EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung des Projektes CURIAplus

Parlamentsdienste

EFK-21310 | inkl. Stellungnahmen | 14. Dezember 2021 | FinDel D1/2022

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	101.21310
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Prüfung des Projektes CURIAplus
Parlamentsdienste

Das Wesentliche in Kürze

Die Parlamentsdienste unterstützen die Bundesversammlung und ihre Organe bei der Erfüllung ihrer Aufgaben. Neben anderen Dienstleistungen stellen sie die Informatiksysteme und -anwendungen für die Bundesversammlung und die eigenen Mitarbeitenden bereit. Der Verwaltungsdelegation obliegt die oberste Leitung der Parlamentsdienste. Mit einer 2018 angenommenen Motion beauftragte das Parlament die Verwaltungsdelegation, die Digitalisierung des Rats- und Kommissionsbetriebs voranzutreiben und den Parlamentsdiensten die dafür notwendigen Aufträge zu erteilen. Die beiden IT-Projekte CURIAplus und Cervin sind dafür von zentraler Bedeutung.

Die Eidgenössische Finanzkontrolle (EFK) prüfte das strategische IT-Projekt CURIAplus. Weil dieses auf den Arbeiten des Projektes Cervin basiert, hat die EFK relevante Themen in diesem Vorhaben ebenfalls geprüft. Die EFK stellt fest, dass in beiden Projekten wesentliche Probleme und Risiken bestehen, insbesondere im Hinblick auf die Informationssicherheit. Die EFK kommt zum Schluss, dass die Ursachen mehrheitlich bei der ungenügenden Governance und Einhaltung von Weisungen sowie den fehlenden Architekturvorgaben zu finden sind. Aufgrund der Dringlichkeit hat die EFK am 30. April 2021 Vertreter der Geschäftsleitung der Parlamentsdienste und der Verwaltungsdelegation über die wesentlichen Erkenntnisse informiert. Die Parlamentsdienste haben die Feststellungen grundsätzlich als bereits bekannt eingestuft, diese aber anders beurteilt als die EFK.

Fehlende IKT-Strategie und IKT-Governance

Eine auf die Geschäftsziele oder auf den Digitalisierungsauftrag abgestimmte IKT-Strategie ist nicht vorhanden. Ebenso eine Betriebs- und Sourcing-Strategie und eine Ziel-Architektur, die alle relevanten Anforderungen berücksichtigen. In diesem Vakuum wurde von den Projekten – teilweise ohne umfassende Abklärung der Konsequenzen – Entscheide getroffen und Fakten geschaffen.

Im Mai 2021 haben die Parlamentsdienste das Engagement externer Spezialisten zur Erarbeitung der Grundlagen für eine IKT-Steuerung bekannt gegeben, was die EFK begrüsst. Bis zum Vorliegen der Arbeitsergebnisse bleibt offen, ob die von den Projekten eingeschlagene Richtung mit den übergeordneten Vorgaben kompatibel sein wird und ob Korrekturen bei Bedarf überhaupt möglich sind.

Die definitive Verabschiedung der seit 2018 erarbeiteten IKT-Governance wurde Anfang 2020 aufgeschoben. Dies unter anderem, weil Abhängigkeiten von der noch fehlenden IKT-Strategie erkannt wurden. Dieser Aufschub verstärkt unter Umständen bestehende interne Spannungen und Unsicherheiten betreffend Aufgaben, Verantwortlichkeiten, Kompetenzen sowie Prozessen bei IKT-Projekten und dem IKT-Betrieb.

Unklare Sicherheitsanforderungen und Nichteinhaltung von Weisungen und Richtlinien

Mit dem neuen Informationssicherheitsgesetz (ISG) werden der Verwaltungsdelegation Führungsaufgaben zur Informationssicherheit zugewiesen und eine übergeordnete Führung etabliert. Aufgrund der bisher geltenden Vorgaben, Weisungen und Richtlinien tragen die

einzelnen IKT-Projekte und die Parlamentsdienste die Verantwortung für angemessene Sicherheitsanforderungen und -massnahmen. Die EFK beurteilt diese Regelung angesichts der zunehmenden Digitalisierung und Bedrohungslage als nicht stufengerecht und begrüsst die vom ISG verlangte oberste Führungsverantwortung durch die Verwaltungsdelegation.

Die Projekte CURIAplus und Cervin halten geltende Richtlinien und Weisungen nicht ausreichend ein. Vorgeschriebene Sicherheitskonzepte bleiben im Anfangsstadium stecken. Arbeitsergebnisse wurden nicht wie vorgeschrieben erstellt und freigegeben. Somit sind nicht alle Sicherheitsanforderungen und -massnahmen in das Pflichtenheft, die Ausschreibung und den Werkvertrag aufgenommen worden.

Cervin: Undefinierter Betrieb, Support und fehlendes Outsourcingkonzept

Cervin (Parlnet) wird seit Ende 2019 von den Parlamentariern genutzt, wichtige Betriebsfragen bleiben aber weiterhin ungeklärt. Die Testmöglichkeiten sind ungenügend, es fand keine Abnahme statt und der Support wird von der Projektorganisation nach best effort wahrgenommen. Den Betrieb der Plattform haben die Parlamentsdienste ohne entsprechenden Vertrag und Service Level Agreement an eine externe Firma übertragen. Die von CURIAplus benötigten Deployment- und Test-Infrastrukturen sowie -Prozesse sind erst bruchstückhaft vorhanden. Ein projektübergreifendes Providermanagement und ein Betriebs- und Outsourcingkonzept fehlen.

Lücken in der Informationssicherheit bei Cervin mit Auswirkungen auf CURIAplus

Die Umsetzung von Sicherheitsanforderungen wurde in dieser Prüfung nicht systematisch geprüft. Das Sicherheitsniveau von Cervin ist gemäss extern durchgeführten Sicherheitsaudits unterdurchschnittlich. Es wurden Schwachstellen identifiziert, die gemäss Auditbericht schnellstmöglich behoben werden müssen, was nicht erfolgt ist. Aufgrund architektonischer bzw. technischer Grundsatzfragen ist unklar, ob die Behebung der Schwachstellen in allen Fällen möglich ist. Ausserdem fehlen Voraussetzungen, um zu erkennen, ob Angreifer bereits Sicherheitslücken ausgenutzt haben. Schwachstellen in Cervin wirken sich vielfach direkt oder indirekt auch auf CURIAplus aus, das mehr sensible Daten und Funktionen für die Parlamentarier zur Verfügung stellt.

Hohes Realisierungsrisiko für CURIAplus

Das von der Geschäftsleitung nach dem Projektabbruch von SOPRANO (einem weiteren Digitalisierungsprojekt) geforderte unabhängige Qualitäts- und Risikomanagement ist trotz fertiger Konzepte nicht etabliert. Eine unabhängige Beurteilung des Projektes bzw. der Projekt- und Risikoberichte fehlt. Im Risiko-Reporting des Projektleiters werden von internen Fachleuten gemeldete Risiken und solche aus externen Berichten nicht aufgenommen.

CURIAplus ist auf die rechtzeitige Fertigstellung von anderen IT-Projekten angewiesen, von denen einige bereits wesentliche Verzögerungen gemeldet haben. Die Entwicklung von CURIAplus ist nach einigen Monaten bereits im Rückstand und es bestehen Differenzen mit dem Lieferanten, ob das Projekt zum definierten Endtermin abgeschlossen werden kann. Dies führt bereits nach kurzer Zeit zu Diskussionen bezüglich Projektumfang und allfälligen Vertragsnachträgen.

Angesichts der Projektrisiken und der ungeklärten strategischen Vorgaben ist ausserdem zu klären, ob eine Sistierung des Projektes CURIAplus angebracht wäre. Nach Fertigstellung der übergeordneten Vorgaben müssen die laufenden Projekte jedenfalls an diese angepasst werden.

Audit du projet CURIAplus
Services du Parlement

L'essentiel en bref

Les Services du Parlement assistent l'Assemblée fédérale et ses organes dans l'accomplissement de leurs tâches. Parmi d'autres services, ils fournissent les systèmes et les applications informatiques pour l'Assemblée fédérale et leur propre personnel. La Délégation administrative assume la direction suprême des Services du Parlement. Dans une motion adoptée en 2018, le Parlement l'a chargée de poursuivre la numérisation des activités des conseils et des commissions et de donner les mandats nécessaires aux Services du Parlement. Les deux projets informatiques CURIAplus et Cervin jouent un rôle essentiel dans ce contexte.

Le Contrôle fédéral des finances (CDF) a audité le projet stratégique CURIAplus. Comme ce dernier repose sur les travaux du projet Cervin, le CDF a aussi examiné les aspects pertinents de ce projet. Il a constaté dans les deux cas des problèmes et des risques majeurs, en particulier sur le plan de la sécurité de l'information. Le CDF conclut que les causes sont en grande partie dues à un manque de gouvernance et de respect des instructions ainsi qu'à l'absence de directives en matière d'architecture. Vu l'urgence de la situation, le CDF a présenté le 30 avril 2021 ses principales conclusions à des représentants de la direction des Services du Parlement et à la Délégation administrative. Les Services du Parlement ont considéré que les constations étaient en principe connues, mais ont porté une appréciation différente de celle du CDF.

Absence de stratégie et de gouvernance informatiques

Il n'existe pas de stratégie informatique adaptée aux objectifs fixés ou au mandat de numérisation. Il n'y a pas non plus de stratégie opérationnelle ou d'approvisionnement, ni d'architecture cible prenant en compte toutes les exigences pertinentes. C'est dans ce vide que les responsables de projets ont pris des décisions et créé des précédents – en partie sans en analyser les conséquences de manière approfondie.

En mai 2021, les Services du Parlement ont annoncé l'engagement de spécialistes externes chargés d'élaborer les bases d'un pilotage informatique, mesure saluée par le CDF. Dans l'attente des résultats des travaux, il reste à déterminer si la direction prise par les projets sera compatible avec les directives supérieures et si des corrections seront possibles, le cas échéant.

L'adoption définitive de la gouvernance informatique élaborée depuis 2018 a été reportée début 2020. Ceci, entre autres, parce que des dépendances de la stratégie informatique encore manquante ont été identifiées. Ce report peut accroître les tensions et incertitudes internes concernant les tâches, les responsabilités, les compétences ainsi que les processus liés aux projets et à l'exploitation informatiques.

Exigences de sécurité peu claires et non-respect des instructions et directives

La nouvelle Loi sur la sécurité de l'information (LSI) confie à la Délégation administrative des tâches dirigeantes en matière de sécurité de l'information et établit une direction supérieure. Selon les exigences, instructions et directives en vigueur jusqu'à présent, chaque projet informatique et les Services du Parlement sont responsables de la mise en place des exigences et

des mesures de sécurité appropriées. Le CDF estime que cette réglementation n'est pas adaptée aux niveaux de compétence concernés face à la numérisation et aux menaces croissantes et salue la responsabilité suprême de la Délégation administrative exigée par la LSI.

Les projets CURIAplus et Cervin ne respectent pas suffisamment les directives et instructions en vigueur. Les plans de sécurité exigés en sont restés à un stade embryonnaire. En outre, les résultats des travaux n'ont pas été établis et validés comme prévu. Par conséquent, toutes les exigences et mesures de sécurité ne figuraient pas dans le cahier des charges, dans l'appel d'offres et dans le contrat de services.

Cervin: mode d'exploitation et assistance non réglés et absence de plan d'externalisation

Les parlementaires utilisent Cervin (Parlnet) depuis fin 2019, mais d'importantes questions d'exploitation restent sans réponse. Les possibilités de test sont insuffisantes, il n'y a pas eu de réception des travaux, et l'assistance est assurée par l'organisation de projet selon le principe du « best effort ». Les Services du Parlement ont confié l'exploitation de la plateforme à une entreprise externe sans contrat correspondant ni accord de niveau de service. Les infrastructures et les processus de déploiement et de test nécessaires à CURIAplus ne sont que partiellement en place. Enfin, il manque une gestion des fournisseurs pour l'ensemble du projet ainsi que des concepts d'exploitation et d'externalisation.

Lacunes de Cervin en matière de sécurité de l'information avec des conséquences pour CURIAplus

La mise en œuvre des exigences de sécurité n'a pas fait l'objet d'un examen systématique dans le présent audit. Le niveau de sécurité de Cervin est inférieur à la moyenne, selon les audits de sécurité externes qui ont été réalisés. Des failles ont été identifiées et, selon le rapport d'audit, doivent être supprimées au plus vite, ce qui n'a pas été fait. Pour des raisons d'architecture ou techniques, il n'est pas certain qu'il soit possible de supprimer ces failles dans tous les cas. En outre, il est impossible de savoir si des cybercriminels ont déjà exploité les failles de sécurité. Les failles de Cervin ont aussi de multiples répercussions directes ou indirectes sur CURIAplus, qui fournit aux membres du Parlement davantage de données ou de fonctions sensibles.

Risques élevés liés à la réalisation de CURIAplus

La gestion indépendante de la qualité et des risques exigée par la direction après l'arrêt de SOPRANO (un autre projet de numérisation) n'est pas établie malgré les concepts prêts à l'emploi. Il manque une évaluation indépendante du projet ou des rapports sur le projet et les risques. Les rapports sur les risques du chef de projet ne mentionnent ni les risques signalés par les spécialistes internes, ni ceux qui ont été constatés par des rapporteurs externes.

CURIAplus est tributaire de l'achèvement dans les délais d'autres projets informatiques, dont certains accusent déjà des retards importants. Après quelques mois, le développement de CURIAplus a déjà pris du retard, et il existe des divergences avec le fournisseur quant à la possibilité d'achever le projet à la date prévue. Après peu de temps déjà, cela donne lieu à des discussions sur l'ampleur du projet et d'éventuels avenants.

Compte tenu des risques inhérents au projet et du manque de clarté des objectifs stratégiques, il convient de déterminer si une suspension du projet CURIAplus serait souhaitable. Une fois les objectifs généraux atteints, les projets en cours devront être adaptés à ces derniers.

Texte original en allemand

Verifica del progetto CURIAplus
Servizi del Parlamento

L'essenziale in breve

I Servizi del Parlamento coadiuvano l'Assemblea federale nell'adempimento dei suoi compiti. Oltre a fornire altri servizi, essi predispongono le applicazioni e i sistemi d'informazione per l'Assemblea federale e per i propri collaboratori. La Delegazione amministrativa è incaricata della direzione suprema dei Servizi del Parlamento. In una mozione accolta nel 2018, il Parlamento ha incaricato la Delegazione amministrativa di accelerare il processo di digitalizzazione delle attività delle Camere e delle Commissioni e di conferire ai Servizi del Parlamento i mandati necessari a tal fine. In questo ambito, i due progetti informatici CURIAplus e Cervin sono di centrale importanza.

Il Controllo federale delle finanze (CDF) ha verificato il progetto informatico strategico CURIAplus. Poiché CURIAplus si basa sui lavori del progetto Cervin, il CDF ha verificato anche i temi rilevanti di quest'ultimo. Ha inoltre constatato che entrambi i progetti presentano problemi e rischi considerevoli, specialmente in relazione alla sicurezza delle informazioni. Ha quindi concluso che le cause sono riconducibili perlopiù a una governance e a un'osservanza delle istruzioni insufficienti nonché alla carenza di direttive in materia di architettura informatica. Data l'urgenza, il 30 aprile 2021 il CDF ha informato i rappresentanti della Direzione dei Servizi del Parlamento e della rispettiva Delegazione amministrativa sui risultati più significativi della verifica. In linea di massima, i Servizi del Parlamento hanno classificato i risultati come già noti, ma li hanno valutati diversamente rispetto al CDF.

Mancano una strategia e una governance delle TIC

Manca una strategia TIC commisurata agli obiettivi aziendali o al mandato di digitalizzazione. Non esiste nemmeno una strategia operativa e di sourcing, né un'architettura target che consideri tutti i requisiti rilevanti. In questa situazione incerta, sulla base dei progetti sono state prese decisioni fattuali, in parte senza valutare in modo esaustivo le conseguenze.

Nel maggio del 2021 i Servizi del Parlamento hanno comunicato di aver incaricato specialisti esterni per l'elaborazione delle basi per la gestione delle TIC, una decisione che il CDF accoglie con favore. Finché non si sapranno i risultati dei lavori rimane da accertare se l'avanzamento dei progetti sarà compatibile con le direttive sovraordinate e se, all'occorrenza, sarà possibile apportare correzioni.

L'adozione definitiva della governance TIC, in corso di elaborazione dal 2018, è stata rinviata all'inizio del 2020. Questo rinvio è in parte dovuto al fatto che sono state riconosciute le interdipendenze dalla strategia TIC, tuttora mancante. In alcune circostanze questo ritardo aumenta le tensioni interne esistenti e le incertezze relative ai compiti, alle responsabilità, alle competenze e ai processi nel quadro dei progetti e dell'esercizio delle TIC.

