces thèmes dispose de sa propre directive. La directive générale prévoit entre autres la désignation d'une personne de contact, appelée « Compliance Partner », dans chacune des unités.

L'implication régulière du conseil d'administration et le comité d'audit dans le domaine de la conformité est documenté dans les procès-verbaux des séances. La décision d'un audit externe de la conformité en 2021 a été prise.

Appréciation

Le système de gestion de la conformité est ancré dans les processus opérationnels et la récente directive globale sur la gestion de la conformité définit un cadre au sens large. La nomination des « Compliance Partner », éléments clés du dispositif, devrait intervenir aussi rapidement que possible et permettre d'augmenter sensiblement le niveau de maturité du système.

Le changement de position du responsable de la conformité dans l'organigramme donnera davantage d'importance et de visibilité à la conformité. Autre point positif : le conseil d'administration s'implique régulièrement dans le domaine de la conformité. Le CDF encourage RUAG MRO à poursuivre l'idée de faire auditer le système de conformité.

3.3 La mise en œuvre pratique de la gestion des risques

Risques stratégiques et existentiels à identifier et évaluer de manière exhaustive

Il est prévu que les risques principaux de RUAG MRO soient consolidés dans un rapport global deux fois par année puis présentés et discutés avec la direction et le conseil d'administration. Par ailleurs, depuis mai 2020, une présentation sur les risques est faite lors de chaque séance du conseil d'administration et de la direction. Ces rapports contiennent une description des risques, une indication sur ceux qui sont nouveaux, ainsi que les mesures de mitigation. Les documents à disposition ne laissent pas transparaître la manière dont les risques ont été consolidés dans ce rapport. Ce dernier ne donne pas d'information en matière de cumul, ni sur les effets de combinaison des risques *(worst case scenario)*.

Un risque stratégique, lié à la forte dépendance de RUAG MRO à l'armée suisse, apparaît dans les rapports. Les risques stratégiques et existentiels pour l'entreprise ne sont toutefois pas tous formalisés et intégrés dans le système gestion des risques.

Appréciation

La production d'un rapport global sur les risques est une première étape importante, mais des éléments indispensables à la gestion du groupe – les risques stratégiques et existentiels – devraient être systématiquement formalisés et intégrés dans le système de gestion des risques.

Le processus de consolidation des risques n'est pas encore satisfaisant. Il devrait inclure des réflexions à tous les niveaux organisationnels en se concentrant sur l'impact au niveau du groupe. Une vision cumulée des risques devrait être ajoutée au rapport et inclure les effets de combinaison.

Améliorer l'exhaustivité de l'inventaire des risques à tous les niveaux organisationnels

Lors des contrôles réalisés en octobre 2020 dans deux entités de RUAG MRO, l'inventaire des risques ne comprenait pas encore tous les risques identifiés et actuels. Pour le site à Emmen, couvrant notamment les activités de l'unité « Subsystems & Products », les risques de conformité et certains risques au niveau des centres font par exemple défaut. Pour Cassel, l'inventaire ne contient aucun risque spécifique aux activités en Allemagne. A titre d'exemple, ces risques pourraient inclure des défauts de paiements, la non-conformité avec les lois et directives allemandes et suisses dans le domaine des exportations, ainsi qu'un changement des lois et des directives dans le domaine du commerce extérieur (embargos, reclassifications, etc.).

La stratégie était de se focaliser dans un premier temps sur les risques à reporter à la direction et au conseil d'administration. Un coaching étroit a été réalisé entre le gestionnaire des risques pour le groupe et les Risk Coaches des unités. Le but était d'obtenir une qualité d'information uniforme entre les unités pour qualifier et évaluer les risques identifiés. L'intégration des risques significatifs (au-delà des cinq risques principaux rapportés aux instances supérieures) auxquels s'exposent chaque niveau organisationnel fait encore défaut.

Appréciation

Au moment de l'audit, l'identification harmonisée et complète des risques n'est encore pas donnée. L'identification des cinq risques principaux par unité n'est pas suffisante. Pour chaque niveau organisationnel, le système devrait garantir une identification harmonisée pour toutes les catégories de risques et dimensions définies.

Les outils de gouvernance et de reporting ne suffisent pas encore

Le domaine du risque au sens large n'est pas couvert et traité de manière systématique et standardisée dans les outils de gouvernance existants à chacun des niveaux organisationnels. Il n'existe pas de rapport standard permettant d'avoir une vue d'ensemble sur les risques auxquels s'expose chaque unité, centre, filiale ou site.

La gestion des risques fait partie intégrante de certains outils de gouvernance comme les TIER Boards ou les comités opérationnels institués au sein des niveaux organisationnels de chaque unité ainsi qu'au niveau de la direction. Mais le lien entre ce qui est discuté lors de ces réunions et le système centrale de gestion des risques n'est pas clairement défini.

Appréciation

Le concept de gestion des risques devrait prévoir un reporting standardisé, permettant au responsable de chaque niveau organisationnel d'avoir une vue d'ensemble sur les risques.

Les outils de gouvernance (les comités et les protocoles correspondants) ne suffisent pas encore pour évaluer si la gestion des risques au sens large est discutée et « remontée » à la hiérarchie de manière appropriée. L'agenda devrait systématiquement comporter des thématiques en rapport avec la gestion des risques. Une alternative serait d'instaurer un comité dédié à la gestion des risques. Cela permettrait d'assurer un échange d'informations et d'expériences liées à ces thématiques entre les organisations centralisées et décentralisées *(community)*.

Gestion des risques diversifiée au sein des projets

Le manuel pour la gestion de projet de RUAG MRO, mis à jour en mars 2020, spécifie les exigences et les rôles en matière de gestion des risques en s'appuyant sur le norme ISO 31000. Des modèles de documents sont mis à disposition des responsables de projet. Il est prévu que la gestion des risques des projets importants se fassent directement dans l'outil informatique centralisé.

Le développement du lance-mine Cobra pour l'armée suisse fait en 2020 l'objet d'une gestion des risques basée sur les standards en vigueur au moment du lancement du projet, en 2015. Il ressort toutefois des entretiens que cette gestion des risques n'a pas toujours fonctionné correctement. Les risques mentionnés dans la description initiale du projet se sont pratiquement tous réalisés (par exemple le manque de savoir-faire et de ressources). Le CDF n'a pas audité ces points en détail, mais constate que ces risques initialement identifiés n'ont pas été suivis par la suite.

Autre projet : le développement d'un système de détection et d'évitement (Detect & Avoid System) pour les nouveaux drones acquis par l'armée suisse. Les risques font l'objet d'une gestion correspondant à la méthodologie qui était applicable en 2016, au moment du lancement du projet. Le CDF n'a pas audité l'efficacité des mesures prises pour minimiser ces risques.

