Audit of risk and pending item management
Federal Office of Information Technology, Systems and Telecommunication

Key facts

The Federal Office of Information Technology, Systems and Telecommunication (FOITT), the largest IT service provider of the Federal Administration, is currently undergoing a major transformation. It is aligning its processes and organisation with a more flexible and agile work organisation and adapting to the changed environment. The modernisation is being steered by the director with the Midar[1] transformation initiative. The transformation attaches particular importance to risk management.

The Swiss Federal Audit Office (SFAO) audited the FOITT's risk management (RM) and the management of risks and pending items arising from the transfer of tasks and changes in functions and roles due to the Midar transformation initiative. The audit showed that the FOITT actively manages the risks associated with the transformation. In addition, the FOITT RM is undergoing restructuring as a result of the transformation; the direction taken is purposeful and plausible.

Finally, the SFAO also examined the open recommendations from the earlier mandate "Audit of the digitalisation platform DIP"[2]. Currently, two of these recommendations have not yet been implemented.

Midar risk management is up and running

The existing FOITT risk management system handles operational risks. It has weaknesses in terms of both formal and active management. There is no consolidated and consistent monitoring of all FOITT risks; the separate Midar risk reporting is also addressed directly to the FOITT Executive Board. This gives a good impression of the transformation risks. The specially created Midar RM will be incorporated into the FOITT RM in the future.

Pending items that arise in the course of the Midar transformation initiative as a result of changes in tasks, roles and functions are actively managed on a person-by-person basis. The approach chosen is target-oriented and reasonable. The transformation has a direct impact on business continuity management and IT service continuity management; pending items that involve updates to these were identified. The SFAO expects these principles to be updated and tested for effectiveness.

FOITT's risk management organisation to be adapted

Risks are now to be recorded at various levels, managed and reported in condensed form to the FOITT Executive Board. The reporting frequency will also be adapted to the new agile world. The SFAO welcomes the path taken and recommends that the restructuring of the FOITT RM be terminated and the effectiveness of the newly established system be reviewed separately at a later date.

Original text in German

---

[1]   "Midar" means "change" in Romansch, one of Switzerland's national languages; see also Appendix 3, glossary
[2]   The audit report mandate 18532 is available on the SFAO website.