Audit of the DTI key project: Data centres DDPS/Confederation 2020

Armed Forces Staff

Key facts

The data centre network approved by the Federal Council in July 2014 is intended to consolidate the heterogeneous data centre landscape of the Federal Administration into a network of four data centres. This will enable the number of data centres to be significantly reduced and the future capacity requirements of the federal IT system to be met in a more cost-effective and environmentally friendly manner. Within this framework, the Federal Department of Defence, Civil Protection and Sport (DDPS) planned the construction of three new data centres. Two of these facilities will be built with full military protection to ensure the functioning of applications and systems relevant to the Armed Forces under any circumstances. The third data centre will also be used by civilian federal offices. These projects are being implemented as part of the DTI key project "Data centres DDPS/Confederation 2020". The project also includes the development of the digitalisation platform of the Armed Forces, i.e. the ICT section of the data centres. The total costs for the project, including all expansion stages, amount to around CHF 900 million for real estate and CHF 320 million for ICT resources.

The audit results of the construction projects painted a rather positive picture. The project management is structured in a target-oriented manner and the deadlines and costs have been largely met. The building automation was implemented appropriately in the FUNDAMENT and CAMPUS facilities, and the management and monitoring are in line with common standards. The concepts for setting up the digitalisation platform describe a highly secure and scalable technology and are based on tried and tested technologies.

Encouraging progress in construction projects

The construction projects are well structured and the documentation is detailed and in good order. Despite partial delays, the projects have either been completed or are on schedule. The credit framework in the CAMPUS and FUNDAMENT projects was respected and cost management proved to be effective. However, the cost estimate for the KASTRO II project was still pending at the time of the audit. Due to the change of location and the fact that the plant is to be built from scratch, significant additional costs are to be expected.

Risk and quality management is established and effective. Nevertheless, particularly risky components should be subjected to more rigorous quality assurance in all future project phases.

According to an early assessment, the requirement from the specifications concerning the availability level of the FUNDAMENT data centre was not fulfilled in two areas. The required availability for the combustion air of the emergency power system was achieved by technical means and the exhaust gas routing was improved through structural measures. In the construction project for the KASTRO II data centre, such reviews are to be carried for all phases.

Action needed for the home automation systems

The security of the home automation systems was given high priority in the two newly built data centres. They were implemented in accordance with the high security requirements of the Confederation and the DDPS. The prescribed security documents are available, but they differ somewhat from the operating manuals and the service agreements. These inconsistencies must be resolved. The risk reduction measures described in the information security and data protection (ISDS) concepts have not yet been consistently implemented, so this must be scheduled and monitored.

Home automation applications generally need to be tested in an integration and test environment before being put into operation. Such an environment does not yet exist for these systems. There is an urgent need for action here, but this has been recognised by the DDPS.

Established standards and new technologies for the digitalisation platform of the Armed Forces

The "Architecture and Infrastructure (ICT A&I)" sub-project is creating the high-security platform for the digitalisation of the Armed Forces. The technology used and the planned communication methods are in line with current technology and security standards for high-security platforms. The operation and further development of the digitalisation platform represent a major challenge for the Cyber Command, which is currently being set up.

Capacity reserves to replace smaller data centres and system rooms

At the time of the audit, the new data centres were being used at 20% of their capacity. Reserves exist in the completed parts which can be used to install additional systems and infrastructures. The planned migrations are intended to achieve a usage rate of about 50% for the military and civilian data centres by approximately the end of 2024.

The Federal Office of Police (fedpol) operates special applications which have stringent requirements in terms of security and availability. The Federal Office for Buildings and Logistics, together with fedpol, planned the system room in centre G1 between 2008 and 2016, and it was completed in 2018. The DTI classified this as a data centre room and also granted a temporary exemption for the operation of the applications. In close cooperation with the IT Service Centre of the Federal Department of Justice and Police (ISC-FDJP), a solution has now been developed for the further exploitation of synergies. In the future, data centre G1 is to be operated for fedpol under the responsibility of the ISC-FDJP and thus become part of the data centre network, in order to be able to satisfy the existing requirements, as well as the new Schengen ones, for maximum availability through a dual-redundant regional concept.

The recommendations from previous audits have been implemented. The results are presented in the tables in Appendix 4.

Original text in German