Le troisième projet sous revue concerne la Halle 3, un hangar appartenant à RUAG MRO et situé à Emmen. C'est là qu'est effectué l'entretien des F/A 18 de l'armée suisse. Une présentation du directeur de RUAG Real Estate, datée du 21 octobre 2019, indique que la structure du toit et la structure porteuse du bâtiment ne remplissent plus les exigences. Un fléchissement de la structure primaire est notamment constaté. Selon ce document, il n'est plus possible de se rendre sur le toit en raison du risque d'effondrement. Ce risque n'apparaît pas dans le rapport sur les risques avant la dissociation de RUAG (novembre 2019). Ce n'est qu'après la dissociation qu'il apparaît pour la première fois dans un rapport des risques à la direction générale le 18 mai 2020 et dans celui destiné au conseil d'administration du 17 juin 2020. Dans ces rapports et les suivants, l'effondrement du toit avec comme possible conséquence la mise en danger de vies et la mise hors service de jusqu'à dix avions de chasse apparaît comme le principal risque de RUAG Real Estate. Selon RUAG MRO, les forces aériennes auraient été informées du risque. RUAG MRO n'a toutefois pas été en mesure d'établir les circonstances, ni de fournir une trace de cette information.

Bien que le projet de sécurisation du toit de la Halle 3 fasse l'objet d'une gestion des risques correspondant aux nouvelles exigences du groupe, le CDF constate qu'une cause majeure (« structure des bâtiments existants problématique ou inconnue ») figurant dans l'inventaire des risques du projet n'a pas été rapportée au comité de pilotage, ni à la direction ou au conseil d'administration de RUAG MRO.

Entre la visite du CDF sur place et la clôture de l'audit, un mandat a été attribué à une société externe pour évaluer la structure porteuse de la Halle 3. Les résultats sont attendus pour fin janvier 2021. Par ailleurs, deux rapports d'essai portant sur la structure du toit ont été établis. Sur la base de ces derniers, RUAG Real Estate a décidé la mise en place d'un concept de sécurité et d'observation ainsi que de mesures hivernales, notamment l'enlèvement de la couche de gravier présente sur le toit ainsi qu'un concept de déneigement pour éviter une surcharge. RUAG MRO s'est engagé à soumettre sans délai à l'agence lucernoise de la SUVA une information concernant la situation, les concepts et les mesures.

Vue d'ensemble sur le parc immobilier nécessaire

Au-delà du cas particulier de la Halle 3 à Emmen figure parmi les principaux risques identifiés par RUAG Real Estate la vétusté du parc immobilier. La question se pose de savoir s'il ne serait pas opportun de disposer d'une vue d'ensemble de l'état des biens immobiliers de RUAG MRO. Un portefeuille immobilier vétuste ou insuffisamment entretenu peut mettre en péril l'obtention de permis pour des activités opérationnelles modernes. Cette vue d'ensemble du parc immobilier devrait indiquer, pour chaque bien, différents éléments, comme la capacité à obtenir les autorisations d'exploitation nécessaires sur le long terme, les possibilités de prolongation de la durée d'exploitation, les utilisations ultérieures possibles, la situation en termes de sécurité, de santé et d'environnement ou encore une analyse coûts-efficacité.

Appréciation

Une gestion des risques a été mise en place dans chacun des trois projets audités, mais elle est réalisée à chaque fois d'une manière différente. Les exemples audités montrent différents points qui demandent à être améliorés, en particulier la cohérence et la traçabilité des risques. De manière générale, la qualité du reporting des risques de projets devrait être améliorée.

En ce qui concerne le projet Cobra, les évènements passés indiquent, pour le CDF, une forte volonté de prendre des risques alors que, dans le même temps, la gestion des risques était relativement faible.

Pour le projet Halle 3, il est incompréhensible que le risque lié à un possible effondrement du toit, identifié par RUAG Real Estate au moins depuis 2019 et dont les conséquences pourraient être graves d'un point de vue humain, sécuritaire et financier, n'apparaisse avant mi-mai 2020 dans aucun des rapports sur les risques fournis au CDF et que les organes de direction n'aient été informés qu'après la dissociation. Il est aussi difficile de comprendre pourquoi les forces aériennes n'ont pas été formellement et régulièrement informées. Dans le rapport de mai 2020, comme dans les suivants, il manque une information essentielle : le risque lié au manque de connaissance de l'état de la structure du bâtiment. Cette lacune aurait dû remonter jusqu'au rapport, et être complété par des mesures validées par la direction générale ou le conseil d'administration. Le CDF prend connaissance du fait qu'un mandat externe a très récemment été émis pour l'analyse de la structure de soutien du bâtiment (structure primaire). Concernant la structure du toit (structure secondaire), les rapports d'essai récemment réalisés ne contiennent aucune indication sur la charge maximale (par exemple en kilogrammes par mètre carré) supportable. De ce fait, ils ne constituent pas une base permettant d'affirmer que le déneigement prévu soit adéquat, suffisant et réalisable. Tant que les connaissances de la structure du toit et du bâtiment sont incomplètes, le bienfondé des mesures décidées ne peut être validé.

La manière dont les risques de projets seront inclus dans le système global de gestion des risques doit être clarifiée. Le fait que certains projets plus « anciens » suivent une méthodologie différente n'est pas problématique en soi. Mais afin d'obtenir une image consolidée et significative des principaux risques au sein de l'entreprise, RUAG MRO devrait adapter la méthodologie pour les projets gérés avec des systèmes de gestion des risques antérieurs. Cela permettrait de s'assurer que les risques des projets soient évalués de manière uniforme.

3.4 La mise en œuvre de la gestion de la conformité est très fragmentée

Un processus existe dans plusieurs domaines spécifiques, comme la Trade Compliance ou la collaboration avec des agents (Third Party Management). Lorsqu'un contrat est en passe d'être conclu, le responsable de la conformité effectue une série de vérifications, à l'aide d'un outil informatique dédié. Il doit donner son aval avant que le contrat soit signé. La durée d'un contrat ne peut excéder trois ans. S'il est renouvelé, un nouveau contrôle est effectué. Par ailleurs, en dehors de ces contrôles prévus dans les processus, des vérifications sont effectuées lorsqu'un doute sur un agent survient.

A l'instar du domaine du risque, il n'existe pas de reporting standardisé de la conformité. Des réflexions sont en cours pour assurer une communication et un échange d'information appropriés, comme l'édition d'un rapport annuel sur la thématique liée à la compliance.

Du point de vue de l'organisation à Cassel, une ligne de reporting des fonctions de support (finances, qualité, informatique, etc.) de RUAG GmbH envers le groupe n'a pas été formalisée, contrairement à ce qui est établi pour les entités décentralisées en Suisse. Cela s'applique également en ce qui concerne les activités liées à la Trade Compliance effectuées en Allemagne.

Toutes les directives édictées par le groupe RUAG MRO ne peuvent pas encore être suivies strictement par RUAG GmbH en raison des spécificités allemandes (par ex. droit de signatures et règles en matière de cadeau). Une planification des activités liées aux adaptations et simplifications des directives existe.

Appréciation

Les directives disponibles, par exemple concernant la collaboration avec des agents (Third Party Management) ou la conformité des exportations (Trade Compliance) ont été rédigées et sont entrées en vigueur le 1er septembre 2020, soit au cours de l'audit du CDF. Il est dès lors trop tôt pour se prononcer sur leur implémentation et effectuer des contrôles ciblés par sondage.

