Audit of the IT security for access to GEVER
Federal Office of Meteorology and Climatology

Key facts

The Federal Office of Meteorology and Climatology (MeteoSwiss) is the national weather service. On behalf of the Confederation, MeteoSwiss provides weather and climate services for the benefit of the public, the authorities and civil and military aviation. As a result, the requirements for the availability and functionality of information and communication technologies (ICT) are very high, which is why MeteoSwiss is also supervised by the Federal Office of Civil Aviation. Due to the special technical and operational requirements, MeteoSwiss operates the ICT infrastructure itself with only a few exceptions and is therefore not directly integrated into the federal network. Instead, it is only connected in a controlled manner.

Following the introduction of the GEVER Ordinance, all federal units must process their business-relevant data in an electronic business management system. Since the migration in December 2020, MeteoSwiss may only process data with no enhanced security requirements in the GEVER system, because it is not directly integrated into the federal network. MeteoSwiss needs full access in order to be able to process data with increased protection requirements. A request for this was submitted to the Federal IT Steering Unit (FITSU)[1] last year. The FITSU imposed certain conditions in order to grant final approval. In order to check compliance with the conditions, the Swiss Federal Audit Office (SFAO) was asked to provide an independent assessment of IT security at MeteoSwiss. Overall, the audit findings were good.

IT security is of a high standard

Both the organisational and the technical maturity of IT security at MeteoSwiss are advanced. No significant deviations were found in the implementation of the federal requirements and international standards during the audit. The network and workplace security is at least equivalent to the level of the Federal Administration.

In order to counteract the risk of unconscious or erroneous tampering, MeteoSwiss should take a more targeted approach to raising the awareness of the employees concerned when using user accounts with privileged rights on workstations.

The SecureCenter encryption software is available at MeteoSwiss, but is not yet well established. Various other tools are used to protect confidential data. In the longer term, this creates a risk of no longer being able to read this information. MeteoSwiss must play an active role here by providing comprehensive information and training.

During the audit, the SFAO was unable to identify any additional risks that would jeopardise MeteoSwiss' full access to the GEVER system. The safeguards in the systems and the networks comply with the federal requirements and are effective. In the SFAO's view, the above recommendations have no negative impact on the federal GEVER system.

Original text in German

[1] Since 1 January 2021: Digital Transformation and ICT Steering unit of the Federal Chancellery