Key points

The Federal IT Steering Unit (FITSU) ensures implementation of the information and communication technologies (ICT) strategy in the Federal Administration. For this purpose, it issues guidelines for the administrative units and manages the ICT standard services. Steering and managing the use of ICT in the Federal Administration was boosted in 2012. The FITSU now performs steering tasks. These changes influence supervision of the administrative units. This report concentrates on supervision in the sense of monitoring implementation of the directives and specifications in the departments. The Swiss Federal Audit Office (SFAO) checked whether or not the tasks, powers and responsibilities are defined and supervision is also carried out.

The FITSU does not see itself as an audit or supervisory body, but it nonetheless performs some supervisory tasks. Control cycles have been defined. In terms of content, they function in the federal ICT portfolio and in the standards if these involve product procurements or standard services. In the other areas, they have no or too little impact. There is room for improvement with regard to the basis for the enforcement and escalation instruments, proof of controls and supervision of the remedying of deficiencies.

Approaches to controls maintained

The SFAO believes the need for cross-departmental offices has been clearly identified. They guarantee a uniform approach in core areas of the Federal Administration. To this end, the authority to issue directives and supervisory and enforcement powers are an essential basis. However, it is not clear enough from the existing legal framework who is responsible for controls and supervision. The departments and service providers and procurers are responsible for the implementation of specifications in their task areas.

Regular reports must be made in various ways to the FITSU, and these are then submitted to the Federal Council. These self-declarations are only partially validated by the FITSU. The reliability of the information submitted to the Federal Council, e.g. on strategic controlling, is thus not fully guaranteed.

In its audits, the SFAO notes time and again that ICT security requirements are not adhered to in the field of ICT security. This is an indication that the control cycle is not effective. A stronger role for the FITSU in this area is essential.

Apart from escalation in its own department, the FITSU does not have any enforcement tools at its disposal.

Using a risk-based supervisory concept for systematic controls

The SFAO recommends clearly transferring the supervisory duty to the authority issuing the directives and amending the Federal Information Technology Ordinance accordingly. It should be subsequently determined by means of a risk-based supervisory concept which ICT areas are significant. The resulting monitoring requirement must ensure that an overview without duplication emerges. The FITSU should be able to intervene and escalate issues across offices and departments within the

scope of its cross-disciplinary tasks. The corresponding enforcement instruments must therefore be defined, and identified deficiencies and weaknesses must be systematically pursued and eliminated via the control cycle. Greater central supervision should be implemented in a manner that is as efficient and as automated as possible.

Original text in German