Toutes fonctions et activités devraient disposer d'une ligne de reporting dans leur organisation fonctionnelle (fonctions de support, Trade Compliance, etc.).

Toutes les adaptations des directives du groupe selon les spécificités locales devraient être quittancées par le groupe.

3.5 Contrôles internes en lien avec la gestion des risques et de la conformité à étendre et à formaliser

Les activités de contrôles sont seulement indiquées au niveau des directives et des instructions de travail. Un registre central regroupant de manière standardisée les contrôles, leur description et leur fréquence fait encore défaut.

La deuxième ligne de défense[5] réalise notamment des actions concrètes définies dans les processus opérationnels (par exemple dans le domaine Trade Compliance ou Third Party Management). Elle effectue peu de contrôles sur l'efficacité des processus opérationnels mis en place par la première ligne de défense, que ce soit de manière globale et standardisée (par exemple à l'aide d'analyse de données, monitoring, testing) ou orientées sur les risques auprès des filiales. Selon RUAG MRO, cette situation est liée à la dissociation et la réorganisation de l'entreprise. Par le passé, des contrôles et des audits spécifiques (dans les domaines Quality ou Trade Compliance par exemple) ont été réalisés, soit par le groupe, soit par les autorités (notamment en Allemagne). En 2020, RUAG MRO a effectué une autoévaluation couvrant l'organisation et les processus liés à la conformité. Des faiblesses dans les domaines du périmètre du système de gestion de la conformité, des processus d'évaluation de risques et des activités de monitoring ont été identifiées. Les mesures définies sont en cours d'implémentation.

[5] Dans le modèle des trois lignes de défense tel que proposée par The Institute of Internal Auditors (IIA), la première ligne correspond aux contrôles pilotés par le management, la seconde aux fonctions instituées par le management pour assurer le suivi du contrôle des risques et de la conformité et la troisième à l'assurance indépendante fournie par l'audit interne.

Les entités responsables de la gestion des risques et de la conformité n'effectuent pas non plus de contrôles de qualité standardisés et formalisés dans leur propre organisation. Cette supervision a surtout été réalisée de manière informelle (par exemple sur la base des échanges réguliers entre les différents niveaux hiérarchiques).

Appréciation

Le cadre de contrôle au niveau de la gestion des risques et de la conformité n'est pas suffisamment formalisé. Dans un système mature, RUAG MRO devrait disposer d'un contrôle interne au sens large qui ne se limite pas au domaine des finances et qui inclut la gestion des risques et de la conformité. Actuellement la deuxième ligne de défense n'est pas suffisamment en mesure de connaître, comprendre et apprécier les risques dans ces domaines.

3.6 Recommandations

Appréciation générale

Dans l'ensemble, la conception du système de gestion des risques de RUAG MRO est en bonne voie. Les études de cas montrent qu'il n'a pas encore été déployé aux niveaux inférieurs de l'organisation. Dans le cadre de son développement, RUAG MRO devrait prêter une attention particulière aux points qui suivent.

Recommandation 1 (Priorité 1)

Le CDF recommande au conseil d'administration de RUAG MRO :

- de formuler, en consultation avec BGRB Holding, ses exigences et ses attentes en matière de gestion des risques et ainsi établir une base pour la mise en place du système par les spécialistes du domaine
- de surveiller régulièrement la réalisation des objectifs et l'état de la mise en œuvre du système de gestion des risques
- de s'assurer que les personnes impliquées dans la gestion des risques disposent de l'indépendance nécessaire pour palier à tout conflit d'intérêts potentiel (par exemple une ligne de reporting fonctionnel ou des objectifs en lien avec la gestion de risque)
- de quantifier la capacité à supporter les risques ainsi que sa tolérance aux risques au niveau du groupe. Ces éléments devraient ensuite être déclinés pour les différentes unités. Les règles d'évaluation des risques et la cartographie devraient être adaptées sur cette base.

Prise de position de RUAG MRO

Les conditions-cadres pour BGRB et RUAG MRO en matière de gestion des risques sont clairement définies par l'objectif stratégique du Conseil fédéral y relatif, la norme ISO mentionnée réglant exhaustivement le domaine d'application.

Suite à la dissociation, RUAG MRO a démarré l'implémentation de la gestion des risques à deux niveaux, d'une part au niveau conceptuel et d'autre part au niveau opérationnel. La phase de conception est toujours en cours. La gestion opérationnelle des risques, nécessaire à la conduite de l'entreprise, a été développée itérativement dès l'indépendance de RUAG MRO et est systématiquement ajustée aux progrès conceptuels. Ce développement s'est fait en concertation et collaboration avec le conseil d'administration et le comité d'audit de RUAG MRO.

La politique de gestion des risques sera entérinée par le conseil d'administration dans la première moitié 2021. L'architecture des risques de RUAG MRO, la tolérance aux risques, les exigences en matière de reporting en font partie. Les organes de direction de RUAG MRO sont régulièrement informés des progrès du développement conceptuel ainsi que de la réalisation des objectifs et influencent la mise en œuvre en conséquence.

Nous sommes d'accord avec la nécessité d'indépendance des organes de gestion des risques et de la conformité et de leur accès direct au conseil d'administration. Les adaptations organisationnelles nécessaires seront effectives dès janvier 2021.

Recommandation 2 (Priorité 1)

Le CDF recommande à RUAG MRO :

- de s'assurer que les risques stratégiques et existentiels soient tous pris en compte, d'effectuer un cumul des risques et de tenir compte des effets de combinaison
- d'améliorer le processus d'identification afin d'assurer l'exhaustivité, l'uniformité, la qualité et la mise à jour régulière de l'inventaire des risques à tous les niveaux organisationnels
- d'améliorer le processus de reporting afin de permettre une vision d'ensemble des risques pour chaque niveau organisationnel
- de s'assurer qu'une interface entre les instances de gouvernance existants et la gestion des risques soit clairement définie
- de définir comment les risques répertoriés dans les anciens systèmes de gestion des projets existants peuvent être intégrés dans le nouveau système, en assurant une gestion uniformisée.

Prise de position de RUAG MRO

Les recommandations du CDF ont également été identifiées par RUAG MRO et sont traitées dans le cadre du développement conceptuel de la gestion des risques.

Sur la base du concept de gestion des risques et des directives opérationnelles de RUAG MRO, l'identification des risques, leur évaluation, la définition des mesures de mitigation ainsi que le reporting se font par l'intermédiaire d'un instrument informatisé. Cet instrument a été paramétré de manière à assurer la perméabilité des différents niveaux de l'entreprise et la consolidation aux échelons hiérarchiques désirés ainsi qu'à mettre en évidence les interactions et les combinaisons entre les risques recensés. Les résultats sont revus par le comité d'audit à chacune de ses séances et sont régulièrement présentés au conseil d'administration.

Les risques spécifiques aux projets seront également intégrés dans cet instrument de façon à disposer in fine d'un pilotage unifié et exhaustif à tous les échelons de RUAG MRO.