Requisiti di sicurezza poco chiari, istruzioni e direttive non rispettate

Con la nuova legge sulla sicurezza delle informazioni (LSIn), alla Delegazione amministrativa vengono affidati compiti dirigenziali in materia di sicurezza delle informazioni e viene designata una direzione sovraordinata. Sulla base delle direttive e delle istruzioni previgenti, i

singoli progetti TIC e i Servizi del Parlamento sono responsabili dei requisiti e delle misure di sicurezza appropriati. In considerazione della digitalizzazione sempre più pervasiva e della situazione di minaccia, il CDF ritiene che questa regolamentazione non sia disciplinata al livello opportuno. Si compiace pertanto che la responsabilità dirigenziale suprema debba essere assunta dalla Delegazione amministrativa, come sancito nella LSIn.

I progetti CURIAplus e Cervin non rispettano in modo sufficiente le direttive e le istruzioni vigenti. I piani di sicurezza prescritti rimangono bloccati nella fase iniziale. I risultati dei lavori non sono stati prodotti e convalidati come prescritto. Di conseguenza, non tutti i requisiti e le misure di sicurezza sono stati inseriti nel capitolato d'oneri, nel bando e nel contratto di appalto.

Cervin: esercizio e supporto non definiti, piano di esternalizzazione mancante

I parlamentari utilizzano la piattaforma Cervin (Parlnet) dalla fine del 2019. Restano però irrisolte importanti questioni inerenti all'esercizio. Le possibilità di test sono insufficienti, non è stato eseguito alcun collaudo e il supporto viene fornito dall'organizzazione del progetto secondo il principio del «best effort». I Servizi del Parlamento hanno trasferito la gestione della piattaforma a una ditta esterna senza stipulare con questa un pertinente contratto e un service level agreement. Le infrastrutture per la distribuzione e il testing nonché i relativi processi necessari per il progetto CURIAplus sono disponibili soltanto in parte. Mancano una gestione trasversale dei fornitori e un piano relativo all'esercizio e all'esternalizzazione.

Le lacune nella sicurezza delle informazioni in Cervin si ripercuotono su CURIAplus

L'attuazione dei requisiti di sicurezza non è stata oggetto di una verifica sistematica in questa sede. Gli audit in materia di sicurezza svolti da specialisti esterni hanno evidenziato che il livello di sicurezza della piattaforma è inferiore alla media. Sono state individuate delle vulnerabilità che, secondo il rapporto di audit, devono essere affrontate il più rapidamente possibile. Ciò non è avvenuto. A causa di problematiche di fondo di carattere architettonico e tecnico, non è dato sapere se l'eliminazione delle vulnerabilità sarà possibile in tutti i casi. Inoltre, non vi sono le condizioni per individuare se gli aggressori hanno già sfruttato le falle di sicurezza. Le vulnerabilità rilevate sulla piattaforma Cervin si ripercuotono direttamente o indirettamente su CURIAplus, che mette a disposizione dei parlamentari un numero maggiore di dati sensibili e di funzioni.

CURIAplus: realizzazione a rischio

La gestione indipendente della qualità e dei rischi chiesta dalla Direzione dopo l'interruzione del progetto SOPRANO (un altro progetto di digitalizzazione) non è consolidata, benché i piani siano stati portati a termine. Manca una valutazione indipendente del progetto. Lo stesso vale per i rapporti sui rischi e per i rapporti di progetto. Il rapporto sui rischi del capoprogetto non include i rischi segnalati dagli esperti interni e quelli contenuti nei rapporti esterni.

Il progetto CURIAplus dipende dal completamento entro i termini di altri progetti informatici, alcuni dei quali hanno già subito importanti ritardi. Dopo alcuni mesi, il progetto CURIAplus non avanza come previsto. Oltre al ritardo già accumulato vi sono divergenze con il fornitore sul rispetto del termine ultimo prefissato per la conclusione del progetto. Nel giro di poco tempo questa situazione è stata fonte di discussioni sulla portata del progetto e su eventuali aggiunte del contratto.

In considerazione dei rischi legati al progetto e delle direttive strategiche non ancora chiarite, è necessario inoltre appurare se non sia opportuno sospendere il progetto CURIAplus. Dopo il completamento delle direttive sovraordinate, i progetti in corso dovranno essere in ogni caso adeguati a tali direttive.

Testo originale in tedesco

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

Generelle Stellungnahme der Parlamentsdienste

Die Parlamentsdienste begrüssen die vertiefte Prüfung des Projekts CURIAplus durch die EFK. Seit der Verabschiedung der Motion Frehner durch die beiden Räte im Jahr 2018 werden die Arbeiten zur Digitalisierung des Parlamentes zügig vorangetrieben. Mit der definitiven Verabschiedung der Roadmap Digitalisierung im Parlament hat die Verwaltungsdelegation am 13. November 2020 die wesentlichen Etappenziele der nächsten Jahre definiert. Einen wichtigen Beitrag dazu leistet die Ablösung der bestehenden Geschäftsdatenbank CURIA durch eine prozessgesteuerte, laufend weiterentwickelbare Anwendung, die den Ratsmitgliedern einen zeitgemässen Nutzerkomfort bietet und ihnen die individuelle Konfiguration ihrer Benutzeroberfläche erlaubt. Es ist wichtig, dass das entsprechende Projekt CURIAPlus professionell geführt und engmaschig kontrolliert wird.

Im Laufe der Digitalisierungsarbeiten seit 2018 hat sich gezeigt, dass die Parlamentsdienste von ihrer früheren, primär sektoriellen Betrachtung der Informatikanwendungen weg zu einem ganzheitlichen und datenzentrierten Ansatz kommen müssen. Dies bedingt die enge Verschränkung der Fach- und Informatikressourcen und die Steuerung der Digitalisierung auf oberster Leitungsebene. Zu diesem Zweck hat die Geschäftsleitung per 1. Januar 2021 einen Informatik-Ausschuss aus ihrer Mitte eingesetzt. Dieser erhielt den Auftrag, die in der geltenden Strategie 2017-2020 enthaltenen Ziele zur digitalen Transformation in einer IT-Strategie zu konkretisieren, die bereits laufende Überarbeitung der IS-Gouvernanz 1.0 von 2014 an die strategischen Anforderungen anzugleichen und die Ressourcen im Zusammenhang mit der Digitalisierung so zu organisieren, dass die digitale Transformation gut umgesetzt werden kann. Ein erster Entwurf für die Eckwerte der neuen IT-Strategie wurde nach einer ersten Lesung durch die Geschäftsleitung am 24. März 2021 intern in Konsultation gegeben; mittlerweile sind unter Beizug externer Experten intensive Arbeiten zum Aufbau einer agilen und stark integrierten Organisation für die digitale Transformation im Gang, diese werden im ersten Quartal 2022 erste Umsetzungsschritte zeitigen und sollen im Laufe des Jahres 2022 abgeschlossen werden. Zudem hat die Geschäftsleitung am 16. November 2020 den Auftrag zur Etablierung eines unabhängigen Qualitäts- und Riskmanagement in den Grossprojekten erteilt.

Anlässlich der Antrittsbesprechung mit der EFK am 23. März 2021 wurde diese über die laufenden Arbeiten an Strategie, Gouvernanz und IT-Organisation informiert und darauf hingewiesen, dass angesichts des laufenden Totalumbaus die jeweiligen Auskünfte eine Momentaufnahme darstellen.

Vor diesem Hintergrund begrüssen die Parlamentsdienste, dass auch die EFK die Arbeiten an Strategie und Gouvernanz als prioritär erachtet. Die im Bericht enthaltenen Hinweise zu den Inhalten der IT-Strategie und zu den zu klärenden Gouvernanzfragen sind mehrheitlich bereits Gegenstand der laufenden Arbeiten; die weiteren Hinweise sind hilfreich und werden in den Arbeiten berücksichtigt.

Die EFK beanstandet, dass verschiedentlich bestehende Konzepte und Arbeitsergebnisse der Projekte Cervin und CURIAPlus nicht in einem formalisierten Verfahren verabschiedet wurden. Dies macht es für Aussenstehende schwieriger, die Entscheidprozesse nachzuvollziehen. Hier werden sich die Parlamentsdienste in Zukunft bemühen, auch als kleine Verwaltungseinheit und trotz knapper Personal-Ressourcen möglichst revisionsfeste Prozesse vorzusehen.

Auch die Hinweise der EFK auf mögliche Sicherheitsrisiken sind wertvoll. Es ist insbesondere erfreulich, dass die Prüfung keine neuen Sicherheitslücken bei den Projekten Cervin und CURIAPlus, respektive bei der, beiden Projekten zugrundliegenden Zweit-Plattform ergeben hat. Die Aufarbeitung der Findings aus früheren Audits betreffend Cervin wird wie geplant per Ende März 2022 abgeschlossen. Damit ist auch die Sicherheit der Anwendung CURIAplus gewährleistet, da diese auf der Cervin-Umgebung aufsetzt. Mit auch künftig weiterhin vorgesehenen Sicherheitsaudits wollen die Parlamentsdienste sicherstellen, dass keine neuen Sicherheitslücken unerkannt bleiben. Aufgrund der Prüfung der EFK wurde zudem mit dem NCSC eine vertiefte und systematisierte Zusammenarbeit vereinbart.

Nicht nachvollziehbar ist für die Parlamentsdienste die grundsätzliche Kritik der EFK am Entscheid für eine Zweitplattformenstrategie. Zu Ende gedacht bedeutet diese Kritik, dass die erstmalige Wahl einer Plattform die betreffende Firma oder Verwaltungsstelle sozusagen «auf Dauer» an den entsprechenden Anbieter bindet – mit allen Nachteilen der daraus folgenden Abhängigkeit.

Schliesslich haben sich die Befürchtungen der EFK bezüglich der Realisierung von CURIAplus nicht bestätigt. Nach einer herausfordernden Anfangsphase schreitet die Realisierung nun zügig voran. Der vorgesehene Einführungszeitpunkt im 2023 wird nach heutigem Stand eingehalten, die Kosten ebenfalls.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die Parlamentsdienste sind die Stabsstelle des Parlaments und unterstützen die Bundesversammlung bei der Erfüllung ihrer Aufgaben. Damit die Parlamentarier ihren verfassungsmässigen Aufgaben nachkommen können, stellen die Parlamentsdienste die notwendigen Mittel bereit, insbesondere auch Informatiklösungen und Prozesse. Sie sind aus Unabhängigkeitsgründen dem Parlament und nicht dem Bundesrat unterstellt. Die Aufsicht und oberste Leitung der Parlamentsdienste obliegt der Verwaltungsdelegation, die aus sechs Parlamentariern besteht.

CURIAplus und Cervin sind zwei wichtige Informatikprojekte der Parlamentsdienste. Mit den beiden Vorhaben soll einerseits ein wesentlicher Schritt zur Digitalisierung realisiert, andererseits die Grundlage für nachfolgende Digitalisierungs-Vorhaben gelegt werden.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung ist zu beurteilen, ob die Initialisierung des Projekts CURIAplus gewährleistet, dass die Bedürfnisse der Nutzer abgedeckt und das Projekt erfolgreich geführt und gesteuert werden kann.

Prüffragen:

- Sind die Organisation und die Führung der Informatik der Parlamentsdienste so aufgestellt, dass Projekte erfolgreich definiert, umgesetzt und in Betrieb genommen werden können?
- Sind in der Projektorganisation CURIAplus die erforderlichen Kompetenzen und Fähigkeiten vertreten?
- Wurden der Projektumfang und die Lösung auf die Bedürfnisse der Nutzer ausgelegt (Scope, User Requirements und Business Case)?
- Unterstützt die IT-Architektur einen zukunftsorientierten, sicheren und kostengünstigen Betrieb? (Architekturgovernance)

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Luc Pelfini, Willy Müller und Daniel Wyniger von Ende März bis Ende Juni 2021 durchgeführt. Sie erfolgte unter der Federführung von Oliver Sifrig. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach Ende der Prüfungsdurchführung.

Zu Beginn der Prüfung hat die EFK festgestellt, dass das Projekt CURIAplus nicht ohne die vom Projekt Cervin geschaffenen und immer noch im Aufbau befindlichen Grundlagen funktionieren würde. Deshalb wurden Belange im Projekt Cervin, die für CURIAplus essentiell sind, ebenfalls geprüft. Da sowohl CURIAplus als auch Cervin auf der neuen Liferay-Plattform entwickelt und betrieben werden, steht primär dieses Umfeld im Fokus der Prüfung. Die Projekt-, Entwicklungs- und Betriebsumgebungen sowie die dazugehörenden Prozesse der Informatiklösungen auf Basis von Microsoft wurden nicht geprüft.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von den Parlamentsdiensten und deren Lieferanten umfassend erteilt. Die gewünschten Unterlagen (sowie die benötigte Infrastruktur) standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Aufgrund der Relevanz der Feststellungen hat die EFK die Geschäftsleitung der Parlamentsdienste und zwei Vertreter der Verwaltungsdelegation (VD) am 30. April 2021 über die Zwischenergebnisse informiert. Mit Schreiben vom 4. Mai 2021 wurden zudem die VD als Aufsichtsorgan der Parlamentsdienste, die Finanzdelegation sowie die Geschäftsprüfungskommission (GPK) über die ersten Feststellungen informiert. Erläuterungen zu den Feststellungen und Rückfragen der VD wurden in einer Sitzung am 28. Mai 2021 behandelt. Teilgenommen haben sowohl die VD wie auch die Geschäftsleitung der Parlamentsdienste.

Die Schlussbesprechung fand am 1.11.2021 statt. Teilgenommen haben von den Parlamentsdiensten der Generalsekretär der Bundesversammlung und der Bereichsleiter Infrastruktur & Sicherheit. Seitens EFK waren der Direktor, der zuständige Mandatsleiter, der zuständige Fachbereichsleiter und der Revisionsleiter vertreten. Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung dem Generalsekretär der Parlamentsdienste und der Verwaltungsdelegation obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Ausgangslage zu den Projekten Cervin und CURIAplus

2.1 Parlamentsdienste und Digitalisierung

Die Parlamentsdienste sind die Drehscheibe zwischen der Bundesversammlung und dem Bundesrat sowie zu weiteren Behörden und der Öffentlichkeit. Viele Aufgaben können die Parlamentarier, Kommissionen und die Mitarbeitenden der Parlamentsdienste ohne angemessene Digitalisierung nicht mehr oder nur erschwert wahrnehmen.

Mit einem Umsetzungsplan von 2016 haben die Parlamentsdienste drei für die Digitalisierung der Parlamentsdienste wichtige Projekte lanciert:

- **Cervin**
  Bereitstellung der neuen digitalen Arbeitsplattform (Applikationsportal) und Ablösung der bestehenden Intra- und Extranet-Lösungen (Parlnet). Erste produktive Einführung Ende 2019. Projektende noch offen.
- **CURIAplus**
  Ablösung der bestehenden CURIA-Anwendung. Bereitstellung der digitalen Infrastruktur zur Unterstützung der Parlamentarier und der parlamentarischen Geschäftsprozesse. In Realisierung seit Anfang 2021. CURIAplus basiert auf den von Cervin geschaffenen technischen Grundlagen.
- **Soprano**
  Entwicklung von Business-Intelligence-Systemen zur Unterstützung der parlamentarischen Arbeit. Das Projekt wurde ab 2018 realisiert und nach einem Pilotbetrieb im Sommer 2020 abgebrochen.

2.2 Digitalisierungsauftrag des Parlaments

Auftragserteilung durch das Parlament bzw. die Verwaltungsdelegation

Die Parlamentsdienste verfolgen seit Jahren die Digitalisierung der eigenen Geschäftsprozesse und derjenigen des Parlaments. Mehrere parlamentarische Vorstösse haben dies ebenfalls verlangt, zuletzt die Motion 17.4026 «digitaler Ratsbetrieb bis 2020». Die Motion wurde im Verlauf des Jahres 2018 von Stände- und Nationalrat angenommen und an die Verwaltungsdelegation überwiesen. Diese liess von den Parlamentsdiensten einen Bericht «Roadmap Digitalisierung im Parlament zur Umsetzung der Motion 17.4026» erstellen. Er beschreibt den Stand der Digitalisierung im Parlament ab 2019 und die vorgesehene Entwicklung bis 2023 anhand von bereits seit längerem geplanten Informatikprojekten. Im Bericht wird Digitalisierung primär als «informationstechnische Verarbeitung von Daten» verstanden und der ortsunabhängige Zugriff zum richtigen Zeitpunkt auf alle erforderlichen Informationen ins Zentrum gestellt. Die Verfasser betonen die Wichtigkeit der Governance über die Informatikprojekte und die Informationssicherheit. Die Parlamentsdienste werden ausserdem beauftragt, zur Förderung der Innovation eine flexible Struktur mit kooperative Arbeitsprozesse und -methoden zu entwickeln. Gefördert werden muss insbesondere eine flexible Arbeitsweise, die Fachkompetenzen, Entwicklung und Betrieb verbindet (Modell BizDevOps).

