AUDIT

Audit of the DTI key project data centres 2020 ICT architecture and infrastructure

Defence Group

KEY FACTS

Under the information and communication technology architecture and infrastructure (ICT A&I) project, the centralised technical services of the Armed Forces' new digitalisation platform (NDP) are to be set up and provided by the Cyber Command together with an external supplier. The aim is to have an operating platform that ensures the automatic operation of ICT in the data centre network on the basis of virtualised systems.

The Swiss Federal Audit Office (SFAO) had already audited the DDPS/federal data centres 2020 ICT A&I project – a key federal project – in 2023, when the focus was on project management and financing.[7]

The audit covered in this present report was aimed at examining whether the project provides the requisite centralised functions and services, and whether the distinction from the applications that run on the NDP is clearly defined. This is intended to ensure that the project managers for the specialist applications know which services they receive from the NDP, and which ones they must provide for themselves.

The audit revealed that the project is on track in terms of substance, and that the information is provided transparently. The architecture requirements are defined in integration guidelines for everyone involved, and these are also complied with. Moreover, the required services are documented and established.

The necessary functionalities and services have been set up and reporting is comprehensible

Changes to or additional requirements for the architecture or functionalities can be requested through various boards, where the change requests are processed, authorised and clearly documented. In addition, integration guidelines have been drawn up which define the requirements for applications that are to be run on the NDP.

The status report of 31 December 2023 clearly shows the project progress, and outstanding recommendations from audit report 23155 are being implemented. The project's financial situation was not reviewed as part of this latest audit.

Upcoming challenges are known

It is becoming clear that the platform's operation following product handover at the end of the project will require considerably more resources that originally expected. The Cyber Command is aware of this, and has drawn up corresponding staff plans and requested additional resources.

Transferring the budget process from the classical project method to one more suited to agile development is another challenge. The aim is to ensure that financial resources are available at the right time. The advantages of agile methods can thus be fully exploited. Here too, the Cyber Command is actively exploring solutions.

---

[7] "Audit of the DTI key project data centres 2020 ICT architecture and infrastructure" (audit mandate 23155), available on the SFAO website

Measures partly implemented

As part of this audit, the implementation of two recommendations from earlier reports was reviewed.[8] The first recommendation concerning an aggregated risk assessment, from the 2017 report, has been implemented. The second recommendation on outstanding issues from information security and data protection concepts (ISDS concepts), from the 2022 report, remains open because the ISDS concepts are still being reworked. However, they are close to completion and are due to undergo acceptance testing in the third quarter of 2024.

---

[8] "Audit of the CAMPUS computer centre" (audit mandate 17410) and "Audit of the DTI key project: Data centres DDPS/Confederation 2020 (audit mandate 21462), both available on the SFAO website