Recommandation 3 (Priorité 1)

Le CDF recommande à RUAG MRO d'approfondir sans délai l'examen de la structure du toit de la Halle 3 (structure secondaire) avec l'aide de spécialistes puis de procéder à une nouvelle analyse des risques et, le cas échéant, d'adapter les mesures hivernales ou prendre d'autres mesures immédiates. La nécessité de prendre des mesures immédiates est laissée à l'appréciation de RUAG MRO. De plus, l'analyse de la structure de soutien du bâtiment commandée (structure primaire) devra servir de base pour choisir les mesures à prendre (assainissement ou construction d'un nouveau toit, par exemple).

Prise de position de RUAG MRO

En tant que propriétaire des infrastructures, RUAG MRO a identifié la nécessité d'examens approfondis des structures primaire et secondaire. Ces examens ont été effectués en septembre et en octobre 2020. RUAG MRO dispose des rapports intermédiaires des experts. Les résultats définitifs seront connus fin janvier 2021. Sur cette base et le cas échéant, RUAG MRO actualisera son analyse des risques et déterminera les mesures adéquates pour l'assainissement ainsi que pour le renforcement de la halle 3.

Les mesures immédiates pour le soulagement de la structure du toit ont été mises en place fin novembre 2020. Sur la base des rapports intermédiaires susmentionnés, des directives concernant la sécurité opérationnelle et des personnes ont été émises mi-décembre 2020. Un concept d'urgence en cas de précipitations météorologiques particulières (mesures hivernales) est en place.

La conduite de l'armée et les forces aériennes ont été informées par écrit de la situation, des risques et des mesures prises à mi-décembre 2020. Simultanément, la SUVA a également été prévenue par écrit.

Les échanges avec les experts du CDF ont été appréciés et ont contribué à renforcer encore la sensibilité concernant la mitigation de ce risque précis.

Recommandation 4 (Priorité 2)

Le CDF recommande à RUAG MRO d'étendre et de formaliser ses contrôles (fondés par exemple sur des analyses de données, monitoring, testing) dans le domaine de la gestion de la conformité et celui de la gestion des risques.

Prise de position de RUAG MRO

RUAG MRO est consciente de la nécessité d'étendre et de formaliser les contrôles dans les domaines de la gestion des risques ainsi que de la conformité et met en place les mesures nécessaires. Ces mesures se basent sur les mécanismes de contrôle existants et seront systématisées et formalisées de façon uniforme au sein de l'entreprise.

4 RUAG International

RUAG International est composé des segments « Space » et « Aerostructures ». A côté de ce qui constitue le cœur de son activité, le groupe comprend actuellement des segments qui ont pour vocation à être désinvesties : Ammotec (fabrication de munitions) et MRO International (systèmes et composants pour l'aviation civile et militaire ainsi que systèmes de simulation et d'entraînement). La conception et la mise en œuvre des systèmes de gestion des risques et de la conformité étaient en cours au moment de l'audit.

Ce chapitre est basé sur l'analyse de documents et d'entretiens dans l'organisation centrale de RUAG International, ainsi que sur différentes études de cas :

- Segment « Space » aux Etats-Unis, environ 160 collaborateurs et 339 millions de francs de chiffre d'affaires en 2019
- Unité « Simulation & Training » aux Emirats arabes unis, rattachée à la division « MRO International », environ 20 collaborateurs et 2,7 millions de francs de chiffre d'affaires en 2019
- Projet Eiger (mise en conformité du site de production de munitions à Thoune).

4.1 Concept de gestion des risques globalement abouti, mais le « tone at the top » doit être amélioré

Des exigences détaillées pour la mise en place du système de gestion des risques font défaut

La mise en place de la gestion des risques est organisée sous forme de projet avec un plan d'action, un budget et des rapports réguliers sur l'avancement. Le conseil d'administration est indiqué comme « sponsor » et le CEO fait partie du groupe de pilotage. Pourtant, le conseil d'administration n'a pas défini initialement ses attentes concrètes. La conception se fait avant tout sur propositions des spécialistes du domaine. Elles sont discutées et validées régulièrement par la direction ou le conseil d'administration. Dans les discussions, leurs exigences ont été développées au fur et à mesure, mais un cadre général n'a pas été donné initialement. Des voix se sont aussi exprimées de façon critique sur l'utilité d'un système de gestion des risques, par exemple en mettant en doute la nécessité d'acheter une solution informatique. Après discussion au sein de la direction, la décision d'investir dans un logiciel a été maintenue. Les réflexions sur les différentes options envisagées pour l'organisation de la gestion des risques n'ont pas été documentées.

L'organisation vient d'être complétée en septembre 2020

La gestion des risques est rattachée au département « Legal, Compliance & Governance ». La responsabilité incombe au responsable « Compliance & Governance » qui est subordonné au responsable de ce département. Depuis août 2019, un Global Risk Manager a été recruté. Il est épaulé depuis septembre 2020 par un gestionnaire des risques. Le responsable « Compliance & Governance », qui gère également le domaine de la conformité, dispose d'un accès direct au conseil d'administration. Au total, 1,9 EPT sont dédiés à la gestion centrale des risques. Un outil informatique permettant une gestion centralisée de la gestion du risque (le même que RUAG MRO) est en cours de déploiement.

A côté de la mise en place du système, le gestionnaire des risques est mobilisé dans la gestion de la crise du COVID-19, les formations pour les collaborateurs et le programme « Leadership » associé ont dû être repoussés. Par ailleurs, en octobre 2020, RUAG International a annoncé la suppression de 150 postes dans les fonctions de support suite à cette crise.

L'une des initiatives les plus récentes prévoit de mettre en place deux nouvelles instances (Compliance & Risk Board et Compliance & Risk Network) afin d'assurer l'alignement des pratiques et de coordonner les actions dans les domaines de la gestion des risques et de celle de la conformité au niveau du groupe. Une dizaine de spécialistes thématiques (Trade Compliance, sécurité de l'information, etc.) ainsi que des représentants des unités opérationnelles (Risk Champion) feront partie de cette communauté. Il ne s'agit pas de fonctions à plein temps, elles sont intégrées à des postes existants. Au moment de l'audit, le Compliance & Risk Board et le Compliance & Risk Network n'étaient pas encore actifs.

Appréciation

Les exigences spécifiques pour le développement et la mise en place du système de gestion des risques, venant du conseil d'administration de RUAG International font défaut. Celui-ci porte pourtant la responsabilité dans ce domaine. Pour le CDF, relayer l'exigence, fixée dans les objectifs stratégiques du Conseil fédéral, de la mise en place d'un système répondant à la norme ISO 31000 n'est pas suffisant. Le conseil d'administration devrait spécifier concrètement ses attentes, par exemple en terme d'organisation, de périodicité des rapports ou de leur niveau de détail. Les personnes responsables de la gestion des risques devraient ensuite proposer différentes variantes à même de remplir ces exigences. Cela permettrait au conseil d'administration de s'assurer que la mise en place correspond à ce qu'il a voulu d'une part et d'autre part de mieux exercer ses fonctions de pilotage et de contrôle. Il permettrait en outre d'éviter qu'il n'intervienne après-coup, ce qui est inefficace. De plus, il soulignerait ainsi l'importance de ce domaine. Ce dernier point est d'autant plus crucial au vu de la transformation attendue du groupe, notamment la vente de certaines activités, et du fort impact de la crise du COVID-19 sur RUAG International. La gestion des risques ne doit pas être négligée dans cette situation.