Bedeutung der Sicherheit

Der Ständerat hat den ursprünglichen Text der Motion «Digitaler Ratsbetrieb bis 2020» ergänzt mit der Forderung: «Die Sicherheit der Datenbearbeitung ist jederzeit zu gewährleisten. » In der Roadmap «Digitalisierung im Parlament» wird präzisiert, dass die digitalen Systeme die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu gewährleisten haben.

Welche Bedeutung der Sicherheit von Informatiksystemen des Parlaments zukommt, geht auch aus einem Bericht des Bundesrats zur Sicherheitspolitik der Schweiz vom 14. April 2021 hervor.[1] Darin weist er auf die Gefahr von Beeinflussungsaktivitäten hin. Sicherheitspolitisch relevant seien insbesondere Aktivitäten, die von Staaten ausgehen und sich gegen das Funktionieren eines Staates und einer Gesellschaft richten, um letztlich die demokratische Ordnung eines Staats zu unterminieren.

Das korrekte Funktionieren der Informatiksysteme, welche die Parlamentsarbeit unterstützen, hat nationale Bedeutung. So stuft das Bundesamt für Bevölkerungsschutz (BABS) die IKT-Infrastruktur des Parlaments bzw. der Parlamentsdienste neben den Systemen von Regierung, Justiz und Verwaltung als kritische Infrastruktur der Schweiz ein.[2]

2.3 Handlungsbedarf bei der Festlegung der Verantwortung für Sicherheitsanforderungen und Risikoakzeptanz

Weder im Parlamentsgesetz (ParlG) noch in der Parlamentsverwaltungsverordnung (ParlVV) ist geregelt, wer für die Definition der Sicherheitsanforderungen an die IKT-Infrastruktur des Parlaments, die Akzeptanz von grossen Risiken und die Überprüfung der Umsetzung von Massnahmen zuständig ist. Da das Parlament keine Sicherheitsanforderungen an die IKT-Systeme des Parlaments definiert hat (z. B. Cervin, CURIAplus), bleibt es den Parlamentsdiensten resp. deren einzelnen Informatikprojekten überlassen, diese zu formulieren.

Verantwortlichkeiten der Verwaltungsdelegation gemäss Informationssicherheitsgesetz

Die Bundesversammlung hat das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) verabschiedet. In diesem sind die Bundesversammlung als verpflichtete Behörde und die Parlamentsdienste als verpflichtete Organisation aufgeführt. Beide müssen das Gesetz umsetzen und ihren jeweiligen Verantwortlichkeiten und Aufgaben nachkommen. Da die Bundesversammlung nicht geeignet ist, um die Steuerungs- und Aufsichtsfunktion einer verpflichteten Behörde wahrzunehmen, überträgt das ISG diese der Verwaltungsdelegation. Sobald das ISG in Kraft tritt, ist die Verwaltungsdelegation daher mindestens für folgende im ISG beschriebenen Führungs- und Aufsichtsaufgaben verantwortlich und rechenschaftspflichtig:

- Oberste Führungsverantwortung: Festlegung der Ziele für Informationssicherheit, Eckwerte für den Umgang mit Risiken und Konsequenzen bei Missachtung von Vorschriften
- Erlass von Ausführungsbestimmungen für den Vollzug des ISG
- Erstellung von Vorsorgeplanungen für Fälle, in denen eine schwerwiegende Verletzung der Informationssicherheit die Erfüllung unverzichtbarer Aufgaben des Bundes gefährden könnte. Durchführung von geeigneten Übungen

[1] «Die Sicherheitspolitik der Schweiz – Bericht des Bundesrates», Entwurf vom 14. April 2021

[2] «Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022» vom 8. Dezember 2017, Kapitel 3.1

- Organisation, Umsetzung und Überprüfung der Informationssicherheit nach dem Stand von Wissenschaft und Technik
- Festlegung der Verantwortlichen Personen bzw. Stellen zur Klassifikation von Informationen
- Festlegung der Verfahren zur Gewährleitung der Informationssicherheit
- Festlegung der Mindestanforderungen für die verschiedenen Sicherheitsstufen.

Die Parlamentsdienste haben im August 2017 eine Analyse des ISG-Entwurfs und des Handlungsbedarfs erstellt und der Verwaltungsdelegation zugestellt.

Réflexions sur la composition de la Délégation administrative

En mars 2018, le Conseiller national (CN) Gerhard Pfister a déposé une interpellation relative à la surveillance des Services du Parlement (18.3301). Il y posait notamment la question suivante:

3. A l'heure actuelle, ce sont les trois membres de chaque collège présidentiel qui sont désignés pour siéger au sein de la Délégation administrative, et ce, pour une durée de fonction de trois ans seulement. La surveillance des Services du Parlement ne serait-elle pas améliorée si le Bureau du Conseil national choisissait d'autres membres pour composer la Délégation administrative ?

Le CN Pfister argumentait comme suit:

3. Les membres de la Délégation administrative sont, du fait qu'il s'agit des présidents et des vice-présidents des conseils, fortement tributaires du soutien qui leur est apporté par les personnes dirigeant les secrétariats des conseils. Dans le même temps, ils sont censés surveiller les Services du Parlement de manière indépendante et efficace. Selon le Code suisse de bonnes pratiques pour le gouvernement d'entreprise, édité par Economiesuisse, les membres des conseils d'administration ne sont considérés comme « indépendants » que s'ils n'entretiennent « aucune relation d'affaires avec la société ou des relations d'affaires relativement peu importantes ». Si l'on suit cette définition, la Délégation administrative ne peut être considérée comme indépendante des personnes dirigeant les secrétariats des conseils.

Outre ce problème de gouvernance, le CDF constate à la lumière du présent audit que les membres de la Délégation administrative sont confrontés à trois défis :

Assurer la continuité : la pratique actuelle entraîne des changements réguliers et automatiques au sein de la Délégation administrative. Ces changements permanents ne facilitent pas la surveillance sur la stratégie, la gouvernance et les projets informatiques, dont le déploiement s'étend souvent sur de nombreuses années.

Maîtrise techniques : le choix actuel des parlementaires ne tient pas compte de leurs connaissances dans le domaine de la gestion informatique.

Disponibilité : les membres des collèges présidentiels sont probablement les parlementaires qui ont le moins de temps à disposition pour suivre des dossiers extrêmement complexes.

La prochaine entrée en vigueur de la Loi fédérale sur la sécurité de l'information au sein de la Confédération va entraîner pour la Délégation administrative de nouvelles tâches et de nouveaux défis. Une réflexion du Parlement sur ce thème serait judicieuse.

Beurteilung

Dass in einzelnen Projekten entschieden wird, welche Sicherheitsanforderungen gestellt und welche (Rest-)Risiken akzeptiert werden, ist nicht stufengerecht. Die Projekte können ohne übergeordnete Vorgaben weder Sicherheitsanforderungen noch Risiken angemessen einschätzen. Die EFK hat bereits mit der Prüfung 16591 folgende Empfehlung abgegeben: «Die EFK empfiehlt dem Ressort «Informatik & neue Technologien» die Sicherheitsanforderungen zur Benutzung und zum Betrieb der Kollaborationsplattform der Räte klar zu definieren, durch die Verwaltungsdelegation bestätigen zu lassen und umzusetzen.» [3] Die EFK betrachtet die Empfehlung von 2016 als generell für alle Projekte gültig und erwartet deren konsequente Umsetzung.

Mit der Inkraftsetzung des ISG werden der Verwaltungsdelegation Führungsaufgaben in der Informationssicherheit zugewiesen, und sie muss für den Vollzug des ISG eine Ausführungsbestimmung erlassen. Dabei sollte auch geregelt werden, wie die Verwaltungsdelegation als Vertreterin der Bundesversammlung in den Risikomanagementprozess eingebunden wird. Um der erhöhten Verwundbarkeit zu begegnen, die sich aus der zunehmenden Digitalisierung ergibt, braucht es unter anderem klare Vorgaben in Bezug auf Risiko-Ownership und ein Risikoakzeptanzmodell (wer Risiken ab einem bestimmten Risikowert akzeptieren darf).

[3] «Wirtschaftlichkeit und Sicherheit der Informatik nach der Auslagerung», S. 23, abrufbar auf der Webseite der EFK (www.efk.admin.ch).

3 Projekt Cervin

Das Projekt Cervin schrieb am 5. Juli 2018 öffentlich ein Standardprodukt aus, das alle Parlamentsprozesse sowie die dafür benötigten Funktionen orts- und geräteunabhängig zur Verfügung stellen sollte. Diese Plattform ist auch das Fundament für CURIAplus.

Gemäss dem Projektleiter Cervin erfüllte keines der eingereichten Angebote das Eignungskriterium, dass Schlüsselpersonen sowohl Deutsch als auch Französisch auf höchster Kompetenzstufe beherrschen müssen. Im öffentlichen Verfahren hatten alle Anbieter Sharepoint angeboten. Das Ressort «Web» (heute Ressort «Publikationen & Produktion») hat gewünscht, dass auch andere Produkte als die übliche Microsoft SharePoint Lösungen angeboten werden, weil dieses Produkt in der Content Bewirtschaftung etliche Mängel aufweisen würde. Aus diesen Gründen haben die Parlamentsdienste die Ausschreibung abgebrochen und ein Einladungsverfahren durchgeführt. Zusätzlich zu einer Auswahl von Anbietern aus der offenen Ausschreibung wurde die Liferay-Anbieterin clavis IT zu einem Angebot eingeladen. Diese erhielt nach der Evaluation den Zuschlag.

3.1 Inbetriebnahme trotz fehlender Grundlagen

Die Anwendung Cervin/Parlnet ist seit Dezember 2019 in Betrieb und wird von den Parlamentariern genutzt. Der Qualitätsmanager hat in einer Mail an den Projektleiter wenige Tage vor der Freigabe der Produktivsetzung, diese als «höchst riskant» beurteilt. Die Anwendung sei unvollständig getestet, nicht abgenommen und mehrere notwendige Konzepte für die produktive Einführung würden fehlen. Er hat die Freigabe für den «Go-Live» erteilt, aber gleichzeitig klargestellt, dass er vom Abbruch des «Go Live» nur nicht abrät, weil es gemäss Auftraggeber keine Option sei, das alte System als Notlösung nach wie vor verfügbar sei und Druck auf dem Projekt notwendig sei, um anstehende Probleme zu lösen.

Die Anwendung Cervin wurde bis zum Prüfungszeitpunkt nicht abgenommen (weder Funktions- noch Sicherheitsabnahme), auch nicht einzelne Realisierungseinheiten. Projektauftraggeber und -leiter streben einen Abschluss mit formeller Abnahme bis Ende 2021 an. Als Grundlage dazu ermittelt der neue IT-Projektleiter seit Anfang 2021 alle noch nicht umgesetzten Anforderungen, nicht behobenen Fehler und Sicherheitslücken. Die Abnahmekriterien müssen noch definiert werden. Zur Umsetzung einiger offener Anforderungen müssen zuerst Spezifikationen bzw. Konzepte erstellt werden. Aufgrund der Komplexität der ausstehenden Arbeiten und der nicht absehbaren Aufwände ist gemäss Projekt Cervin noch nicht klar, ob der Projektabschluss wie gewünscht per Ende 2021 realisierbar ist.

Betriebsrelevante Konzepte sind noch nicht fertiggestellt. Dies betrifft insbesondere das Betriebskonzept, das Berechtigungs- und Benutzerverwaltungskonzept, das Monitoring- und Logging-Konzept sowie das Backup- und Recovery-Konzept. So fehlt im Betriebskonzept die Rollenteilung zwischen clavis IT und der IT der Parlamentsdienste. Im Backup-Konzept sind beispielsweise Angaben nicht vorhanden, ob Backup-Daten zum Schutz gegen Verschlüsselungsangriffe offline gespeichert oder wie das Wiederaufsetzen (Recovery) systemübergreifend mit Anwendungen und Daten sichergestellt werden kann.

Des Weiteren fehlt eine übergreifende Testumgebung für Cervin. Bereits früh haben sowohl der Testmanager als auch clavis IT auf das Problem hingewiesen. Deshalb können nicht alle Fehlerbehebungen und Neuentwicklungen in der Testumgebung getestet werden. Mehr-

fach mussten Tests direkt in der Produktionsumgebung durchgeführt werden. Gemäss Projektleiter Cervin soll mit der Implementation des von CURIAplus initialisierten «Portal Integrator Konzepts» auch eine Testumgebung aufgebaut werden.

Sowohl Betrieb und Wartung als auch Support sind mit clavis IT nicht vertraglich geregelt. Im Rahmenvertrag sind Optionen für Einzelverträge für Betrieb und Wartung (Option 6) sowie Support (Option 7) vorgesehen. Diese wurden aber noch nicht abgeschlossen. Im Anhang 3 des Rahmenvertrags ist ein Service Level Agreement (SLA) beschrieben, das mit dem Abschluss der Option 6 erst noch finalisiert werden muss. Einzelverträge für Betriebsleistungen treten gemäss Rahmenvertrag erst mit der erfolgreichen Abnahme der vorangehenden Projektleistungen in Kraft. Auf das Fehlen des Betriebs- und Wartungsvertrags hat clavis IT bereits am 19. September 2019, also vor der Betriebsaufnahme, aufmerksam gemacht. Interimistisch nimmt die Projektorganisation die Betriebs- und Supportaufgaben nach best-effort selbst wahr. Wegen fehlenden Supportverträgen muss das Projekt Supportaufwände über bestehende Verträge/Aufträge für Änderungen abrechnen.

Als gemeinsames Werkzeug für Problemtickets, Fragen, neue Anforderungen etc. verwenden clavis IT und die Parlamentsdienste das Werkzeug «JIRA». Verschiedene Problemtickets zeigen, dass Fehler, Anfragen und Probleme nicht rasch und nachhaltig analysiert sowie behoben werden. Der Lieferant hat mehrfach in Abstimmsitzungen und JIRA-Tickets darauf hingewiesen, dass seine Arbeiten blockiert sind oder verzögert werden, weil von den Parlamentsdiensten Antworten auf Fragen bzw. Entscheide zu Anforderungen fehlen.

Beurteilung

Dass eine Anwendung in Produktion geht, ohne systematisch getestet zu sein, ohne Überprüfung der Sicherheitsanforderungen, ohne fertiggestellte und umgesetzte Betriebskonzepte sowie ohne vertragliche Grundlagen, widerspricht bewährten Geschäftspraktiken. Ein solches Vorgehen führt vermehrt zu fehlerhaften Anwendungen, unsicheren Systemen, vermeidbaren Mehraufwänden und ist einer transparenten Ausgabenkontrolle nicht zuträglich. In Cervin aufgetretene Betriebsprobleme, Fehler und Sicherheitslücken hätten mit einem konformen Vorgehen aus Sicht der EFK erheblich reduziert werden können (vgl. Kapitel 3.2 Unvollständige Sicherheitsanforderungen und -massnahmen).

Die langen Liegezeiten von verschiedenen Tickets haben ihren Ursprung darin, dass die Parlamentsdienste ihrer Verantwortung als Auftraggeber von clavis AG nicht nachkommen, die Anforderungen an die Auftragnehmer zeitgerecht zu definieren und an Lösungskonzepten mitzuwirken.

Empfehlung

Hinweis: Im Kapitel 7 werden die Schlussfolgerungen und alle Empfehlungen thematisch gruppiert aufgeführt sowie Abhängigkeiten zwischen diesen erläutert.

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlungen 4 und 5.

3.2 Unvollständige Sicherheitsanforderungen und -massnahmen

In den Parlamentsdiensten gilt die vom Generalsekretär am 2. Februar 2015 erlassene «Weisung für die integrale Sicherheit in den Parlamentsdiensten». Sie regelt für die Parlamentsdienste die Prozesse, Zuständigkeiten, Aufgaben, Kompetenzen und Verantwortlichkeiten in Bezug auf die integrale Sicherheit. Die Weisung verlangt, dass Sicherheit und die Sicherheitsmassnahmen überprüfbar und messbar sein müssen. Es sind Nachweise in Form

von Protokollen, Aufzeichnungen, Belegen, Berichten etc. zu führen, welche die Einhaltung, Kontrolle und Überprüfung der geltenden Weisungen und Richtlinien bestätigen und nachvollziehbar machen. Für Projekte, die Änderungen an Informationssystemen zur Folge haben, gilt die «Richtlinie Informationssicherheit in Projekten» vom 1. September 2014. Diese lehnt sich inhaltlich an die Projektmethode HERMES an und legt die Grundsätze für Prozesse, Aufgaben, Kompetenzen und Verantwortlichkeiten für Projekte fest.

