Audit of CuriaPlus security

Parliamentary Services

Key facts

Parliamentary Services (PS) 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 their own staff. The Administrative Delegation is responsible for the overall management of PS. 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 PS the necessary mandates to do so. The two IT projects CuriaPlus and Cervin (Parlnet) are of central importance for this.

Back in 2021, the Swiss Federal Audit Office (SFAO) audited the CuriaPlus application and Parlnet, and the underlying Liferay platform.[1] It identified various deficiencies during the course of the audit. Accordingly, the SFAO audited IT security again before CuriaPlus went into operation. It also examined the status of implementation of previous recommendations.

Despite positive developments in terms of governance and organisation, there is still room for improvement in both the CuriaPlus and Parlnet projects, particularly in terms of IT security, service level agreements (SLAs) and data backup.

The establishment of governance and the reorganisation of IT have provided the desired results

In October 2022, PS management put the Parliamentary Services' digitalisation strategy into effect. At the beginning of 2023, the Administrative Delegation put into force the directive on governance for digital services. In terms of IT, PS carried out a comprehensive reorganisation and restructured themselves according to the agile SAFe framework. In addition, the new digital services department received additional staff.

Future developments such as the new Information Security Act or the possible consequences of using cloud services were proactively addressed and presented to the Administrative Delegation.

Security documents need to be revised and accepted

PS are following the SAFe guidelines for project implementation. CuriaPlus is still being managed according to HERMES and will continue to be managed according to SAFe specifications after commissioning and formal completion. Accordingly, a protection needs analysis and an information security and data protection concept were also prepared. However, these documents have not been formally accepted.

The basic IT protection is intended to define the minimum organisational, HR and technical security requirements in terms of IT security. This applies to all IT resources in a binding manner, including the measures to be taken. Within PS, it is not clearly regulated which standards are to be used for basic protection and which measures are planned.

[1] "Audit of the CURIAplus project" (audit mandate 21310), available on the SFAO website.

The scope of the IT security tests should be expanded

A number of external security tests were carried out on Parlnet and the Liferay platform. It has not yet been possible to resolve all of the findings from these. In addition, a source code review was conducted, which did not identify any critical vulnerabilities. Furthermore, there was no extension of the scope of testing to other connected peripheral systems, as requested in the last SFAO audit. This is necessary, however, to obtain a holistic view of PS' IT security.

An external security audit of CuriaPlus in April 2023 could not be fully carried out due to new installations. PS have requested that the tests be repeated in August 2023, i.e. after the installations have gone live in July. According to the SFAO's recommendation, the tests should be extended to include the peripheral systems.

The SLAs and emergency concepts must be defined and coordinated with each other

In order to be able to react quickly in the event of a fault, the responsibilities of the various suppliers must be clarified and contractually defined in the SLAs. Emergency concepts are still missing for both CuriaPlus and Parlnet. In addition, the emergency measures must be tested regularly to ensure they are feasible.

Outsourced backups must be created and geo-redundancy must be tested

Since PS are classified as critical infrastructure, they should consider geo-redundancy with two physically separated data centres. At the very least, PS should keep offsite backups on a remote server or on external media away from their own data centre location.

Three recommendations from the 2021 audit have been partially implemented

PS arranged a further security audit and a code review. However, the scope of the security audit was not expanded as recommended.

The required documents, contracts and risk analysis exist but are still being worked on. Therefore, the recommendations have been only partially implemented.

Original text in German