L'environnement réglementaire développé cette dernière année concernant la gestion des risques est solide. Il s'appuie sur la norme ISO 31000 et correspond aux meilleures pratiques de l'industrie. Maintenant que cette base est posée et les ressources à disposition, il s'agit de procéder le plus rapidement possible à la mise en œuvre.

Le cumul d'une fonction opérationnelle et du rôle de Risk Champion comporte des risques qu'il faut prendre en compte. Des mesures doivent être prises pour éviter les conflits d'intérêts, par exemple en définissant des lignes directes de reporting et des objectifs clairs dans chacun des domaines. Des incitations afin de favoriser une gestion proactive et une identification précoce des risques pourraient aussi être envisagées.

Conditions cadres à définir et culture du risque à développer

Les procès-verbaux des séances du conseil d'administration et du comité d'audit montrent que la thématique des risques est régulièrement abordée. L'engagement des instances supérieures sur cette thématique est visible.

La capacité à supporter les risques ainsi que la tolérance dans ce domaine n'a pas été définie au niveau du groupe. Cet élément n'est pas prévu selon la feuille de route du projet. Actuellement, le choix de la cartographie des risques s'appuie sur celle utilisée dans l'administration fédérale avec une matrice où chaque axe compte six niveaux.

Une communication à l'ensemble des collaborateurs sur l'importance d'une gestion des risques efficace et sur la plus-value qu'elle peut amener fait défaut.

Appréciation

Si la sensibilité des instances dirigeantes à la thématique des risques est de plus en plus démontrée, les attentes et les limites devraient être fixées, de manière chiffrée. En quantifiant la capacité à supporter les risques ainsi que sa tolérance dans ce domaine, le conseil d'administration définirait un cadre pour la prise de décision.

Si le choix de s'appuyer d'abord sur la cartographie des risques utilisée par l'administration fédérale est compréhensible, il ne doit pas exclure une réflexion sur l'adéquation de cette cartographie avec les besoins spécifiques à RUAG International, notamment vu la taille de la société et de son appétence aux risques, une fois que cette dernière aura été définie.

Une communication à large échelle sur la thématique de la gestion des risques devrait être prévue. Il s'agit d'un élément important pour qu'à terme, la culture soit vécue dans l'ensemble du groupe. Par ailleurs, l'utilité dans les processus opérationnels et la plus-value du nouveau système pour les collaborateurs eux-mêmes doivent clairement être démontrées pour faciliter son adoption.

4.2 Concept de gestion de la conformité bien défini

La gestion de la conformité relève, tout comme la gestion des risques, de la responsabilité du responsable « Compliance & Governance » au sein de l'unité « Legal, Compliance & Governance ». Au total, 4,4 EPT sont dédiés à la gestion centrale de la conformité. Les activités de l'unité « Compliance & Governance » se focalisent sur la prévention, notamment par l'élaboration de directives et l'organisation de formation, d'actions concrètes définies dans les processus opérationnels, ainsi que sur les mitigations de violations de la conformité.

Une directive générale décrit les domaines qui relèvent de la conformité : éthique des affaires (intégrité, code de conduite, conflits d'intérêts), conformité des exportations (Trade Compliance), conformité commerciale (corruption, relation avec des tiers, concurrence) et protection des données. Chacun de ces thèmes dispose ensuite de sa propre directive. Les directives en place devaient encore faire l'objet d'adaptations à la nouvelle organisation. Un travail qui est prévu dans les mois à venir.

Appréciation

Les directives réglant l'organisation et les différents domaines de la conformité sont en vigueur. L'adaptation formelle devraient être faite dès que les plans organisationnels, y compris les désinvestissements, seront plus clairs.

Par ailleurs, de la même manière que la gestion des risques, le domaine de la conformité doit faire l'objet d'une attention et d'une adaptation – notamment en ce qui concerne les ressources – en fonction de l'évolution de la stratégie du groupe.

4.3 La mise en œuvre pratique de la gestion des risques

Les risques stratégiques manquent au rapport global

Un rapport global sur les risques est préparé deux fois par année par le Global Risk Manager. Il est ensuite présenté et discuté avec la direction et le conseil d'administration.

Un premier rapport global a été produit en novembre 2019, soit peu avant la dissociation. Il contenait les risques de chacune des unités (y compris celles qui allaient constituer

RUAG MRO quelques mois plus tard). En juin 2020, un second rapport concernant uniquement RUAG International a été établi. Les risques des fonctions de support ont été ajoutés. Par contre, les risques stratégiques ou existentiels pour le groupe n'y figurent pas. Leur ajout est souhaité par le conseil d'administration, mais la manière de les intégrer et de les évaluer n'a pas encore été définie. Selon les procès-verbaux, certains de ces risques sont discutés de manière *ad-hoc* dans le cadre du comité stratégique du conseil d'administration.

Les documents à disposition ne laissent pas transparaître la manière dont les risques sont consolidés en vue du rapport. Par ailleurs, la cumulation des risques *(worst case scenario)* n'est pas effectuée.

Appréciation

L'évolution des rapports globaux va dans la bonne direction, mais des éléments indispensables à la gestion du groupe – les risques stratégiques et existentiels – manquent encore. Dans la mesure où RUAG International se trouve en pleine transformation, les risques liés à cette situation devraient être évoqués.

Le processus de consolidation des risques doit être amélioré. Des réflexions doivent être menées à tous les niveaux organisationnels en se concentrant sur l'impact au niveau du groupe. Les tout nouveaux Compliance & Risk Board et Compliance & Risk Network devraient apporter une amélioration importante sur ce point. Une vision cumulée des risques et des réflexions sur les effets de combinaison, particulièrement importante au vu des activités très hétérogènes de RUAG International, devraient être ajoutées au processus d'établissement du rapport global.

Inventaire lacunaire et absence de vue d'ensemble dans les filiales

En septembre 2020, l'exhaustivité des risques enregistrés n'est pas encore assurée dans les filiales. Le tableau des risques pour le segment « Space » aux Etats-Unis, actualisé mensuellement, ne dispose pas encore des risques jugés moins importants (« medium » ou « low »), ni ceux liés à des projets ou spécifiquement à l'un des quatre sites américains de la filiale. De plus, les risques identifiés concernent les dimensions opérationnelles et financières, mais ne couvrent pas encore les aspects de conformité. Même si le risque lié à la Trade Compliance est élevé aux Etats-Unis, il ne figure dans aucun inventaire des risques pour le segment « Space ».