Für Cervin wurde in der Schutzbedarfsanalyse (Schuban) ein erhöhter Schutzbedarf festgestellt. Daher hat das Projekt drei Informationssicherheits- und Datenschutzkonzepte (ISDS-Konzepte) erstellt. Eines für die Anwendung, eines für den «Data Hub» und eines für die Web-Services. Diese hätten gemäss «Richtlinie Informatiksicherheit in Projekten» vor Abschluss der Phase Konzept fertiggestellt und vom Informationssicherheitsbeauftragten (ISBD) geprüft und freigegeben werden müssen. Zwei davon wurden erst im Zusammenhang mit der Produktivsetzung abgenommen. Dasjenige für die Web-Services liegt der EFK erst in einem Entwurf zur Freigabe vor. Die gemäss Weisung geforderte nachvollziehbare Dokumentation der Entscheide fehlt.

In den ISDS-Konzepten sind wichtige Risiken nicht aufgeführt. Beispiele sind Denial-of-Service-Attacken oder anbieterbezogene Sicherheitsrisiken, wenn dieser die Sicherheitsanforderungen nicht oder nicht angemessen umsetzt.

Der Rahmenvertrag mit dem Lieferanten clavis IT referenziert auf ein Dokument «Sicherheitsanforderungen bei den Parlamentsdiensten». Dieses enthält 26 konkrete Anforderungen an IKT-Systeme. Obwohl sie Vertragsbestandteil sind, wird im ISDS-Konzept nicht darauf referenziert. Zu den Anforderungen werden somit keine Massnahmen definiert. Beispiele dazu sind die Protokollierung von Zugriffen auf sensitive Daten oder der Schutz von Log- und Protokolldateien vor unerlaubten Veränderungen. Betreffend Aufbewahrungsdauer von Logdaten sind widersprüchliche Anforderungen dokumentiert.

Als weiteres Basisdokument für den Lieferanten gilt das «Betriebsmodell Housing». Dieses liegt in einem unfertigen Entwurf in Version 0.6 vor, ist aber gemäss Bereichsleiter «Infrastruktur & Sicherheit» bereits in Kraft. Verschiedene darin beschriebene Sicherheitsanforderungen sind nicht im ISDS-Konzept behandelt. Beispielsweise sind die Methoden und Prozesse nicht spezifiziert, wie ausser Betrieb genommene Datenträger zu vernichten sind. Voraussetzung für die Durchsetzung einer Vernichtungsvorgabe wäre, dass die Parlamentsdienste eine vertraglich festgehaltene Weisungsbefugnis auf den Unterakkordanten von clavis IT haben.

Beurteilung

Die Vorgaben zum Umgang mit IT-Projekten mit erhöhtem Schutzbedarf sind bei den Parlamentsdiensten angemessen. Sie können nur eine Wirkung entfalten, wenn sie eingehalten werden, was bei Cervin wie auch bei CURIAplus (vgl. Kapitel 4.2 Sicherheitsanforderungen und -massnahmen nicht definiert) nicht der Fall ist. Im ISDS-Konzept müssen die Risiken möglichst umfassend analysiert und daraus die Sicherheitsanforderungen abgeleitet werden. Zu den Sicherheitsanforderungen müssen Massnahmen definiert werden, welche die Risiken wirksam reduzieren. Wo dies nicht möglich ist, muss dies dem Auftraggeber transparent und verständlich kommuniziert werden, denn er hat die Restrisiken zu tragen. Die definierten Massnahmen sind dann im Rahmen der Realisierung umzusetzen und deren korrekte Umsetzung ist in regelmässigen Abständen zu überprüfen.

Die gemäss Richtlinie der Parlamentsdienste vorgeschriebenen Interventionspunkte zum beschriebenen Vorgehen wurden nicht eingehalten:

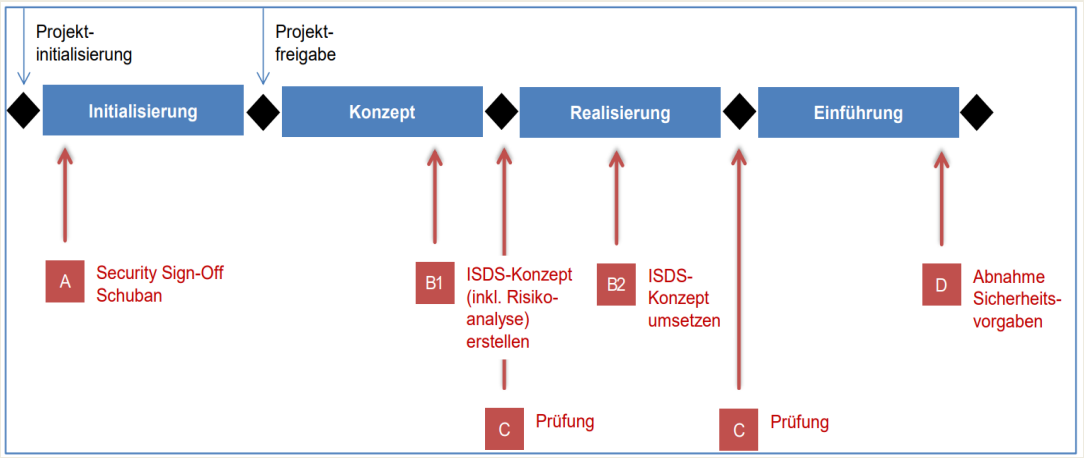


Abbildung 1: Projektphasen mit sicherheitsrelevanten Meilensteinen (Aktivitäten und Lieferobjekte), Quelle: «Richtlinie Informationssicherheit in Projekten», Parlamentsdienste

Da die Sicherheitsanforderungen und -massnahmen nicht rechtzeitig spezifiziert wurden, konnten sie vor der Freigabe des produktiven Betriebs nicht umgesetzt und überprüft werden.

Ein IT-System mit erhöhten Sicherheitsanforderungen darf nicht auf Basis von teilweise unfertigen, nicht qualitätsgesicherten Dokumenten, mit fehlenden und stellenweise widersprüchlichen Sicherheitsanforderungen erstellt und in Betrieb genommen werden. Gerade im Bereich Sicherheit ist ein systematisches Vorgehen, eine gewissenhafte Qualitätssicherung und die Einhaltung von Weisungen und Richtlinien unabdingbar.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 1, 4 und 5.

3.3 Sicherheitsmängel werden nicht zeitnah behoben

Gut ein halbes Jahr nach Produktivsetzung wurden zwei Sicherheitsaudits (September und November 2020) und eine Review der technischen Architektur (Herbst 2020) in Auftrag gegeben. Alle drei Überprüfungen zeigen sicherheitsrelevante Schwachstellen auf, einige davon sind als «hoch» eingestuft. Diese sind gemäss Schwachstellenklassifizierung im Bericht «schnellstmöglich zu beheben».

Der Bericht «Security Audit Parlnet» kommt zum Schluss, dass nicht alles Notwendige getan wurde, um einen ausreichenden Schutz der Anwendung zu gewährleisten. Das Resultat liegt gemäss Urteil der Prüfer unter dem Durchschnitt vergleichbarer Projekte. Die mit den Audits beauftragte Firma hat empfohlen, auch die nicht geprüften Komponenten einem Sicherheitsaudit zu unterziehen. Die Parlamentsdienste sehen dies erst nach der laufenden Architekturbereinigung vor. Der Bericht identifiziert insgesamt 9 Schwachstellen mit hohem[4], 31 mit mittlerem und 34 mit tiefem Schweregrad. Eine schnellstmögliche Umsetzung der als «hoch» eingestuften Schwachstellen wurde empfohlen.

[4] Im Bericht wir das Risiko «Hoch» wie folgt definiert: «Die Sicherheitsmassnahmen können direkt oder indirekt (mit vorherigem Aufwand) umgangen werden. Vertraulichkeit, Integrität und Verfügbarkeit der Umgebung ist unter Umständen nicht gewährleistet. Eine schnellstmögliche Umsetzung ist erforderlich. »

Protokolle belegen, dass die Projektleitung die Umsetzung des Sicherheitsreleases zweimal als «nicht prioritär» eingestuft hat. Gemäss schriftlicher Stellungnahme des Auftraggebers von Cervin wurden allerdings die aus Sicht der Parlamentsdienste «kritischen Issues» bereits 2020 behoben. Gemäss JIRA-Tickets war bis Ende 2020 keine der von der Audit-Firma als «hoch» eingestuften und nur eine der als «mittel» eingestuften Schwachstellen behoben.

Die Projektunterlagen vom 25. Mai 2021 weisen aus, dass bis zu diesem Zeitpunkt von den neun Schwachstellen mit hohem Schweregrad drei behoben worden sind. Sechs Schwachstellen sind noch offen. Davon betreffen drei konzeptionelle Mängel, die gemäss Projektleiter entsprechend aufwendig zu beheben sind:

1. Ein Rollenmodell fehlt, in dem die Rollen und ihre Rechte dokumentiert sind. Die vergebenen Zugriffsrechte sind nicht auswertbar und die Korrektheit der Rechtevergabe damit nicht überprüfbar.
2. Datenzugriffe können nicht nachvollzogen werden.
3. Es gibt kein Monitoring- und Logging-Konzept. Damit fehlen Voraussetzungen, um unerlaubte Zugriffe zu entdecken, beispielsweise auf Kommissionsdokumente.

Alle drei aufgeführten Sicherheitsanforderungen waren schon im Februar 2019 definiert, wurden aber trotz verschiedener Hinweise des Qualitätsverantwortlichen und von Mitarbeitenden des Ressorts «Informatik und neue Technologien» nicht umgesetzt.

Zum Prüfungszeitpunkt wies die von den Parlamentariern produktiv genutzten Anwendung gleich drei Schwachstellen auf, die es Angreifern ermöglichen, die Identität von Parlamentariern zu übernehmen:

- Liferay bietet als Standardfunktion die Möglichkeit, dass Rechteverwalter einzelnen Benutzern das Recht geben können, beliebige andere Benutzer zu «imitieren». Die «Imitation» ermöglicht es, ohne sich neu einloggen zu müssen, die Identität eines beliebigen anderen Benutzers zu übernehmen. Danach kann man in Liferay jegliche Aktionen ausführen, zu denen dieser berechtigt ist. Man kann sehen, was er sehen darf, die Daten herunterladen, die er herunterladen darf oder in seinem Namen Informationen anpassen, ändern und löschen. Gemäss Parlamentsdiensten sind das Einsehen der Abrechnungen in «Mein Raum» und Änderungen in «E-Parl» davon nicht betroffen. Ein Benutzer kann imitiert werden, während er selber bereits eingeloggt ist. Es wurde Extra-Code implementiert, damit die Imitation auch für selbst entwickelte Anwendungsteile funktioniert. Der technische Architekturreview hat darauf hingewiesen, dass die Imitation in Systemen mit sensitiven Daten nicht eingeschaltet werden sollte.
- Im Juni 2020 entdeckte der Chief Technology Officer (CTO), dass Personen mit Verwaltungsrechten im Active Directory durch Mutation eines einzigen Attributs im Active Directory die Identität eines beliebigen Benutzers in Cervin übernehmen können. Das Recht für derartige Mutationen haben rund 40 User, darunter mehrere Systemuser (technische User). Obwohl der CTO bereits damals Vorschläge gemacht hat, wie die Lücke behoben werden könnte, dauerte es bis Sommer 2021, bis die Sicherheitslücke geschlossen wurde.
- Liferay bezieht die Dokumente, wie beispielsweise Sitzungsprotokolle der Kommissionen, aus der auf Sharepoint implementierten Dokumentenverwaltung. Weil Sharepoint das vorgesehene Sicherheitsprotokoll nicht unterstützt, wurde dafür eine Ersatzlösung implementiert. Gemäss Sicherheitsaudit können Angreifer unter gewissen Umständen,

im Namen einer anderen Person auf Kommissionsdokumente mit Leserechten zugreifen. Die Fachabteilung hat den Antrag gestellt, auf eine Behebung der Sicherheitslücke zu verzichten, was der ISBD abgelehnt hat. Der Sicherheitsaudit vom 10. September 2020 empfahl, diese Lücke spätestens in vier Monaten zu beheben.

Die Log-Einträge wurden entgegen der Forderung im ISDS-Konzept «Web-Services» nicht überwacht und ausgewertet. Somit fehlen die technischen und organisatorischen Voraussetzungen für die Identifikation von Sicherheitsvorfällen und Unregelmässigkeiten. Es lässt sich daher nicht eruieren, ob Cervin/Parlnet seit Inbetriebnahme Ende 2019 angegriffen wurde.

Beurteilung

Die EFK begrüsst, dass der ISBD eine spezialisierte Firma mit Sicherheitsaudits beauftragt hat. Es ist zu bemängeln, dass bereits davor bekannte Schwachstellen nicht früher behoben wurden und die Behebung der in den Audits identifizierten Schwachstellen nicht umgehend an die Hand genommen wurde.

Besonders kritisch sind die Möglichkeiten der Identitätsübernahme. Es ist nicht akzeptabel, dass Personen – auch solche mit Administratorenrechten – sie benutzen können, ohne dass die Betroffenen dabei sind und sehen können, worauf die Administratoren zugreifen und welche Aktionen sie vornehmen. Ein weiterer schwerwiegender Mangel ist, dass die Logfiles nicht geschützt und ausgewertet werden sowie relevante Zugriffe nicht so aufgezeichnet werden, damit Angriffe entdeckt werden können.

Die Sicherheitsüberprüfungen sollten wiederholt und, wie im Sicherheitsaudit empfohlen, auf alle betroffenen Komponenten ausgedehnt werden. Ausserdem empfiehlt sich ein Codereview der von Cervin in Liferay implementierten sicherheitsrelevanten Funktionen. Auch künftig ist die korrekte Umsetzung der Grundschutz-, wie auch der erhöhten Sicherheitsanforderungen in regelmässigen Abständen zu überprüfen.

Ohne diese Massnahmen nehmen die Parlamentsdienste in Kauf, dass Schwachstellen unentdeckt weiterbestehen. Nach Einschätzung der EFK ist die vom Projekt Cervin bereitgestellte Infrastruktur aktuell nicht sicher genug, um darauf die noch deutlich sensiblere Anwendung CURIAplus zu implementieren und zu betreiben.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 1.

4 CURIAplus

4.1 Übersicht zum Projektverlauf

Seit den frühen 1990er-Jahren dient das für die Parlamentsdienste entwickelte CURIA der Verwaltung der Parlamentsgeschäfte. CURIA besteht aus mehreren einzelnen Anwendungen und einer Datenbank. Gemäss Parlamentsdiensten laufen bestehende Verträge 2022 aus, und die Anwendung ist an ihr Lebensende gekommen.

Bereits 2014 wurde eine Roadmap CURIA 2015–2020 erarbeitet. Ab 2017 wurden in der Initialisierungsphase Grundlagen zur Beschaffung einer neuen IT-Lösung CURIAplus erstellt. Die erarbeitete Studie empfahl, ein Standardprodukt für die Geschäftsverwaltung mit individueller Konfiguration zu beschaffen. Die Projektkosten wurden auf 2,7 Millionen Franken und die jährlichen Betriebskosten auf 0,5 Millionen Franken geschätzt.

Von Ende 2018 bis Ende 2019 hat das Projektteam in der Konzeptphase die Anforderungen und weitere Grundlagen für eine Ausschreibung des Projektes erarbeitet. Ziel war eine Ausschreibung mit Abschluss eines Werkvertrags. Die Geschäftsprozesse wurden durch Fachspezialisten der Parlamentsdienste beschrieben, die sich dabei auf ihre praktische Erfahrung und auf typische Benutzerprofile von Parlamentariern (sog. Personas) abstützten. Ergänzend dazu wurden Gespräche mit einzelnen Parlamentariern geführt. Auf eine systematische Abnahme von Geschäftsprozessen durch Parlamentarier sei wegen deren zeitlicher Belastung bewusst verzichtet worden. Die Parlamentsdienste beurteilen dieses Vorgehen als vertretbar, weil die Geschäftsprozesse detailliert in Gesetzen und Verordnungen definiert und über Jahre bzw. Jahrzehnte als *good practices* entstanden seien.

Im Verlauf der Konzeptphase wurde die im Projektauftrag gewählte Lösung basierend auf einer Standard-Geschäftsverwaltung als nicht zielführend beurteilt. Grund für diese Neuorientierung waren Abklärungen der Parlamentsdienste mit Lieferanten für Geschäftsverwaltungssysteme, Erfahrungen aus dem Pilotbetrieb «Papierloser Ständerat» und neue Anforderungen. Die Parlamentsdienste haben sich für Liferay als Basis für CURIAplus entschieden, um damit die mit Cervin aufgebaute Plattform zu nutzen. Das Architekturboard hat diesen Entscheid gestützt. Risiken und Probleme in Cervin wirken sich vielfach auch direkt auf CURIAplus aus.

