Audit of the security and availability of the GEVER system

Federal Chancellery and IT Service Centre of the Federal Department of Economic Affairs, Education and Research

Key facts

With the GENOVA programme, the Federal Chancellery (FCh) aims to introduce a single electronic business management product (GEVER) for all units of the Federal Administration. The programme is planned to run from November 2015 to September 2021 and is expected to cost more than CHF 68 million. The IT Service Centre of the Department of Economic Affairs, Education and Research (ISCeco) is primarily responsible for running the platform. By autumn 2020, more than 22,000 users were working with the new system.

In this audit, the Swiss Federal Audit Office (SFAO) assessed whether the measures implemented at the operational level are adequate from the point of view of security and availability. It also examined whether the transition from project status to operational status has been completed and whether outstanding issues are being followed up. Finally, this audit follows up on four recommendations from previous audits.

Overall, the SFAO reached a satisfactory conclusion, although the complex system architecture places high demands on operations and a significant amount of work remains to be done.

Security requirements are defined but process is not yet complete

The architecture of the solution is complex, with several players involved in its operation. Their prerogatives are clearly defined, they judge the collaboration to be satisfactory. Specialist positions are filled, operations can be regarded as stable, and the development of incidents is favourable. The management, planning and operational processes are defined within ISCeco. An internal audit of operations was conducted and more are planned. The SFAO considered the definitions of the organisation, management and processes of operations to be appropriate. The security requirements for the technical solution and operations are documented. Residual risks are recognised and accepted. However, the SFAO found that the implementation of basic protection is not fully documented.

As regards the service procurers, the SFAO did not examine the status of the security measures in detail. It did, however, find one case where the division of tasks between departments and offices was not clearly defined. The SFAO calls for further effort in terms of communication here.

Access and integrity protection: mechanisms are appropriate, some points need to be finalised

The GEVER platform is installed in the Federal Administration's private cloud at the Federal Office of Information Technology and Telecommunication (FOITT). It is used within the Confederation's secure IT network. Two-factor authentication is provided by the standard ICT

service eIAM[1]. Users are assigned their department's system and permissions limiting the operations and objects they can access. A limited number of administrators are defined, both at application and technical levels. The mechanisms in place are generally appropriate. However, the SFAO found that the annual checks on the lists of privileged users were not yet operational.

A Defence Group solution ensures the confidentiality of documents up to CONFIDENTIAL level. However, the user regulations prohibit the processing of documents at SECRET level and the system blocks the definition of a document in this classification category. The risk of entering sensitive data in the metadata remains and is recognised by the client.

The change management process in place at ISCeco adequately defines the steps to be followed (request, validation, execution, testing). However, changes are not systematically logged in all the system's components. The SFAO was therefore unable to check the effectiveness of the change management process. Tools regularly check the integrity of the servers. Hash[2] mechanisms are available in the platform, but not yet in use. The SFAO asked for clarification on this point.

Continuity management: approach is not fully developed

To meet the increased need for system availability, the infrastructure is designed with redundancy in separate computer centres. Tests have shown that the failovers work in case of failure. A monitoring system for the platform components is in place at ISCeco, alerts are issued and incident tickets are automatically generated in the event of a serious malfunction. These are then processed according to the procedures in force. The SFAO points out that some components are not under ISCeco's control. In such cases, ISCeco has to rely on other service providers to resolve incidents.

In terms of recovery management, the SFAO noted that some aspects had not yet been documented. Although various measures are defined and regular backups and recovery tests are carried out, there is no structured overview of this area (policy). Failure scenarios, up-to-date recovery plans and more extensive reconstruction tests also need to be prepared.

Transition to the permanent organisation is regulated

Various activities and bodies are defined to deal with the transition to operational status. Working groups at the steering, management and implementation levels meet regularly and involve the various players concerned. This facilitates the transfer of knowledge. Pending lists are managed at these levels. The SFAO considered these mechanisms to be adequate, although it expects some uncertainty in connection with the takeover of the FITSU's functions by the Federal Chancellery from January 2021.

The SFAO's previous recommendations have largely been implemented.

Original text in French

[1] Standard ICT service for identity and access management, managed by the FITSU.
[2] Cryptographic function used for verification purposes.