Des risques inventoriés ne soient pas parfois traités d'une manière holistique, c'est-à-dire en considérant toutes les dimensions ou les catégories de risques. Dans l'unité « Simulation & Training » aux Emirats arabes unis, concernant les obligations offsets, le risque n'est pas seulement l'amende liée au non-respect des délais fixés, mais aussi le risque de générer les crédits d'offset de façon irrégulière (marge de manœuvre dans le bouclement qui sert de base pour calculer ces crédits d'offset, par ex.) ou par des activités à haut risque qui ne seraient pas alignées sur la stratégie du groupe. Il n'existe pas, pour cette filiale, de processus régulier d'actualisation des risques, hors du processus semestriel lancé par le groupe.

Appréciation

L'intégralité et la qualité des risques figurant dans le tableau des risques doivent être améliorées. L'objectif serait de mieux comprendre et discuter l'exposition aux risques au sens large, front-to-back et à plusieurs niveaux organisationnels (y compris ceux des pays et des filiales). Globalement l'objectif ultime serait que, pour chaque niveau organisationnel, toutes les dimensions et catégories de risques définies soient couvertes. La directive de gestion des risques définie au niveau du groupe devrait prévoir une actualisation régulière des risques au niveau de chaque filiale et de chaque pays.

Les outils de gouvernance et le reporting ne suffisent pas encore

Les risques sont traités et discutés dans plusieurs structures de gouvernance, notamment par les TIER Boards des différents niveaux de l'organisation, les comités de direction aux Etats-Unis et aux Emirats arabes unis, ainsi que dans le cadre du Country Management Meeting aux Etats-Unis. Par contre, ces discussions se focalisent sur les aspects opérationnels. Le domaine du risque au sens large n'est ainsi pas couvert et traité de manière systématique et standardisée à tous les niveaux organisationnels. Il n'existe pas de reporting standardisé et documenté permettant d'avoir une vue d'ensemble sur les risques auxquels s'exposent chaque unité, chaque filiale ou chaque pays.

De même, dans les filiales, il n'existe pas toujours une personne responsable des risques au sens large (aux Emirats arabes unis notamment) ou celle-ci ne dispose pas d'une ligne de reporting dans l'organisation centrale. A titre d'exemple, les personnes responsables des risques aux Etats-Unis (Country Manager) dispose d'une ligne de reporting vers le Chief Operating Officer du segment « Space ». Un lien dans l'unité « Compliance & Governance » ou vers le responsable des risques au niveau du segment (Risk Champion) fait cependant défaut. Les personnes ayant des fonctions clés pour l'implémentation d'un système de gestion des risques auprès des filiales n'ont pas d'objectifs explicites.

Appréciation

Les outils de gouvernance (les comités et les protocoles correspondants) ne suffisent pas encore pour évaluer si la gestion des risques au sens large est discutée et « remontée » à la hiérarchie de manière appropriée.

Un reporting standardisé, permettant au responsable de la filiale et du pays d'avoir une vue d'ensemble sur les risques, devrait être défini et implémenté.

La deuxième ligne de défense devrait être renforcée dans les filiales. Dans l'idéal, les tâches et la responsabilité liées à la gestion des risques au sens large devraient être centralisées auprès d'une personne sur place, tout en assurant une ligne de reporting dans l'organisation centrale. De manière générale, cette assurance de reporting devrait s'appliquer pour toutes les fonctions décentralisées, qu'elles soient liées à la deuxième ligne de défense ou aux fonctions de support occupées sur place.

La gestion des risques dans les projets n'est pas toujours suffisamment formalisée

RUAG International ne dispose pas de prescriptions valables pour l'entier du groupe quant à la gestion des risques au sein des projets. Des unités, comme le segment Space aux Etats-Unis, disposent toutefois de leurs propres directives.

Dans le cadre du projet Eiger, dont le but est de rendre le site de production de munitions à Thoune conforme aux normes de sécurité en vigueur, la gestion des risques existe sans être complétement formalisée. Les mesures pour minimiser les risques liés au projet apparaissent par exemple dans la « task-list » du projet, parmi plusieurs autres tâches opérationnelles. Elles ne sont d'ailleurs pas attribuées à des personnes et les rapports sur le projet ne contiennent pas de vue d'ensemble complète des risques (la priorité est donnée aux nouveaux risques, sans indiquer ce qu'il est advenu des anciens). Ainsi, il est difficile pour une personne extérieure au projet de les identifier clairement ou de retracer leur évolution.

L'intégration des risques de projets dans l'outil central de gestion n'a pas encore été définie.

Appréciation

Des standards minimaux quant à la gestion des risques au sein d'un projet devraient être définis au niveau du groupe. De plus, le reporting des risques de projets dans la gestion des risques au niveau du groupe doit être définie.

4.4 La gestion de la conformité fonctionne, mais doit être améliorée dans les filiales

Une liste des cas problématiques en matière de conformité est tenue à jour par le responsable de la conformité. Elle inclut les décisions et les mesures prises pour chacune de ces situations qui est discutée au conseil d'administration. La conformité est un point fixe dans l'ordre du jour des séances du conseil d'administration.

Tout comme en matière de gestion des risques, les filiales ne disposent pas toujours d'une personne responsable de la conformité au sens large. Pour le segment Space aux Etats-Unis, seuls certains aspects de la conformité sont couverts (Trade Compliance, Legal, par exemple). Ainsi une ligne de reporting pour ces domaines envisagés de manière globale fait défaut.

L'unité « Simulation & Training » aux Emirats arabes unis se trouve dans une période transitoire sans directeur sur place. A Abu Dhabi, personne ne remplit de fonctions liées à la conformité ou à la gestion des risques. Celles-ci sont déléguées à l'organisation définie au siège.

RUAG International estime que le risque lié aux exportations (Trade Compliance) est important. Pourtant, le Trade Compliance Officer aux Etats-Unis n'établit pas de rapport régulier au Country Manager. Un projet d'acquisition d'un outil informatique pour ce domaine est en cours, en complément des applications et interfaces de transmission des autorités utilisées sur place. Aussi longtemps qu'il n'a pas été implémenté aux Etats-Unis, l'efficacité des activités liées à la Trade Compliance restent limitées.

Appréciation

Dans l'idéal, les tâches et la responsabilité liées à la gestion de la conformité au sens large devraient être centralisées auprès d'une personne dans chacune des filiales, tout en assurant une ligne de reporting dans l'organisation centrale.

Dans le cas de « Simulation & Training » aux Emirats arabes unis, l'absence d'une personne responsable des risques et de la conformité sur place est très problématique dans un pays où les risques de réputation sont élevés, malgré le volume financier relativement modeste de cette filiale (moins de 3 millions de chiffre d'affaires en 2019).

Le CDF salue le projet d'acquisition d'un logiciel dédié à la gestion de la Trade Compliance au sein du groupe, avec une application aux Etats-Unis, dans la mesure où celui-ci devrait permettre d'augmenter l'efficacité dans ce domaine.

4.5 Contrôles internes en lien avec la gestion des risques et de la conformité à étendre et à formaliser

Les activités de contrôles sont seulement indiquées au niveau des directives et des instructions de travail. Un registre central regroupant de manière standardisée les contrôles, leur description et leur fréquence fait encore défaut.