Im Januar 2020 erfolgte die Ausschreibung auf simap.ch. Nach Aufforderung zu Nachbesserungen an die beiden einzigen Anbieter hat einer sein Angebot zurückgezogen. Basierend auf dem verbleibenden Angebot genehmigte die Geschäftsleitung im August 2020 die von 2,7 auf 4,5 Millionen Franken erhöhten Grundkosten für CURIAplus sowie die ebenfalls höheren Betriebskosten von 900 000 Franken pro Jahr. Die Optionen von rund 7 Millionen Franken wurden dabei nicht thematisiert.

Seit Ende 2020 befindet sich CURIAplus in der Realisierungsphase. Der Lieferant erstellt gemeinsam mit den Parlamentsdiensten die Detailspezifikation und implementiert diese.

Beurteilung

Die Laufzeit des Vorhabens CURIAplus ist mit ca. sieben Jahren bis zum Start der Realisierungsphase sehr lang. Dass die Parlamentarier nicht stärker in die Erarbeitung und Genehmigung der Anforderungen einbezogen wurden, ist nachvollziehbar, da deren verfügbare Zeit sehr begrenzt ist. Bei solchen Rahmenbedingungen wird üblicherweise ein Vorgehen

mit vielen kleinen Realisierungseinheiten gewählt. Der Abschluss eines Werkvertrages basierend auf Business Use Cases ohne Detailspezifikationen ist ein Risiko, da in der Regel Zusatzanforderungen und Anpassungen notwendig werden. Diese müssen in der Folge entweder weggelassen oder zusätzlich zum Werkvertrag bestellt werden.

4.2 Sicherheitsanforderungen und -massnahmen nicht definiert

Im Rahmen der Projektinitialisierung wurde eine Schuban erstellt und vom ISBD abgenommen. Darin wird festgehalten, dass ein erhöhter Schutzbedarf vorliegt und somit ein ISDS-Konzept und eine umfassende Risikoanalyse notwendig sind. Gemäss Vorgaben der Parlamentsdienste müsste festgelegt werden, in welcher Form der ISBD das Projekt begleiten und unterstützen soll. Ausserdem müsste eine Planung erstellt werden, wie die sicherheitsrelevanten Ergebnisse bei den Phasenübergängen von ihm geprüft und abgenommen werden. Dies ist nicht erfolgt und die in den internen Weisungen geforderte Abnahme des ISDS-Konzepts vor Freigabe des Phase Realisierung Ende 2020 blieb aus.

Das ISDS-Konzept liegt nach wie vor erst in der Version 0.9 vom 19. Dezember 2018 vor und enthält ungeklärte Grundsatzfragen und Kommentare von internen Fachpersonen. Es sind lediglich vier Risiken identifiziert. Manche der dazu definierten Massnahmen sind kaum oder völlig unwirksam. Beispielsweise kann der Service-Ausfall nicht durch ein SLA verhindert werden, sondern durch redundante Komponenten. Wichtige Risiken fehlen. Etwa solche, die sich aus der verfolgten Bring-your-own-Device-Strategie ergeben und solche, welche die Datenintegrität betreffen (d. h. die unberechtigte oder unbeabsichtigte Veränderung von Daten). Gemäss ISDS-Konzept wurden aber keine Restrisiken identifiziert.

Die fehlende Abnahme ist aus Sicht des Projektleiters CURIAplus wie auch des Sicherheitsbeauftragten der Bundesversammlung nicht kritisch, weil CURIAplus auf der Plattform von Cervin aufsetzt und dieses die Sicherheitsanforderungen von CURIAplus abdecke.

Beurteilung

Die Situation gleicht jener bei Cervin: Die gemäss Richtlinie der Parlamentsdienste vorgeschriebenen Interventionspunkte zum beschriebenen Vorgehen wurden nicht eingehalten, was den Verantwortlichen bekannt ist. Im Gegensatz zu Cervin wurde der ISBD aber nach Abnahme der Schuban nicht mehr einbezogen, was zusätzliche Risiken mit sich bringt.

Wie in der Schuban festgehalten, ist ein ISDS-Konzept für CURIAplus notwendig. Die Sicherheitsmassnahmen von Cervin können die Anforderungen von CURIAplus nicht vollständig abdecken, denn der System-, Funktions- und Datenumfang von CURIAplus und damit die Sicherheitsrisiken und -anforderungen sind deutlich grösser als bei Cervin. Ausserdem sind die ISDS-Konzepte von Cervin wie bereits dargelegt ihrerseits mangelhaft (vgl. Kapitel 3.2 Unvollständige Sicherheitsanforderungen und -massnahmen).

Die im ISDS-Konzept von CURIAplus enthaltene Risikoanalyse weist substanzielle Lücken auf, so sind gegenwärtig keine Massnahmen definiert, um Angriffen zu begegnen wie:

- das systematische Herunterladen von Kommissionsunterlagen für Aussenstehende;
- mutwillige oder ungewollte Veränderungen von Daten eines Parlamentsmitglieds zu dessen Schaden;
- Denial-of-Service-Attacken, die CURIAplus lahmlegen;
- Ransomware-Attacken.

Bereits vor der Ausschreibung hätte das Projekt CURIAplus eine detaillierte Risikoanalyse durchführen müssen. Entsprechende Vorlagen wären beispielsweise im BSI-Grundschutzpapier enthalten, auf dem die Parlamentsdienste basieren. Nur so hätte das Projekt die nötigen Sicherheitsanforderungen und -massnahmen ableiten und im Pflichtenheft, der Systemarchitektur und den Verträgen spezifizieren können. Da die Anbieter sie unvollständig kannten, konnten sie sie in ihrer Offerte auch nicht vollumfänglich berücksichtigen.

Gerade in sicherheitskritischen Anwendungen beeinflussen Sicherheitsüberlegungen häufig die Benutzer-Abläufe. Nicht alles was sich Benutzer wünschen, ist aus Sicherheitsüberlegungen zulässig. Mangels Risikoanalyse und Sicherheitsanforderungen konnten und können solche Abwägungen bei der Erstellung der Detailspezifikationen und der Implementierung nicht berücksichtigt werden.

Gesamthaft betrachtet ist das Risiko hoch, dass die erstellte Anwendung wie im Projekt Cervin Sicherheitslücken aufweisen wird und Nachbesserungskosten zu deren nachträglichen Schliessung anfallen werden. Ausserdem zeigt die Erfahrung, dass es nicht immer möglich ist, Sicherheit im Nachhinein in Systeme «einzubauen». Das kann in letzter Konsequenz bedeuten, dass eine Lösung komplett neu aufgebaut werden muss.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 6.

4.3 Betrieb und Entwicklung ungenügend geregelt

clavis IT soll den Betrieb der Liferay-basierten Komponenten von CURIAplus übernehmen. Obwohl die erste Realisierungseinheit auf Ende März 2021 terminiert war, waren die Entwicklungs-, Test- und Integrationsumgebungen wie auch die zugehörigen Bereitstellungsprozesse Mitte Jahr noch im Aufbau. Die konzeptionelle Grundlage dafür bildet das «Portal Integrator Konzept» für eine Multi-Lieferanten-Plattform. Es beschreibt die Bedingungen, die zu schaffen sind, damit mehrere Lieferanten parallel Liferay-Anwendungen für das Parlaments-portal entwickeln können, die reibungslos miteinander funktionieren. Ausserdem dokumentiert es die dafür nötigen technischen Grundlagen und Prozesse.

clavis IT erstellt ein solches Konzept zum ersten Mal und kennt kein anderes Unternehmen, das eine Multi-Lieferantenplattform für Liferay entwickelt hat und produktiv nutzt. Von der Version 1.6 vom 29. April 2021 ist erst der technische Teil abgenommen, die organisatorischen Themen hingegen noch nicht. Unter anderem noch nicht geregelt ist der Umgang mit Releasewechseln. Die Verwaltung von Testdaten und -werkzeugen wird im Dokument nicht behandelt. Im Konzept «bewusst» nicht berücksichtigt sind Komponenten, die nicht von clavis IT betrieben werden, z. B. die von den Parlamentsdiensten für CURIAplus zu betreibenden Datenbanken. Dazu wird vermerkt, dass nicht von jedem Umsystem ein Testsystem vorhanden sei.

Für CURIAplus liegt ein Betriebskonzept vom Februar 2020 vor. Es enthält über 30 Use Cases als Kapitelüberschrift ohne ausformulierten Inhalt. Gemäss dem Projektleiter CURIAplus soll das Konzept überprüft werden, nachdem clavis IT das «Portal Integrator Konzept» fertiggestellt hat.

Wer künftig die übergreifende Betriebsverantwortung für alle CURIAplus-Komponenten (Liferay, SQL-Datenbank etc.) tragen soll, ist noch ungeklärt.

Beurteilung

Dass die Entwicklungs-, Test- und Integrationsumgebungen auch für CURIAplus ein halbes Jahr nach Realisierungsstart und drei Monate nach dem Termin für die erste Realisierungseinheit noch nicht vollumfänglich zur Verfügung stehen, bemängelt die EFK. Dass die Betriebsmodalitäten, Prozesse und Zuständigkeiten der zugrundeliegenden, von Cervin bereitzustellenden Liferay-Plattform noch nicht abschliessend geklärt sind, kommt erschwerend hinzu. Eine zielgerichtete, effiziente Entwicklungsarbeit und ein ordnungsgemässes Testen sind so nur bedingt möglich.

Mit der geplanten Multi-Lieferantenplattform begeben sich die Parlamentsdienste wie auch die Betreiberin auf unbekanntes Terrain. Ob die angedachte Lösung ausbau- und betreibbar bleibt, wird sich erst offenbaren, nachdem schon viel investiert worden ist.

Die Betriebsaufgaben und -verantwortlichkeiten der Parlamentsdienste im Kontext CURIAplus und die Gesamtbetriebsverantwortung müssen geklärt werden. Die Prozesse des Testens, der Freigabe und Inbetriebnahme müssen betreiberübergreifend definiert werden, damit nicht dieselben Probleme wie bei Cervin auftreten.

4.4 Mängel im Projekt-Qualitäts- und -Risikomanagement

Fehlendes unabhängiges Qualitäts- und Risikomanagement

Auf Stufe der Informatikprojekte der Parlamentsdienste ist kein unabhängiges Qualitäts- und Risikomanagement (QRM) etabliert. Im Oktober 2020 hat die Geschäftsleitung beschlossen, dass für IKT-Grossprojekte wie beispielsweise CURIAplus, ein unabhängiges QRM inklusive Projektcontrolling und -reporting aufgebaut werden soll. Sie hat den Leiter «Finanzen, Systeme & Administration» damit beauftragt, der dazu eine externe Unterstützung beigezogen hat. Per Februar 2021 haben beide der Projektauftraggeberin ein Konzept für die Einführung des QRM in CURIAplus vorgestellt. Seither kommt die Etablierung eines unabhängigen QRM nicht weiter, trotz umsetzungsbereitem Konzept und verfügbarem Qualitäts- und Risikomanager für CURIAplus.

Ungenügendes Projekt-Risikomanagement

Der Projektleiter CURIAplus aktualisiert monatlich den Risikobericht und liefert diesen an die Auftraggeberin und das Kernteam. In die Risikoberichte nimmt er keine Risiken auf, zu denen keine risikomindernden Massnahmen bekannt sind oder die von der Auftraggeberin bereits akzeptiert wurden.

Die Risiken decken hauptsächlich solche ausserhalb des Projektes ab (z. B. Schnittstellen). Im Risikobericht fehlen Projektrisiken, die teilweise von Mitarbeitenden bereits gemeldet oder in externen Berichten identifiziert wurden. Beispielsweise:

- Vom IT-Projektleiter gemeldete Risiken aufgrund der in Cervin identifizierten Sicherheitsschwachstellen (gemäss Bericht «Security Audit Parlnet»), die sich auf CURIAplus auswirken. Für Details vgl. Kapitel 3.3 Sicherheitsmängel werden nicht zeitnah behoben.
- Aus dem Ressort «Informatik & neue Technologien» gemeldete Risiken im Zusammenhang mit der Wahl von Liferay als Plattform für CURIAplus.

- Gemäss Projektberichten nimmt das Risiko für Verzögerungen der Einführung ab Februar 2021 wegen Mehraufwänden für die Detailspezifikation und Realisierung, erheblich zu. Falls deswegen die Ende 2022 auslaufenden Verträge für CURIA verlängert werden müssen, besteht das Risiko für Mehraufwände.
- Risiko einer Einführung per Stichtag mit allen Schnittstellen und Abhängigkeiten (Big-Bang-Einführung), ohne Möglichkeit für einen Parallelbetrieb.

Beurteilung

Es ist positiv, dass die Geschäftsleitung im Herbst 2020 die Einführung eines unabhängigen QRM für Grossprojekte beschlossen hat. Weshalb dieses aber nicht eingeführt wird, obschon eine Lösung erarbeitet wurde, ist nicht nachvollziehbar.

Das Risikoreporting von CURIAplus vermittelt ein unvollständiges Bild. Beispielsweise werden von Fachpersonen und in unabhängigen Beurteilungen identifizierte Risiken nicht aufgenommen. Ausserdem widerspricht es der bewährten Praxis, Risiken nicht zu rapportieren, zu denen keine risikomindernden Massnahmen möglich sind. Auch einmal akzeptierte, aber wesentliche Risiken müssen weiter rapportiert werden, da sich deren Beurteilung ändern kann.

Wenn bekannte Risiken nicht im Risikomanagement geführt werden, fehlt die Ableitung von risikomindernden Massnahmen. Ausserdem werden Veränderungen der Risikosituation so nicht erkannt.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 3.

4.5 Ungenügende Einbindung aller Rollen in die Projektarbeit

Die Einbindung der Architekten und des ISBD werden nicht wie in den Parlamentsdienstrichtlinien oder HERMES vorgesehen konsequent sichergestellt. Ausserdem wünscht der Projektleiter keine direkten Kontakte zwischen den im Projekt involvierten Parteien. Nach seiner Einschätzung seien diese nicht notwendig, verfrüht oder ineffizient. Er lässt daher Anfragen und Klärungen über sich selber als «single point of contact» laufen. Verschiedene Parteien haben geltend gemacht, dass unter diesen Umständen ihre Arbeiten stark erschwert seien. So hat der Lieferant für CURIAplus im Juni 2021 als Grundbedingung für eine Weiterarbeit gefordert, dass er bei Bedarf mit allen beteiligten Parteien direkt kommunizieren kann. Der Projekterfolg sei sonst gefährdet.

Mitverursacht und erschwert wird die Situation durch Spannungen zwischen den Fachverantwortlichen und Vertretern der Einheiten «Innovation und Fachanwendungen» mit Vertretern der Einheit «Informatik & neue Technologien».

Beurteilung

Ein Informations- und Koordinationsmonopol wie es in CURIAplus zu beobachten ist, erhöht die Risiken für Missverständnisse, Verzögerungen und Informationsdefizite und gefährdet daher den Projekterfolg. Die konstruktive Zusammenarbeit der beteiligten Parteien wird stark behindert, sowohl bei internen als auch externen Stellen.

Unter den im Verlauf der Prüfung eingesehenen Fragen, Hinweise und Risikomeldungen aus dem Ressort «Informatik & neue Technologien» konnte die EFK kritische, aber keine

offensichtlich unsachlichen oder tendenziösen Meldungen identifizieren. Fragen oder Hinweise waren nachvollziehbar und sachlich begründet.

Die gemäss «Roadmap Digitalisierung» im Parlament zur Umsetzung der Motion 17.4026[5] verlangte Einführung einer flexiblen Arbeitsweise nach dem Modell der «BizDevOps» und die in der Zweisparten-Strategie verlangte Innovation und Agilität werden durch die gelebte Kultur verhindert. Für eine Entwicklung in Richtung BizDevOps und Agilität müssten die Parlamentsdienste geeignete Massnahmen treffen. Das wären beispielsweise interdisziplinäre Teams (Fach, Entwickler und Betreiber), eine offene Kommunikationskultur und kooperative Arbeitsprozesse.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 4.

4.6 Rasch ansteigendes Realisierungsrisiko

Der Meilenstein «Realisierungseinheit 1» per März 2021 konnte nicht eingehalten werden. Das wird gemäss Projektstatusbericht auch für den Meilenstein «Realisierungseinheit 2» per September 2021 zutreffen. Der geplante Funktionsumfang soll gemäss Projektleiter CURIAplus trotzdem bis zum Einführungstermin noch realisierbar sein, was der Lieferant aber als nicht machbar erachtete. Ausserdem treten Terminverzögerungen bei mindestens zwei Umprojekten auf, die für CURIAplus Funktionen oder Daten zur Verfügung stellen müssen (Gottardo, Cervin). Eine systematische, projektübergreifende Abstimmung zu Inhalten und Terminen ist nicht etabliert.

