Audit of information security
RUAG MRO Holding AG

Key facts

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

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

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

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

ICT split successfully completed, despite complexity and delays

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

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

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

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

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

RUAG AG's new security organisation is appropriately structured

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

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

Individual aspects of operational security need to be improved

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

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

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

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

Original text in German