La deuxième ligne de défense réalise notamment des actions concrètes définies dans les processus opérationnels (par exemple dans le domaine Trade Compliance ou Third Party Management). Elle effectue peu de contrôles sur l'efficacité des processus opérationnels mis en place par la première ligne de défense, que ce soit de manière globale et standardisée (par exemple à l'aide d'analyse de données, monitoring, testing) ou orientées sur les risques auprès des filiales. Par le passé, des contrôles et des audits spécifiques (notamment dans le domaine Trade Compliance) ont été réalisés.

Les entités responsables de la gestion des risques et de la conformité n'effectuent pas non plus de contrôles de qualité standardisés et formalisés dans leur propre organisation. Cette supervision a surtout été réalisée de manière informelle (par exemple sur la base des échanges réguliers entre les différents niveaux hiérarchiques).

Appréciation

Le cadre de contrôle au niveau de la gestion des risques et de la conformité n'est pas suffisamment formalisé. Dans un système mature, RUAG International devrait disposer d'un contrôle interne au sens large qui ne se limite pas au domaine des finances et qui inclut la gestion des risques et de la conformité. Actuellement la deuxième ligne de défense n'est pas suffisamment en mesure de connaître, de comprendre et d'apprécier les risques dans ces domaines.

4.6 Recommandations

Appréciation générale

Le concept de gestion des risques de RUAG International est documenté et sa mise en œuvre a débuté. Les études de cas montrent que le concept n'a pas été étendu à toutes les filiales. Le CDF identifie un potentiel d'améliorations sur les points suivants.

Recommandation 5 (Priorité 1)

Le CDF recommande au conseil d'administration RUAG International :

- de formuler, en consultation avec BGRB Holding, ses exigences et ses attentes en matière de gestion des risques et ainsi établir une base pour la mise en place du système par les spécialistes du domaine
- de surveiller régulièrement la réalisation des objectifs et l'état de la mise en œuvre du système de gestion des risques
- de s'assurer que les personnes impliquées dans la gestion des risques disposent de l'indépendance nécessaire pour palier à tout conflit d'intérêts potentiel (par exemple une ligne de reporting fonctionnel ou des objectifs en lien avec la gestion de risque)
- de quantifier la capacité à supporter les risques ainsi que sa tolérance aux risques au niveau du groupe. Ces éléments devraient ensuite être déclinés pour les différentes unités. Les règles d'évaluation des risques et la cartographie devraient être adaptées sur cette base.

Prise de position de RUAG International

Der Verwaltungsrat hat seine konkreten Erwartungen wiederholt und deutlich kommuniziert. Das Risikomanagement Konzept und Programm wurden im Verwaltungsrat verabschiedet und werden in regelmässigen Updates zum Fortschritt in Audit Committee und

Verwaltungsrat detailliert erörtert. In diesen regelmässigen Status-Updates überwacht der Verwaltungsrat auch die Zielerreichung und konnte so gewährleisten, dass die ERM-Einführung in dem aufgrund der Covid-19-Krise sehr herausfordernden Jahr 2020 voll im ursprünglich aufgestellten Zeitplan ist.

Entsprechend den etablierten Compliance und Governance Standards ist die Unabhängigkeit von Funktionen des Risikomanagements sichergestellt.

Nach der ursprünglichen Planung werden auch Risikotragfähigkeit und Risikoappetit des Konzerns gemäss der strategischen Ausrichtung als bestimmende Faktoren für das ERM bestimmt.

Recommandation 6 (Priorité 1)

Le CDF recommande à RUAG International :

- de s'assurer que les risques stratégiques et existentiels soient pris en compte, d'effectuer un cumul des risques et de tenir compte des effets de combinaison
- d'améliorer le processus d'identification pour assurer l'exhaustivité, l'uniformité, la qualité et la mise à jour régulière de l'inventaire des risques à tous les niveaux organisationnels
- d'améliorer le processus de reporting afin de permettre une vision d'ensemble des risques pour chaque niveau organisationnel
- de s'assurer qu'une interface entre les instances de gouvernance existantes et la gestion des risques soit clairement définie
- de définir des standards minimaux pour la gestion des risques dans le cadre de projets et, par la même occasion, de formaliser la manière dont les risques de projets doivent être intégrés dans l'outil central
- de sensibiliser l'ensemble des collaborateurs à l'importance et la plus-value d'une gestion des risques.

Prise de position de RUAG International

Die strategischen und potenziell bestandsgefährdenden Risiken sind in dem Group Risk Report für das zweite Halbjahr 2020 bereits enthalten. Spiegelbildlich zu der Bestimmung von Risikotragfähigkeit und Risikoappetit werden die Einzelrisiken zu einer Gesamtrisikoposition des Konzerns aggregiert.

Die ERM-Prozesse werden laufend verbessert. Die Schnittstellen zwischen den einzelnen Governance-Funktionen sind durch deren Zusammenfassung in einen umfassenden Compliance & Governance-Bereich (Compliance, Risikomanagement, Health, Safety, Security & Environment und Informationssicherheit) bereits etabliert. Das neu eingeführte zentrale Risk Management IT-Tool wird seit 1. Dezember 2020 angewendet. Nach einer ersten Phase der operativen Etablierung dieses IT-Tools werden dessen Anwendung und die dazugehörigen Prozesse des Risikomanagements auch auf die Ebene der einzelnen Projekte ausgerollt.

Risikomanagement ist für RUAG International ein wichtiges Führungsinstrument und Anliegen. So hat der neue CEO bereits an seinem zweiten Arbeitstag an die gesamte Belegschaft entsprechend kommuniziert. Gemeinsame Kommunikationsinitiativen von Verwaltungsrat und Konzernleitung sind in Planung.

Recommandation 7 (Priorité 1)

Le CDF recommande à RUAG International de clarifier les responsabilités en matière de risques et de conformité dans toutes les entités décentralisées et d'assurer une ligne de reporting dans l'organisation centrale.

Prise de position de RUAG International

Über die bereits implementierten Abstimmungsgremien Compliance & Risk Network und Board wird die operative Verantwortung für Compliance und Risikomanagement durch die Zusatzfunktionen «Compliance & Risk Champions» in den Konzerneinheiten weiter vertikal integriert, mit entsprechenden Berichtslinien zur Gewährleistung der Unabhängigkeit.

Recommandation 8 (Priorité 2)

Le CDF recommande à RUAG International d'étendre et de formaliser ses contrôles (fondés par exemple sur des analyses de données, monitoring, testing) dans le domaine de la gestion de la conformité et celui de la gestion des risques.

Prise de position de RUAG International

Eine Initiative zur formalisierten Zusammenfassung der bereits bestehenden Kontrollen in ein zentrales Compliance & Risikomanagement-IKS-Register läuft bereits. Im Zuge dessen werden die bestehenden Kontrollen überprüft und erforderlichenfalls zusätzliche Kontrollen definiert und operativ implementiert.