Die Ursachen für Verzögerungen und Mehraufwände werden von den Parlamentsdiensten und dem Lieferanten unterschiedlich beurteilt. Erschwert wird die Softwareentwicklung von CURIAplus durch fehlende Definitionen und Konzepte, die der Lieferant für die Implementierung benötigt. Beispiele sind die Schnittstellen-Definitionen zum Enterprise Service Bus, zum Identity und Access Management oder das Portal-Integrator-Konzept.

Beurteilung

Fehlenden Grundlagen, Konzepte und Spezifikationen für die Implementierung sowie Abhängigkeiten von anderen Projekten und Uneinigkeiten zwischen den Parlamentsdiensten und dem Lieferanten führen zu einem raschen Anstieg des Realisierungsrisikos, bevor das erste Viertel der Realisierungsphase überhaupt vorbei ist. Das Fehlen einer projektübergreifenden Steuerung erschwert die Früherkennung und Problemlösung bei Abhängigkeiten gegenüber anderen Projekten und Vorhaben.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 2.

4.7 Uneinigkeit über den Auftragsumfang

In der Realisierungsphase seit Januar 2021 erarbeitet der Lieferant gemeinsam mit den Parlamentsdiensten die Detailspezifikationen pro Business Use Case. Nach einigen Monaten Realisierungsphase besteht zwischen den Parlamentsdiensten und dem Lieferanten Uneinigkeit, ob die gemeinsam zu erarbeitenden Detailspezifikationen zu einer Ausweitung des

[5] «Digitaler Ratsbetrieb bis 2020»

Auftrages führen. Aus Lieferantensicht werden damit nicht nur Business Use Cases konkretisiert, sondern auch Anforderungen formuliert, die über den ausgeschriebenen Umfang hinausgehen. Der Lieferant führt eine grössere Menge an Differenzen auf, beispielsweise:

- In den Detailspezifikationen werden Funktionen verlangt, die über die Standardfunktionen von Liferay hinausgehen. Die Grundannahme bzw. Forderung in der Ausschreibung zur Verwendung der Standardfunktionen kann nicht eingehalten werden und Funktionen müssten individuell und aufwendig nachgebaut werden.
- Im Business Use Case beschriebene Datenfelder zu einem Ratsmitglied mit 11 Datenfeldern vs. 166 Datenfelder in der Detailspezifikation.

Der CURIAplus-Projektleiter und die Auftraggeberin sind der Meinung, dass die Detailspezifikationen lediglich Konkretisierungen zu den Ausschreibungsunterlagen enthalten, die somit Teil der gemäss Werkvertrag zu erbringenden Leistungen sind. So sei etwa beim zweiten Beispiel die Anzahl der Datenfelder im Datenmodell (Beilage zur Ausschreibung) erkennbar und werde aus dem Business Use Case ersichtlich.

Seit April 2021 sollte eine Besprechung zwischen den Parlamentsdiensten (Auftraggeberin und Projektleiter CURIAplus) sowie dem Lieferanten stattfinden. Ziel war eine gütliche Einigung in den strittigen Punkten. Zur Vorbereitung hat der Lieferant eine Aufstellung der Punkte erarbeitet, in denen nach seiner Ansicht der Umfang der Ausschreibung wesentlich überschritten wird, und der Projektleiter hat diese zusammen mit der Fachprojektleiterin kommentiert.

In einem Treffen Mitte Juni konnte dem Lieferanten zufolge keine Einigung erzielt werden. Als nächster Schritt sei vereinbart worden, dass beide Parteien Voraussetzungen definieren, die aus ihrer Sicht für einen Projekterfolg notwendig sind. Weiter sei vereinbart worden, dass ein Testlauf im Juni 2021 anschliessend zeigen soll, ob ein gemeinsamer und zielführender Weg gefunden werden kann. Für Ende Juli 2021 sei dann eine weitere Sitzung geplant, um das weitere Vorgehen festzulegen.

Beurteilung

Die unterschiedliche Einschätzung bezüglich der im Werkvertrag enthaltenen Leistungen erschweren die Zusammenarbeit zwischen den Parlamentsdiensten und dem Lieferanten und können potenziell zu Mehrkosten oder einem Projektabbruch führen.

5 Steuerung der Informatik bei den Parlaments-diensten

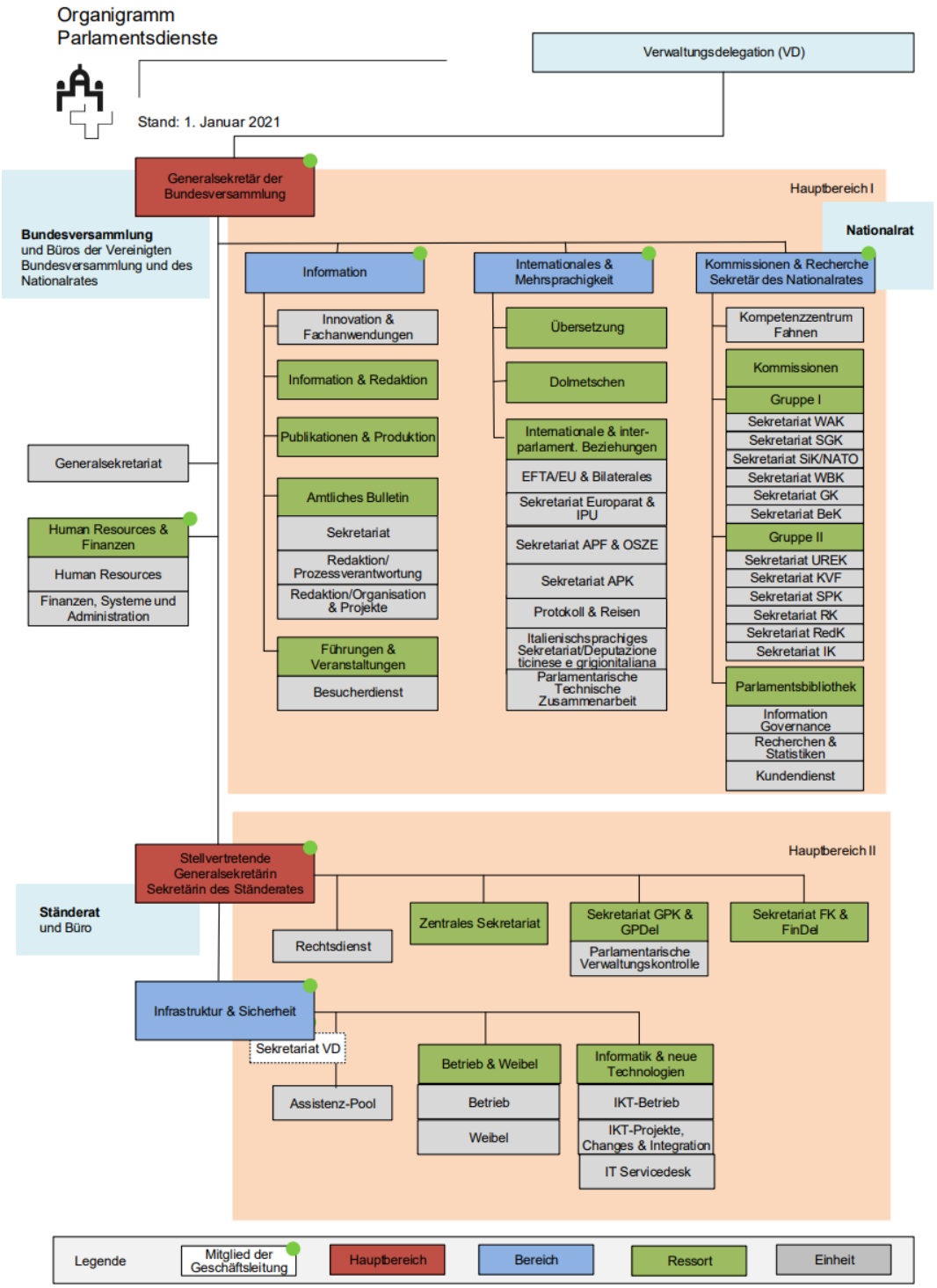


Abbildung 2: Organigramm der Parlamentsdienste per 1.1.2021 (Quelle: Parlamentsdienste)

Per 1. Januar 2021 wurde das Ressort «Sicherheit & Projektmanagement» aus dem Bereich «Infrastruktur» ausgegliedert und im Bereich «Information» direkt dem Bereichsleiter unterstellt. Das bisherige Ressort ist neu eine Einheit und wurde in «Innovation & Fachanwendungen» umbenannt. Mit dieser Trennung der Projektleiter vom Ressort «Informatik & neue Technologien» sollten Spannungen zwischen den beiden Gruppierungen entschärft werden und der Leiter «Infrastruktur» von seiner Vermittlerrolle entlastet werden.

5.1 IKT-Strategie und -Governance fehlen

In den Parlamentsdiensten gilt die IKT-Governance von 2014 nach wie vor, und es besteht keine IKT-Strategie. Mit verschiedenen Aufträgen hat die Geschäftsleitung der Parlamentsdienste die Aktualisierung der IKT-Governance und die Erarbeitung einer IKT-Strategie veranlasst. Dieser Prozess verlief nicht immer gradlinig und wurde durch die Pandemie 2020 erschwert.

Externe Beurteilung der Informatik stellt Handlungsbedarf zur Steuerung der IKT fest

Vor der Neubesetzung der Ressortleitung «Informatik & neue Technologien» per 1. April 2020 wurde die Informatik einer umfassenden externen Analyse unterzogen. Die Analyse identifiziert grossen Handlungsbedarf und hat verschiedene Empfehlungen gemacht.

IKT-Strategie

Da die Parlamentsdienste über keine IKT-Strategie verfügten, erteilten die Stellvertretende Generalsekretärin und der Bereichsleiter «Infrastruktur & Sicherheit» dem im April 2020 neu eintretenden Ressortleiter «Informatik & neue Technologien» den Auftrag, eine IKT-Strategie und eine IKT-Governance zu erstellen. Im Verlauf der Arbeiten wurden diese sistiert. Stattdessen wurde unter Leitung des IT-Ausschusses der Geschäftsleitung die «Eckwerte einer Zweispartenstrategie für die Informatikdienstleistungen» erarbeitet. Sie wurden im März 2021 fertiggestellt und schlagen vor, die Informatik der Parlamentsdienste in zwei Sparten aufzuteilen:

- Die Sparte I bildet die IT-Unterstützung für die parlamentarischen Prozesse. Hier soll Innovation und Agilität im Vordergrund stehen. Die Lösungen sollen auf Liferay / Open Source aufbauen.
- Die Sparte II deckt die IT-Unterstützung für operative Supportprozesse der Parlamentsdienste ab. Hier sollen primär Standardprodukte auf Basis von Sharepoint und Windows zum Einsatz kommen.

Vorgaben, Anforderungen und Verantwortlichkeiten sind je nach Thema für beide Sparten identisch oder abweichend definiert. Für die Themen Verantwortung, Serviceorganisation und finanzielle Steuerung des Betriebs werden je zwei Optionen vorgeschlagen, die noch entschieden werden müssen. Die Koordinationsverantwortung für beide Sparten hängt von der Wahl dieser Optionen ab. Die «Eckwerte einer Zweispartenstrategie» sind als Entwurf vorhanden und werden intern diskutiert und weiterentwickelt.

IKT-Governance

2014 wurde die erste IKT-Governance der Parlamentsdienste in Kraft gesetzt. Die Steuerung der IKT-Unterstützung des Parlaments und der Parlamentsdienste wurde auf drei Steuerungsgremien verteilt: Geschäftsleitung, Strategische Steuerung Informationssysteme, Operative Führung Informationssysteme.

Die Geschäftsleitung hat 2018 den Auftrag erteilt, die IKT-Governance zu überarbeiten. Aufgrund der Rückmeldungen und Diskussionen zum Entwurf der neuen IKT-Governance hat die Geschäftsleitung im April 2020 beschlossen, die Abnahme bzw. Inkraftsetzung um ein Jahr zu verschieben. Grund waren u. a. Abhängigkeiten mit Organisationsstruktur, Prozessdefinitionen, IKT-Strategie. Ausserdem sollten die Ergebnisse der Personalumfrage und der IT-Analyse über die Informatik (externer Bericht vom April 2020) berücksichtigt werden. Die Gremien ABE (Ausschuss zur IKT-Bedarfsevaluation) und APPF (Ausschuss zur Vorbereitung des strategischen Projektportfolios) arbeiten jedoch bereits auf Grundlage der neuen IKT-Governance weiter. Der IKT-Betrieb wird nicht in der IKT-Governance geregelt. Leistungen und Anforderungen des Betriebs werden durch die Geschäftsleitung festgelegt.

Im Januar 2021 wurde der IT-Ausschuss der Geschäftsleitung gegründet und übernahm die steuernde Funktion der Informatik, die in Unternehmen häufig vom Chief Information Officer (CIO) wahrgenommen wird. Von den Mitgliedern des IT-Ausschusses verfügt nur eine Person über Informatikkenntnisse und -erfahrung: der Bereichsleiter «Infrastruktur & Sicherheit». Der IT-Ausschuss ersetzt das strategische Steuerungsgremium. Die EFK hat widersprüchliche Aussagen darüber, ob und wie der Ressortleiter «Informatik & neue Technologien» einbezogen wird.

Beizug externer Experten zur Erarbeitung von IKT-Strategie, -Governance, Soll-Architektur etc.

Am 12. Mai 2021 haben die Parlamentsdienste bekannt gegeben, dass sie externe Experten mit der Erarbeitung der Digitalisierungsstrategie beauftragt haben.[6] Der Auftrag muss zwischen Anfang Mai und Ende Oktober 2021 erledigt werden und umfasst die Erarbeitung einer Digitalisierungsstrategie (inkl. Sourcing, Organisation etc.), IKT-Governance und Architekturzielbild. Ausserdem soll ein Massnahmenplan zur Umsetzung erstellt werden und das Setup für eine Steuerung der Umsetzung geschaffen werden.

Beurteilung

Es ist wichtig, dass die Informatik im IT Ausschuss der Geschäftsleitung angemessen vertreten ist. Dadurch wird die nahtlose Zusammenarbeit von Fach und Informatik auf strategischer Ebene unterstützt.

Ohne IKT-Strategie und IKT-Governance kann die Geschäftsleitung die Entwicklung und den Betrieb der IKT nicht steuern. Dies führt dazu, dass Projekte eigenmächtig Entscheide treffen, die nur schwer zu korrigieren sind. Ausserdem fehlt eine umfassende und übergeordnete Ausrichtung und Steuerung der Informatik für das Parlament und die Parlamentsdienste. Daher ist die Auftragserteilung zur Erarbeitung von IKT-Strategie und IKT-Governance durch die Geschäftsleitung zielführend, benötigte aber längere Zeit und ist noch nicht abgeschlossen.

Die EFK begrüsst den Beizug von externen Spezialisten zur Erarbeitung dieser komplexen und wichtigen Grundlagen. Angesichts der schwierigen Ausgangslage und des umfassenden Auftrags beurteilt die EFK den gesetzten Zeitrahmen allerdings als zu ehrgeizig. Auch der Einbezug von Mitarbeitenden für eine nachhaltige und breit abgestützte Entwicklung ist in dieser kurzen Zeit schwer sicherzustellen.

[6] Medienmitteilung der Parlamentsdienste vom 12. Mai 2021

Die wesentlichen Feststellungen, Beurteilungen und Empfehlungen der externen Beurteilung vom April 2020 decken sich weitgehend mit denen der EFK aus dieser Projektprüfung. Bedauerlich ist, dass seither ein Jahr verstrichen ist.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 4.

