

# ICT governance audit

## General Secretariat of the Federal Department of Defence, Civil Protection and Sport

### Key facts

---

In its annual programme for 2020, the Swiss Federal Audit Office (SFAO) announced that it would audit the ICT governance of the Federal Department of Defence, Civil Protection and Sport (DDPS). The audit was subsequently scheduled for 2022, as various factors made it impossible to perform in the preceding years. In light of the findings from the audit preparation in summer 2022, the SFAO decided not to carry out a full audit for the following reasons: The heads of the department and the Defence Group (Group V) have recognised the need for action and the risks in relation to ICT governance, and have initiated corresponding measures. Moreover, the SFAO currently sees no urgent need for action. However, a conclusive evaluation is not yet possible, as the results of these efforts are still outstanding.

This report presents the findings from the audit preparation. The SFAO found that ICT governance had been overhauled at department level and was now ready to be implemented. Owing to numerous changes, particularly within Group V, an overhaul of the Group V ICT governance is now urgently needed and has already been requested.

#### **DDPS ICT governance: improvements needed in some areas**

DDPS ICT governance was overhauled in 2021/22, following strategic realignments at federal and department level. The newly established DDPS ICT and digitalisation governance was put into effect on 1 November 2022 by means of a new DDPS directive. A decision has not yet been made on the deadline for full implementation of ICT governance in the department and all offices. There is room for improvement in specific areas of DDPS ICT governance, for instance as regards alignment with existing DDPS regulations. In addition, further changes will be needed in light of forthcoming legislative amendments in 2023.

The General Secretariat of the DDPS (GS-DDPS) must regularly assess the need for changes to ICT governance as planned, and implement any necessary changes in a timely manner. Particular attention must be paid to changes in Group V, in order for the ICT governance of the department and Group V to consistently and seamlessly regulate ICT management. Against this background, the SFAO recommends that the GS-DDPS implement the process "setting up and maintaining the governance framework" as envisaged in the ICT governance.

#### **Group V ICT governance: urgently needed overhaul already requested**

On 1 September 2021, the Federal Council instructed Group V to set up the Cyber Command as a service provider for the mission-critical ICT services of the Armed Forces. It will replace the Armed Forces Command Support Organisation with effect from 1 January 2024. Until then, the new ordinance on Armed Forces IT should provide the necessary legislative frame-

work. Group V is currently clarifying the associated changes needed in ICT governance, ordinances and directives at all levels (federal, department, Group V). It will then draw up the ordinance on Armed Forces IT as part of a legislative project.

The Armed Forces management has fleshed out and added more detail to its strategy with the 2026 ICT target vision. The burden on Group V is to be reduced by relocating the ICT operations of ICT basic services from the Armed Forces Command Support Organisation to the Federal Office of Information Technology, Systems and Telecommunication (FOITT). Some mission-critical ICT services will also be temporarily relocated to the FOITT. ICT governance of all ICT services will now be performed centrally by the Armed Forces Staff, while the new service provider, Cyber Command, will focus on mission-critical ICT services.

These strategic decisions have far-reaching consequences in terms of organisation, processes and staff, and need to be reflected in a revised Group V ICT governance. An overhaul has already been requested.

**Original text in German**