5 BGRB Holding

La société de participation financière chapeaute les deux sous-groupes, RUAG MRO et RUAG International. Selon des arrêtés du Conseil fédéral de mars et de juin 2019, BGRB Holding est une pure société de participation financière. Elle n'exerce aucune activité opérationnelle, notamment afin d'éviter les conflits d'intérêts. Sa structure devrait garantir la réalisation des objectifs stratégiques du Conseil fédéral, l'indépendance opérationnelle des sous-groupes, la prévention de conflits d'intérêts et la responsabilité de l'entreprise.

Son conseil d'administration est composé de trois personnes indépendantes, désignées par le Conseil fédéral, auxquelles s'ajoutent le président du conseil d'administration de chacun des deux sous-groupes. En dehors d'un poste de secrétaire récemment créé, BGRB Holding ne dispose d'aucun personnel.

5.1 Des conflits d'intérêts à résoudre au plus vite

Selon les objectifs stratégiques du Conseil fédéral, le conseil d'administration de BGRB Holding est responsable de la concrétisation des objectifs stratégiques dans l'ensemble du groupe, de la gestion uniforme de RUAG MRO et de RUAG International ainsi que des sociétés du groupe. Ainsi le Conseil fédéral va plus loin que la Loi fédérale sur les entreprises d'armement de la Confédération (LEAC, RS 934.21), qui prescrit que le conseil d'administration de la société de participation doit « veiller » à la réalisation des objectifs stratégiques.

Le règlement d'organisation de BGRB Holding indique qu'elle n'est pas compétente, ni responsable de la stratégie, de l'organisation, des processus ou du financement décidés par chacun des deux sous-groupes dans le cadre des objectifs stratégiques. Elle dispose uniquement d'un droit de consultation lorsque les décisions des sous-groupes ont une incidence sur BGRB Holding ou ses activités.

En dehors de l'élection des membres des conseils d'administration des sous-groupes, les possibilités d'intervention de BGRB Holding sont inexistantes. Selon le conseil d'administration actuel, l'expérience montre qu'il est possible de signaler un écart par rapport aux objectifs stratégiques, mais que les canaux de communication établis ne permettent pas de trouver des solutions dans les délais opportuns.

Appréciation

La société de participation financière est cantonnée au rôle de spectatrice, car elle ne peut pas donner des directives aux deux sous-groupes. Cette position semble contredire l'objectif d'assurer une gestion uniforme des deux sous-groupes fixé par le Conseil fédéral.

La structure de BGRB Holding comporte des conflits d'intérêts inhérents non résolus. Les obligations personnelles de diligence des présidents des conseils d'administration des sous-groupes exigent que les intérêts de « leur » société soient défendus, même si cela est en conflit avec les intérêts de la société mère. Les présidents des conseils d'administration des sous-groupes sont confrontés, en raison de la structure en place, à des dilemmes qui ne peuvent être résolus.

Dans le cas où la société mère (BGRB Holding) ou le propriétaire (Confédération) viendrait à imposer des directives aux conseils d'administration des sous-groupes, cela pourrait engager la responsabilité de l'organe qui donne les instructions (art. 754 Code civil).

Le conseil d'administration mise sur l'instauration d'un climat de confiance et de dialogue pour parvenir à atteindre les objectifs stratégiques. Cette intention louable risque d'être mise à l'épreuve en situation de crise.

5.2 La question de la gestion des risques n'est pas résolue

Le règlement d'organisation de BGRB Holding prévoit qu'elle doit disposer des instruments nécessaires, comme une gestion des risques. Dans les faits, BGRB Holding ne dispose pas, à ce jour, de concept ou de documents dans ce domaine. Elle a en revanche mis en place un comité d'audit et de gestion des risques. Le conseil d'administration de BGRB Holding tente, par le biais de comparaison avec d'autres entreprises proches de la Confédération ou par des questionnaires envoyés aux sous-groupes, de trouver une direction pour le développement d'un système de gestion des risques. Il n'existe pas de lignes directrices sur la manière dont les objectifs stratégiques devraient être atteints.

Dans le troisième rapport trimestriel de 2020, que la société de participation remet au propriétaire, figurent les deux principaux risques que BGRB Holding identifie pour chacun des sous-groupes. Ces quatre éléments sont décrits de façon sommaire et ne sont pas évalués (impact financier ou probabilité d'occurrence) et les mesures de mitigation ne sont pas détaillées. Deux de ces quatre risques sont identiques à ceux figurant dans les résumés préparés par les sous-groupes pour le reporting trimestriel. La méthodologie qui a conduit à la mise en avant de ces risques ne fait pas l'objet d'un processus et n'est pas transparente. La société de participation n'évoque pas ses propres risques.

Appréciation

L'impact de BGRB Holding sur les sous-groupes en matière de gestion des risques n'est pas encore visible. L'objectif qui consiste à assurer la gestion uniforme des sous-groupes n'est pas atteint. Cette situation s'explique par les possibilités d'action extrêmement limitées de BGRB Holding relevées au chapitre précédent. Cette constellation n'est pas satisfaisante pour toutes les parties, tend à freiner la mise en place du système de gestion des risques et ne semble pas à la hauteur de l'évolution très dynamique des deux sous-groupes.

Sur la communication des risques au propriétaire, la BGRB Holding devrait soit se reposer uniquement sur la gestion des risques des sous-groupes, soit faire sa propre évaluation. Cette dernière devrait prévoir l'agrégation des risques des deux sous-groupes ainsi que l'ajout des risques propres à BGRB Holding. Il est essentiel que les risques principaux soient identifiés et évalués selon une méthodologie clairement définie afin d'assurer que le propriétaire dispose d'informations solides et d'une vue d'ensemble des risques sur l'entier du groupe. En ce qui concerne le troisième rapport trimestriel de 2020, ce n'est pas le cas. Le fait de communiquer, par manque de temps ou de moyens, des informations lacunaires risquerait de donner une fausse assurance au destinataire quant aux risques encourus par l'ensemble du groupe.

Annexe 1 : Bases légales

Textes législatifs
Loi fédérale sur les entreprises d'armement de la Confédération (LEAC), RS 934.21
Loi fédérale sur le matériel de guerre (LFMG), RS 514.51
Ordonnance sur le matériel de guerre (OMG), RS 514.511
Loi fédérale sur les prestations de sécurité privées fournies à l'étranger (LPSP), RS 935.41
Ordonnance sur les prestations de sécurité privées fournies à l'étranger (OPSP), RS 935.411
Loi fédérale sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques (LCB), RS 946.202.1
Ordonnance sur le contrôle des biens (OCB), RS 946.202.1

Annexe 2 : Abréviations

CDF	Contrôle fédéral des finances
EPT	Equivalent plein temps

Priorités des recommandations

Le Contrôle fédéral des finances priorise ses recommandations sur la base de risques définis (1 = élevés, 2 = moyens, 3 = faibles). Comme risques, on peut citer par exemple les cas de projets non-rentables, d'infractions contre la légalité ou la régularité, de responsabilité et de dommages de réputation. Les effets et la probabilité de survenance sont ainsi considérés. Cette appréciation se fonde sur les objets d'audit spécifiques (relatif) et non sur l'importance pour l'ensemble de l'administration fédérale (absolu).