5.2 Outsourcing nicht strategisch geführt

Outsourcing ohne Sourcing-Strategie

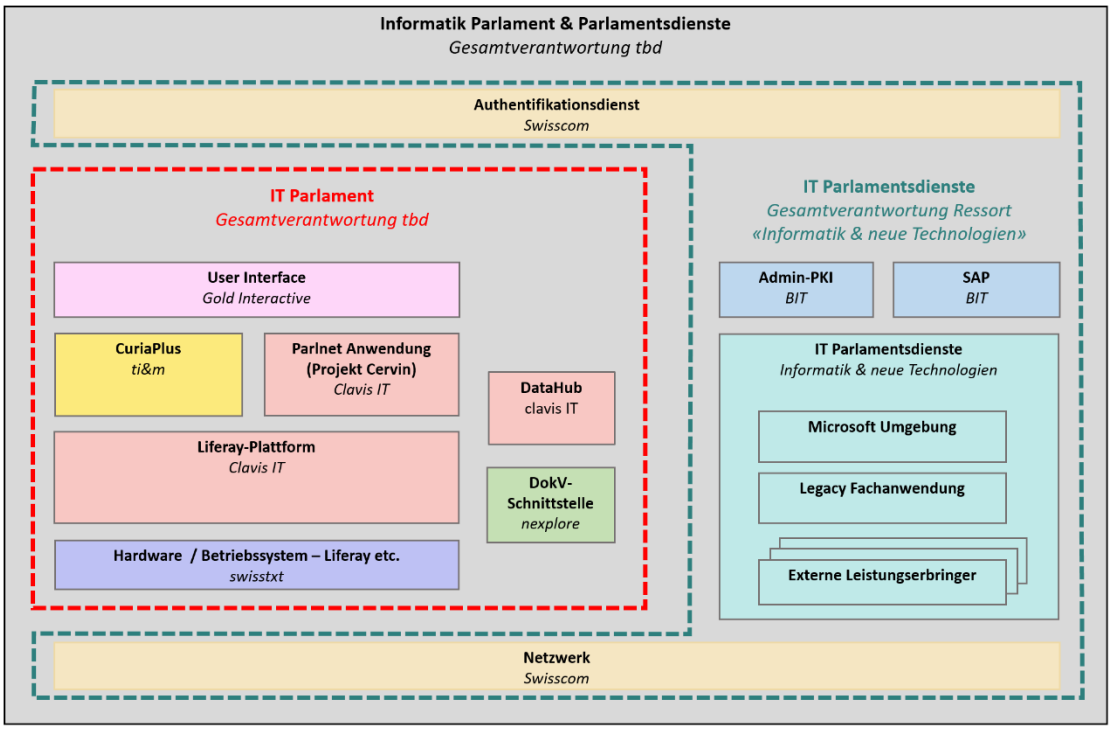


Abbildung 3: IT-Komponenten (fett geschrieben) mit Entwicklungs- und Betriebspartnern der Parlamentsdienste (Darstellung EFK)

Bis zur Einführung der Open-Source-Plattform für neue Informatiklösungen für das Parlament hatte das Ressort «Informatik und neue Technologien» die Gesamtverantwortung für den Informatikbetrieb (Abbildung 3, grüner Rahmen). Es arbeitet mit Swisscom und dem BIT zusammen.

Mit den Projekten Cervin und CURIAplus kamen weitere Sourcing-Partner dazu. Die Parlamentsdienste haben den Betrieb von Parlnet/Cervin und damit auch der künftigen Plattform für den Parlamentsbetrieb an die Firma clavis IT ausgelagert. Die Bereitstellung und der Betrieb der Hardware und die Gestaltung der Benutzerschnittstelle hat clavis IT seinerseits an Unterakkordanten ausgelagert, die in keinem Vertragsverhältnis zu den Parlamentsdiensten stehen. Somit können die Parlamentsdienste auch nicht sicherstellen, dass vertragliche Verpflichtungen von clavis IT auch für die Unterakkordanten gelten. Das Outsourcing basiert nicht auf einer Sourcing-Strategie.

Management des Outsourcings der Liferay-Umgebung ungenügend

Im Rundschreiben 2018/3 Outsourcing[7] beschreibt die Eidgenössische Finanzmarktaufsicht (FINMA) die Pflichten eines Unternehmens, das Leistungen auslagert. Dieses Rundschreiben kann als Orientierungshilfe dienen. Neben bankenspezifischen Vorgaben enthält das Rundschreiben übliche Geschäftspraktiken, die insbesondere auch für das Outsourcing von IKT-Leistungen gelten. Die Parlamentsdienste erfüllen die Mehrheit dieser Anforderungen für das Outsourcing der Liferay-Umgebung (Abbildung 3, «IT Parlament») nicht, darunter:

- Wirtschaftlichkeit, Nutzen, Chancen und Risiken des Outsourcings sind nicht nachvollziehbar dokumentiert.
- In den Verträgen mit clavis IT fehlen wichtige Vertragsbestandteile oder sind unvollständig. Beispielsweise die Festlegung der gegenseitigen Zuständigkeiten und Schnittstellen, die Betriebsanforderungen oder die Weiterverpflichtung der Unterakkordanten.
- Vorkehrungen für eine allfällige Rück- oder Überführung des Betriebs fehlen weitgehend.

Beurteilung

Die Parlamentsdienste haben bereits wichtige Teile ihrer Informatik ausgelagert ohne nachvollziehbare Kosten, Nutzen- und Wirtschaftlichkeitsüberlegungen. Es ist eine komplexe Betriebs- und Sourcing-Situation entstanden, die nicht zentral und strategisch geführt wird. Ungeklärte Verantwortlichkeiten und Betriebsprobleme sind die Folge (vgl. Kapitel 3.1 Inbetriebnahme trotz fehlender Grundlagen und 4.3 Betrieb und Entwicklung ungenügend geregelt). Insbesondere an den Schnittstellen bestehen ungeklärte Zuständigkeiten.

Trotz der zunehmenden Abhängigkeit von externer Unterstützung fehlt eine Sourcing-Strategie und ein Providermanagement, das die Wahl geeigneter Partner, die nachvollziehbare Beauftragung und Überwachung der Dienstleister sowie nötigenfalls den Providerwechsel bzw. die Rückführung von ausgelagerten Leistungen sicherstellt.

Problematisch ist insbesondere, dass Betriebs- und Supportleistungen der Lieferanten nicht formell geregelt und überprüfbar sind. Ausserdem werden Vertragsverpflichtungen sowie das Weisungs- und Kontrollrecht nicht auf die Unterakkordanten der Anbieter ausgeweitet.

Die vertragliche, organisatorische und technische Betriebsinfrastruktur erfüllt nach Einschätzung der EFK die Anforderungen nicht, um darauf die geschäftskritischen Anwendungen des Schweizer Parlaments zu betreiben.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 4.

5.3 IT-Risikomanagement der Parlamentsdienste unvollständig

Das Risikomanagement ist zusammen mit dem internen Kontrollsystem der Parlamentsdienste in einer Richtlinie aus dem Jahre 2014 geregelt. Als Geltungsbereich werden die Parlamentsdienste und die Bundesversammlung genannt. Unter «Risiko» versteht die

[7] FINMA Rundschreiben 2018/3 Outsourcing, letzte Änderung 4. November 2020

Richtlinie Ereignisse, die sich negativ auf die Zielerreichung oder Aufgabenerfüllung der Parlamentsdienste auswirken. Negative Auswirkungen auf die Zielerreichung und Aufgabenerfüllung des Parlamentes sind in der Risikodefinition nicht aufgeführt.

Mindestens einmal jährlich wird für die Geschäftsleitung der Parlamentsdienste ein Risikoreporting erstellt. Ein summarisches Reporting der Risiken an die Verwaltungsdelegation erfolgt jeweils im Rahmen des Jahresberichtes Infrastruktur. Risikoeigner sind immer die Bereichs- und Ressortleiter der Parlamentsdienste.

Im Auszug aus dem Risikokataster per Frühling 2021 fallen Massnahmen auf, deren Umsetzung als «nicht dokumentiert bzw. eingeführt» oder «ungenügend dokumentiert bzw. eingeführt» rapportiert werden. Dies sind betreffend Informatik beispielsweise:

- Auswertung/Überwachung der Protokolldateien (M00243)
- Einführung eines Intrusion-Detection und -Prevention Systems (M00285)
- Vergabe von Zugriffsrechten (M00134)
- Bereitstellung Test Infrastruktur (M00157)
- Business Continuity Management einführen (M00066).

Zu den Risiken und Massnahmen wird ein Umsetzungsstand und die verantwortliche Person rapportiert. Pro Massnahme wird ausserdem ein Fälligkeitsdatum angegeben, das aber gemäss Parlamentsdiensten bis zur Migration in ein neues Tool im März 2021 nicht bewirtschaftet wurde.

Beurteilung

Die Regelung des Risikomanagementprozesses in einer Richtlinie und die Erstellung eines periodisch aktualisierten Risikokatasters sind für eine Organisation dieser Grösse gut. Diese Grundlage wird im Bereich der Informationssicherheit aber nicht konsequent umgesetzt.

Risiken (und Massnahmen) der Liferay-basierten Plattform für das Parlament werden im Risikomanagement nicht nachvollziehbar gesteuert. Betroffene Risiken und Massnahmen müssten doppelt und pro Plattform geführt werden. Wenn beispielsweise das Server Hardening für die bestehende Microsoft-Plattform als vollständig dokumentiert und eingeführt rapportiert wird (M00245), gilt das nicht für die Liferay-Plattform (siehe Kapitel 3.3 Sicherheitsmängel werden nicht zeitnah behoben). Diese wesentliche Information wird im aktuellen Risikoregister nicht wiedergegeben.

Dass auch elementare Massnahmen wie Intrusion Detection/Prevention, Business-Impact-Analyse oder Changemanagement nicht umgesetzt sind, verstösst gegen übliche Geschäftspraxis und erhöht die Risiko-Exposition für die Informatiksysteme erheblich.

Weitere Massnahmen werden im Risikobericht als nicht oder unvollständig umgesetzt rapportiert. Die Beurteilung der Massnahmenumsetzung wird dadurch erschwert, dass das Entscheiddatum für eine Massnahme und das Fälligkeitsdatum zur Umsetzung bisher nicht bewirtschaftet wurde. Das Ausmass von Verzögerungen bei der Umsetzung von Massnahmen kann so nicht im vollen Umfang nachvollzogen werden.

6 Die Architektur wird nicht gesteuert

Die Unternehmensarchitektur der Parlamentsdienste bestimmt auf Jahre hinaus die Gestaltung der Digitalisierung des Parlaments. Architekturfehler können Prozesse verkomplizieren, wiederkehrend hohe Kosten verursachen, den künftigen Gestaltungsspielraum einschränken und schlimmstenfalls zu Projektabbrüchen führen.

6.1 Architekturzuständigkeiten sind unklar

Die Parlamentsdienste beschäftigen einen Unternehmens- und einen Technologie-Architekten. Ein Architekturboard behandelt Architekturthemen und fällt Architekturentscheidungen. Leiter ist der Unternehmensarchitekt. Im Rahmen der beiden Projekte wurden die Architekten kaum einbezogen.

Von HERMES vorgesehene Quality-Gates, in denen die Architekten die Systemarchitekturen der Projekte zu beurteilen hätten, sind nur teilweise eingeführt.

Im Entwurf der «Eckwerte einer Zweisparten-Strategie» ist für die Zukunft folgende Aufteilung der Architektur-Verantwortlichkeiten angedacht:

Zuständigkeitsbereich	Verantwortlicher
Geschäftsarchitektur	Unternehmensarchitekt
Informations- und Datenarchitektur	offen
Anwendungsarchitektur	je nach Anwendung externe Lösungsarchitekten
Technologie-Architektur / IKT-Architektur	IKT-Architekt
Sicherheitsarchitektur	Informationsschutzbeauftragter (ISBD)
übergreifende Architekturverantwortung	nicht vorgesehen

Abbildung 4: Architekturverantwortung gemäss «Eckwerte einer Zweisparten-Strategie für die Informatikdienstleistungen» vom 24.3.2021

De facto prägen die Projekte die IT-Architektur der Parlamentsdienste «bottom-up»:

1. Cervin entschied sich für das Produkt Liferay.
2. Der Projektleiter CURIAplus hat zur Erfüllung seines Jahresziels, einen Verbesserungsvorschlag zu machen, anfangs 2019 eine Soll-IT-Architektur entwickelt. Gemäss dieser soll das gesamte Parlamentsgeschäft künftig mit dem bereits mit Cervin beschafften Liferay und bei Bedarf weiteren Open-Source-Produkten gebaut werden. Diese Soll-Architektur wurde nicht weiter kommuniziert, durchlief keinen Qualitätssicherungsprozess und wurde von der Geschäftsleitung nicht verabschiedet, aber schrittweise realisiert.
3. Die Ausschreibung CURIAplus erfolgte basierend auf Liferay.
4. Initialisiert durch den Projektleiter CURIAplus hat Cervin ein Konzept «Portal Integrator – Lieferantenzugang» in Auftrag gegeben, das bereits umgesetzt wird. Gemäss diesem beabsichtigen die Parlamentsdienste, «basierend auf Liferay DXP den Aufbau eines

ganzen Ökosystems an Applikationen und Self-Services für die User. Bestehende Anwendungen sollen sukzessive abgelöst werden. [...] Damit stellt sich die Herausforderung, dass mehrere Lieferanten unterschiedliche Teile des Parlnets entwickeln und diese Zusammenarbeit und das Zusammenführen der Applikationen möglichst reibungslos laufen muss.»

Erst im April 2020, kurz vor dem Zuschlag für die CURIAplus-Ausschreibung, haben sich die Parlamentsdienste mit den Chancen und Risiken des strategischen Architekturentscheids auseinandergesetzt. Auslöser war der damals neu angestellte Ressortleiter «Informatik & neue Technologien». Er erhielt von der Auftraggeberin CURIAplus und deren Stellvertreter (beides GL-Mitglieder) den Auftrag für eine Risikoanalyse des Liferay-Einsatzes für CURIAplus. Der Ressortleiter veranlasste intern eine Risikoanalyse des Liferay-Einsatzes aus Sicht IT-Betrieb und eine detaillierte Gegenüberstellung der Vor- und Nachteile, Chancen und Risiken (inkl. Wirtschaftlichkeitsbetrachtung) von Liferay und Sharepoint. Ergänzend dazu gab er eine externe Studie zur Beurteilung der Chancen und Risiken des Liferay-Einsatzes für CURIAplus in Auftrag. Diese kam zum Schluss, dass den Parlamentsdiensten eine klare IT-Strategie und eine verbindliche Unternehmensarchitektur fehlen, was zu «Wildwuchs» führen könne. Generell hält die Studie fest, dass unabhängig vom weiteren Verlauf alle Entscheidungen (egal ob für oder gegen Liferay) einen negativen Einfluss haben würden. Dies weil die Reihenfolge der Entscheide vom Ablauf her nicht optimal sei und der Plattform-Entscheid strategische Bedeutung habe. Auf die strategische Bedeutung hat auch der Projektleiter CURIAplus in seiner informellen Soll-Architektur hingewiesen.

Die Studie stellt ausserdem fest, dass die erhöhte technische Komplexität der Zwei-Sparten-Landschaft zu höheren Kosten und komplexeren Betriebsprozessen führt und die Sicherheit des Gesamtsystems senkt. Die daraus entstehenden Folgekosten sollten mindestens ansatzweise in die Gesamtüberlegung einfliessen. Ebenso weist sie daraufhin, dass wiederholt Vorhaben der öffentlichen Hand zur Einführung von Open-Source-Plattformen gescheitert sind, insbesondere wegen mangelnde Kompatibilität und Integrationsfähigkeit dieser Plattformen.

Der Projektleiter CURIAplus hält dagegen: Es wäre ein Fehler für eine Firma, die höhere Ansprüche an Offenheit und Flexibilität ihrer Anwendungsinfrastruktur stellt, nicht mit Liferay fortzufahren. Die Microsoft-Office-Integration würde immer weniger wichtig, weil Word und Excel immer weniger verwendet werden sollten und würden. Auch weist er auf die mit einem Wechsel verbundenen Mehrkosten, Verzögerungen und Image-Schäden für die Parlamentsdienste hin. Die Innovation würde gebremst, und man vergäbe sich die Chance, intern Know-how im Java/Open-Source-Umfeld aufzubauen. Letztlich würde auch der Benutzerkomfort leiden.

Aus Sicht der Auftraggeberin CURIAplus ergaben die Ergebnisse der Analysen keinen Anlass, die bereits laufende Ausschreibung abzubrechen.

Beurteilung

Gemessen an der Organisationsgrösse sind die Parlamentsdienste im Bereich IT-Architektur personell adäquat ausgestattet. Die Architekten sind allerdings kaum in die geprüften Projekte eingebunden und können die Architektur nur begrenzt mitgestalten. Damit bleibt ihre Arbeit nahezu wirkungslos.

Die angedachte Aufgabenteilung zwischen den unterschiedlichen Architekturrollen ist zu überdenken:

- Verschiedenen Teilarchitekturen müssen in ihrem Zusammenspiel die Geschäftsanforderungen abdecken und geeignet sein, um die Geschäftsstrategie umzusetzen. Es gibt niemanden, der die Gesamtverantwortung dafür wahrnimmt und über die zur Durchsetzung notwendigen Kompetenzen verfügt.
- Die Verantwortung für die Anwendungsarchitektur können und dürfen die Parlamentsdienste nicht an externe Firmen übertragen, insbesondere nicht an die Auftragnehmer für die Entwicklung von Anwendungen. Sie ist Teil der Anforderungsdefinition und dient als Grundlage für die Projektdefinition und die Auftragsvergabe an Lieferanten.
- Die Verantwortung für die Sicherheitsarchitektur darf nicht dem ISBD aufgebürdet werden. Seine Aufgabe ist es, diese unabhängig zu prüfen (segregation of duty).

