Audit of the CURIAplus project
Parliamentary Services

Key facts

Parliamentary Services support the Federal Assembly and its bodies in the fulfilment of their tasks. Among other services, they provide the IT systems and applications for the Federal Assembly and its own staff. The Administrative Delegation is responsible for the overall management of Parliamentary Services. In a motion adopted in 2018, Parliament instructed the Administrative Delegation to push ahead with the digitalisation of council and committee operations and to give Parliamentary Services the necessary mandates to do so. The two IT projects CURIAplus and Cervin are of central importance for this.

The Swiss Federal Audit Office (SFAO) audited the strategic IT project CURIAplus. As this is based on the work of the Cervin project, the SFAO also audited relevant topics in this project. The SFAO found that there are significant problems and risks in both projects, particularly with regard to information security. The SFAO concluded that the causes were mainly to be found in inadequate governance and compliance with directives, as well as the lack of architectural specifications. Due to the urgency of the matter, the SFAO informed representatives of the management of both Parliamentary Services and the Administrative Delegation of the key findings on 30 April 2021. In principle, Parliamentary Services regarded the findings as already known, but assessed them in a different manner to the SFAO.

No ICT strategy or ICT governance

There is no ICT strategy that is aligned with the business objectives or the digitalisation mandate. Likewise, there is no operational and sourcing strategy, nor target architecture, that takes all relevant requirements into account. In this vacuum, decisions were made by the projects – sometimes without a comprehensive clarification of the consequences – and facts were produced.

In May 2021, Parliamentary Services announced that external specialists had been commissioned to develop the basis for ICT governance, which the SFAO welcomes. Until the results of the work are available, it remains to be seen whether the direction taken by the projects will be compatible with the overarching requirements and whether any necessary corrections are even possible.

The definitive adoption of the ICT governance that has been under development since 2018 was postponed until the beginning of 2020. This was partly because dependencies on the still pending ICT strategy were identified. This postponement may have increased existing internal tensions and uncertainties regarding tasks, responsibilities, competences and processes in ICT projects and ICT operations.

Unclear security requirements and non-compliance with directives and guidelines

The new Information Security Act (ISA) assigns management tasks for information security to the Administrative Delegation and establishes an overarching management. Based on the previously applicable specifications, directives and guidelines, the individual ICT projects and Parliamentary Services bear responsibility for appropriate security requirements and

measures. In view of the increasing digitalisation and threat situation, the SFAO does not consider this regulation to be appropriate for the various levels and welcomes the top-level management responsibility which the ISA requires of the Administrative Delegation.

The CURIAplus and Cervin projects do not sufficiently comply with applicable guidelines and directives. Mandated security concepts stall at the initial stage and work results have not been produced and released as prescribed. Consequently, not all security requirements and measures have been included in the specifications, the invitation to tender or the contract for work.

Cervin: Undefined operations and support, no outsourcing concept

Cervin (Parlnet) has been used by members of parliament since the end of 2019, but important operational issues remain unresolved. The testing possibilities are insufficient, no acceptance has taken place and support is provided by the project organisation on a best efforts basis. Parliamentary Services transferred the operation of the platform to an external company without a corresponding contract or service level agreement. The deployment and test infrastructures and processes required by CURIAplus are only partially in place. Cross-project provider management and an operational and outsourcing concept are lacking.

Vulnerabilities in information security at Cervin with implications for CURIAplus

The implementation of security requirements was not systematically examined in this audit. According to externally conducted security audits, Cervin's security level is below average. Vulnerabilities were identified which, according to the audit report, must be remedied as quickly as possible, but this has not been done. Due to fundamental architectural and technical issues, it is unclear whether it is possible to eliminate the vulnerabilities in all cases. Furthermore, there are no prerequisites for detecting whether attackers have already exploited security vulnerabilities. Vulnerabilities in Cervin often have a direct or indirect knock-on effect on CURIAplus, which provides more sensitive data and functions for members of parliament.

Realisation of CURIAplus carries a high risk

The independent quality and risk management system required of the management following the abandonement of SOPRANO (another digitalisation project) has not been established, despite ready-made concepts. There is no independent assessment of the project and/or the project and risk reports. Risks reported by internal experts and those from external reports are not included in the project manager's risk reporting.

CURIAplus relies on the timely completion of other IT projects, some of which have already reported significant delays. After only a few months, the development of CURIAplus is already behind schedule and there are differences with the supplier as to whether the project can be completed by the defined deadline. After only a short time, this has led to discussions regarding the scope of the project and any possible contractual amendments.

In view of the project risks and the unclarified strategic guidelines, it must also be clarified whether it would be appropriate to suspend the CURIAplus project. Once the overarching requirements have been finalised, the current projects will have to be adapted to them in any case.

Original text in German