Audit of the IT application landscape
Federal Office of Transport

Key facts

The Federal Office of Transport (FOT) is the supervisory authority responsible for public transport in Switzerland. It supervises railways, cable cars, trolleybuses, trams, buses and ships. In this respect, the FOT regulates the allocation of approximately CHF 4 billion p.a. to the affiliated transport companies for investments for the preservation of value and compensation for operating expenses.

The Swiss Federal Audit Office (SFAO) carried out a preliminary analysis of the IT application landscape at the FOT and selected the "transport company directory" (TU-V) application for an in-depth audit. The SFAO examined the extent to which the TU-V is operated in a stable, secure, reliable and economical manner. In addition, it examined the information flow for financial postings from the TU-V to SAP accounting.

Geocloud AG is responsible for the maintenance of the TU-V application. It is operated by the Federal Office of Information Technology, Systems and Telecommunication.

Compliance with the Data Protection Act should be ensured as a high priority issue

Additional data fields were included in the TU-V in December 2015 as part of a program change. These included not only personal data such as surnames, first names, dates of birth and places of origin, but also particularly sensitive personal data such as information on criminal offences and criminal sanctions, as well as information on medical problems. As the application was not designed to protect this data, this led to non-compliance with the provisions of the Data Protection Act. The SFAO informed the FOT and the competent units of the department (particularly the Federal Data Protection and Information Commissioner) about the issue in a letter.

The FOT thereupon took immediate measures and submitted an action plan to the SFAO. Based on current knowledge, the SFAO considers this plan appropriate for achieving the necessary improvements. Since a formal process workflow for making changes to programs has not yet been defined, the FOT must define and implement a clear change process for change management. The approval of changes, their testing and release, and the functional separation of the units involved is to be regulated in this.

An access protection and role concept is to be created and implemented

Regarding the administration of user accounts within the TU-V, clear processes for administration and the assignment of rights must be defined and implemented. Likewise, the corresponding TU-V documentation, e.g. the protection requirements analysis, should be updated.

Original text in German