Die Projekte haben Fakten geschaffen, die nachträglich nur schwer zu korrigieren sind. Wichtige Architekturentscheide müssen aus Unternehmenssicht gefällt werden, bevor Projekte Präjudizien schaffen. Sie haben sich an der Geschäftsstrategie zu orientieren und Sicherheit, Betreibbarkeit, Zukunftsfähigkeit und Anpassbarkeit umfassend zu gewährleisten. Diese Anforderungen können nicht oder nur mit hohen Kosten und Aufwänden nachträglich «hineingebaut» werden.

Strategische Architekturentscheide zu fällen, liegt in der Verantwortung der Geschäftsleitung. Ihre Entscheide müssen dabei auf Unterlagen basieren, die mögliche Handlungsalternativen, deren Konsequenzen, Vor- und Nachteile, Chancen und Risiken transparent aufzeigen.

6.2 Informelle Soll-Architektur problematisch

Es existiert keine ausgearbeitete, formell abgenommene Soll-Architektur, die beschreibt, wie der Digitalisierungsauftrag des Parlaments umgesetzt werden soll. Aus den vorhandenen Unterlagen kann folgende Architekturvision abgeleitet werden:

- Die Gesamtheit der parlamentarischen Geschäfte soll künftig weitgehend unverändert papierlos und IT-unterstützt abgewickelt werden. Allen Beteiligten wird dafür eine zentrale Plattform bereitgestellt. Sie müssen sich darauf nur einmal anmelden und erhalten auf alle Funktionen und Daten Zugriff, die sie benötigen und sehen dürfen. Die Plattform ist webbasiert, sodass sie nach Bedarf ortsunabhängig und jederzeit zur Nutzung bereitsteht. Sie bietet den Teilnehmern Zugang zu Informationen, Prozessunterstützung und Kollaborationsfunktionen. Unklar ist, ob künftig auch die Dokumentenverwaltung und E-Mails integriert werden sollen.
- Die Plattform basiert im Wesentlichen auf Liferay DXP. Soweit möglich werden alle Prozesse und Funktionalitäten darauf implementiert. Für in Liferay fehlende Funktionalitäten werden weitere Open-Source-Produkte beigezogen. Lediglich für Parlamentsdienst-interne Zwecke werden andere, mehrheitlich Microsoft-basierte Produkte eingesetzt.
- Nach und nach sollen alle parlamentsbezogenen Anwendungen auf Liferay migriert werden. Erwähnt werden unter anderem die elektronischen Abstimmsysteme des Stände- und Nationalrats (ELAS und ELAN) wie auch das Protokolliersystem VERBALIX.
- Eine zentrale Anforderung an die IKT-Unterstützung des Parlaments sind Innovation und Agilität. Der EFK liegen keine Unterlagen vor, die dokumentieren, wie die gewählte Architektur diese unterstützen soll.

- Wie clavis IT in einem Papier zuhanden der Parlamentsdienste illustriert, existieren unterschiedliche Optionen, wie eng Funktionalitäten in ein Portal eingebunden werden können. Manche der Optionen sind unabhängig von der gewählten Plattform (Liferay, Sharepoint etc.). Gemäss den zur Verfügung stehenden Dokumenten haben sich die Parlamentsdienste für eine Vollintegration entschieden, auch wenn der Entscheid nicht explizit dokumentiert ist.

In den Unterlagen gab es keine Hinweise darauf, wie die Liferay-Welt mit den auf Microsoft-Produkten basierenden Umgebungen und Prozessen zusammenarbeiten soll, beispielsweise mit der für die Parlamentarier neu beschafften Collaboration Plattform Teams. Ebenso ist aus den Unterlagen nicht ersichtlich, wie die Sicherheitsanforderungen gemäss Digitalisierungsauftrag der Verwaltungsdelegation konkretisiert und umgesetzt werden sollen. Anbieter wie T-Systems, IBM und BIT haben aus verschiedenen Gründen den Einsatz von Liferay aufgegeben und die Anzahl von erfahrenen Anbietern für Liferay ist klein.

Das Forschungs- und Analystenunternehmen Gartner hat auf die Probleme monolithischer Digital Experience Plattformen (DXP) hingewiesen.[8] Gemäss ihrer Beurteilung hätten Unternehmen, die sie im Einsatz haben, Schwierigkeiten, rasch genug neue Lösungen zu realisieren. Ausserdem würden technische Altlasten und Anbieter-Abhängigkeit ihre Innovationskraft behindern. Um aufwendige und teure Releasewechsel von monolithischen Anwendungen und Produkt-Lock-In zu vermeiden, zerlegen agile Organisationen ihre Anforderungen so, dass sie durch kleine, einfache Anwendungen (Gartner: Packaged Business Capabilities oder PBCs) realisierbar sind. Diese können unabhängig voneinander rasch entwickelt, getestet und durch neue ersetzt werden.

Beurteilung

Die wenigen vorliegenden Architekturunterlagen erlauben keine abschliessende Beurteilung der gewählten Architektur. Die EFK hat aber Zweifel, ob die nötige Digitale Transformation, die geforderte Innovation und Flexibilität wie auch die notwendige Sicherheit damit realisierbar sind. Die informelle Zielarchitektur weist kritische Lücken und Mängel auf:

- Das Zusammenspiel der um Liferay herum aufzubauenden Open-Source-Plattform mit der bestehenden, primär Microsoft-basierten Informatiklandschaft ist ungeklärt.
- Ebenfalls fraglich ist, ob damit die Sicherheitsanforderungen abdeckbar sind.
- Der Einsatz von Liferay und Open Source ist kein Garant für Innovation und Flexibilität. Mit geeigneten architektonischen Gegenmassnahmen muss verhindert werden, dass sich die gewählte Architektur als Kostenfalle, Innovationshemmnis und Agilitätsblockade erweist. Open Source ist kein Garant für Lieferantenunabhängigkeit. Je mehr Funktionen in Liferay hineingebaut werden, um so unrealistischer wird ein Produktwechsel. Die Abhängigkeit von Liferay wäre folgenschwerer als eine von Microsoft, da der verfügbare Expertenpool dafür wesentlich kleiner ist, wie die Abkehr vom Produkt von drei grossen, ehemaligen Liferay-Providern aufzeigt.

Empfehlung

Siehe Kapitel 7 Schlussfolgerungen und Empfehlungen, Empfehlung 4.

[8] «Adopt a Composable DXP Strategy to Future-Proof Your Tech Stack», Published 16th December 2020, By Irina Guseva u. a.

7 Schlussfolgerungen und Empfehlungen

7.1 Erforderliche Sofortmassnahmen zur Schadensminimierung

Umfassende Sicherheitsprüfung sowie Schliessung von Sicherheitslücken bei Cervin

Die seit 2019 im Betrieb befindliche Plattform Cervin weist gemäss mehreren Sicherheitsüberprüfungen wesentliche Schwachstellen auf. Diese waren grösstenteils zum Prüfzeitpunkt noch nicht geschlossen. Ausserdem fehlt für eine umfassende Beurteilung der Sicherheit die Überprüfung von weiteren Komponenten (vgl. Bericht «Security Audit Parlnet», Kap. 3.3). Ohne Schliessung der wesentlichen Schwachstellen sowie ergänzenden Sicherheitsüberprüfungen ist eine Weiterbetrieb mit Risiken verbunden.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, rasch eine umfassende Sicherheitsprüfung von Cervin und direkt damit verbundenen Komponenten wie auch einen Code-Review der sicherheitsrelevanten Eigenentwicklungen in Liferay durchzuführen. Die Ergebnisse müssen in der zu erarbeitenden Soll-Architektur berücksichtigt werden.

⇨ Für Details siehe Kapitel 3.3

Stellungnahme der Parlamentsdienste

Die Empfehlung ist angenommen.

Die Parlamentsdienste liessen das Projekt Cervin im Juni und November 2020 durch eine auf solche Audits spezialisierte Firma auf Sicherheitsmängel prüfen. Die Prüfungsergebnisse (Findings) wurden aufgrund ihrer Schwere priorisiert und werden bis Ende März 2022 abgearbeitet. Zudem ist eine Architekturbereinigung im Gang, die ebenfalls Ende März 2022 abgeschlossen sein wird. Die Prüfung der EFK ergab keine neuen Sicherheitsmängel. Zudem nahmen die Parlamentsdienste im Mai 2021 am Bug-Bounty-Programm des NCSC teil. Dieses ergab für Cervin ein Finding der niedrigsten Stufe («low»), das umgehend behoben wurde. Im April 2022 ist eine erneute Sicherheitsprüfung durch dieselbe Firma vorgesehen, welche bereits 2020 die Prüfungen durchgeführt hat.

Damit wird die Empfehlung 1 der EFK weitgehend umgesetzt, noch umfassendere Sicherheitsprüfungen erachten die Parlamentsdienste zum jetzigen Zeitpunkt als unverhältnismässig.

Entscheiden, ob CURIAplus vorläufig gestoppt werden soll

Aktuell ist mit Cervin eine Plattform in Produktion, die wesentliche betriebliche und sicherheitsbezogene Mängel aufweist. Sie ist noch nicht fertig entwickelt. CURIAplus basiert darauf und ist daher von den Mängeln ebenfalls betroffen.

CURIAplus hängt nicht nur von Cervin ab, sondern auch von weiteren Projekten der Parlamentsdienste, von denen einige bereits Verzögerungen gemeldet haben. Ausserdem sind in der Realisierungsphase projektinterne Verzögerungen aufgetreten.

Es fehlen eine übergeordnete IKT-Strategie und eine wirksame IKT-Governance. Allfällige Anpassungen der IKT-Strategie, der IKT-Governance und der Gesamtarchitektur der Parlamentsdienste führen potenziell zu grösseren Anpassungen in beiden strategischen Projekten Cervin und CURIAplus. Damit können erhebliche Kosten und Verzögerungen entstehen. Sollte sich beispielsweise herausstellen, dass mit der gewählten Open–Source-Plattform im Zusammenspiel mit den Microsoftprodukten, die erforderliche Sicherheit nicht realisierbar ist, müssten beide Projekte neu aufgesetzt werden.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, basierend auf einer fundierten Analyse, zu entscheiden, ob CURIAplus weitergeführt oder sistiert werden soll. Neben Realisierungs- und Einführungsrisiken muss auch eine mögliche Fehlentwicklung wegen nicht vorhandener Grundlagen (IKT-Strategie, IKT-Governance, Soll-Architekturen, Betriebs- und Sourcing-Konzept etc.) berücksichtigt werden.

⇨ Für Details siehe Kapitel 4.6

Stellungnahme der Parlamentsdienste

Die Empfehlung ist abgelehnt.

Die Parlamentsdienste sehen keinen Anlass, die Frage der Weiterführung des Projekts CURIAplus vertieft zu prüfen. Die Realisierung wird gemäss schriftlicher Bestätigung des Lieferanten mit Datum vom 11. November 2021 termingerecht und zu den vereinbarten Kosten umgesetzt. Nennenswerte Einführungsrisiken sind zurzeit nicht ersichtlich. Soweit damit Sicherheitsrisiken gemeint wären, sind diese Gegenstand des Projekts Cervin, da die Anwendung CURIAplus auf derselben Plattform aufsetzt. Die entsprechenden Findings werden bis März 2022 abgearbeitet, während die neue Anwendung CURIAplus erst rund ein Jahr später eingeführt wird (siehe Stellungnahme zu Empfehlung 1). Die Arbeiten an der IT-Strategie, der IKT-Gouvernanz und der Architektur sind im vollen Gang (siehe generelle Stellungnahme der Parlamentsdienste) und berücksichtigen bereits die Ausrichtung des Projekts CURIAplus. Die laufenden Arbeiten haben die Richtigkeit und Machbarkeit des eingeschlagenen Wegs bestätigt.

Die Parlamentsdienste haben aufgrund dieser Überlegungen entschieden, das Projekt CURIAplus weiterzuführen.

Unabhängiges Qualitäts- und Risikomanagement angeordnet, aber nicht umgesetzt

Das von der Geschäftsleitung beschlossene, unabhängige Qualitäts- und Risikomanagement ermöglicht eine zweite, unabhängige Beurteilung von Projekten. Es ist ein wichtiges Führungsinstrument, die benötigten Konzepte wurden bereits Anfangs 2021 erarbeitet.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, das unabhängige Qualitäts- und Risikomanagement für alle IKT-Grossprojekte wie beispielsweise CURIAplus spätestens bis Ende 2021 operativ umzusetzen.

⇨ Für Details siehe Kapitel 4.4

Stellungnahme der Parlamentsdienste

Die Empfehlung ist angenommen.

Die Parlamentsdienste sehen sich durch die EFK in ihrer Vorgehensweise bestätigt und werden die bereits vor der Prüfung begonnenen Arbeiten an einem unabhängigen Qualitäts- und Riskmanagement wie geplant weiterführen. Eine operative Umsetzung bis Ende 2021 erachten sie aber nicht als sinnvoll und auch nicht möglich. Das dafür notwendige Konzept wurde von der Geschäftsleitung noch nicht abgenommen. Sie hat den Auftrag erteilt, dieses mit den Arbeiten an der digitalen Transformation abzustimmen. Damit wird die Empfehlung der EFK weitgehend umgesetzt. Einzig die von der EFK explizit geforderte Umsetzung für das Projekt CURIAplus ist nicht zielführend, da dieses mittlerweile so weit fortgeschritten ist, dass der Nutzen gegenüber den zusätzlich entstehenden Kosten nicht gegeben ist.

7.2 Erstellung einer IKT-Strategie, -Governance und -Architektur

Zum Zeitpunkt des Starts der Projekte Cervin und CURIAplus existierten bei den Parlamentsdiensten weder eine angemessene IKT-Strategie und IKT-Governance noch verbindliche Architekturvorgaben. Die Projekte haben deshalb Entscheide von strategischer Bedeutung gefällt. Dabei wurde weder die Gesamtsituation angemessen abgewogen noch wurden die Entscheide auf einer adäquaten Hierarchiestufe gefällt.

Der Entscheid für ein Open–Source- und eine Microsoft-Plattform wurde inzwischen gefällt, bezüglich Schnittstellen und Abhängigkeiten sind aber viele Fragen noch nicht geklärt. Mit diesem Vorgehen werden Projekte vorangetrieben, obschon die Rahmenbedingungen, die das Fundament bilden, nicht feststehen.

Betreffend IKT-Governance stellt die EFK fest, dass diese noch nicht alle relevanten Rollen angemessen einbindet. Ein Providermanagement gemäss üblicher Geschäftspraxis fehlt. Die Aufgabenteilung zwischen den beteiligten Betriebsorganisationen wie auch die Verantwortung für den Gesamtbetrieb sind noch nicht abschliessend geklärt. Insbesondere fehlen wirksame Massnahmen, welche die Einhaltung von Weisungen und Richtlinien sicherstellen.

Mit dem neuen Informationsschutzgesetz erhalten die Verwaltungsdelegation und die Parlamentsdienste neue Aufgaben. Sie müssen unter anderem Ausführungsbestimmungen dazu erlassen und die Umsetzung überwachen. Zu dieser Überwachung gehört auch die formelle Risikoakzeptanz und die Massnahmenüberwachung. Aufgaben können wohl delegiert werden, nicht jedoch die Verantwortung.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, eine IKT-Strategie und darauf abgestimmt eine IKT-Governance, eine Soll-Architektur, Sourcing- und Betriebskonzepte sowie ein Providermanagement rasch zu erarbeiten und einzuführen. Diese müssen auf fundierten, dokumentierten Grundlagen beruhen und üblicher Geschäftspraxis entsprechen. Die nachvollziehbare Durchsetzung der Vorgaben muss durch geeignete Massnahmen sichergestellt werden.

⇨ Für Details siehe Kapitel 3.2, 4.5, 5.1, 5.2 und 6.2

Stellungnahme der Parlamentsdienste

Die Empfehlung ist angenommen.

Die Parlamentsdienste sehen sich durch die EFK bestätigt und werden ihre bereits vor der Prüfung durch die EFK gestarteten diesbezüglichen Aktivitäten im Rahmen der digitalen

Transformation wie geplant weiterführen. Aufgrund der Empfehlungen der beigezogenen externen Berater wird die Bereitstellung einer neuen Organisationsstruktur prioritär verfolgt; die Konkretisierung der bereits formulierten strategischen Ziele im Bereich der digitalen Transformation und der nach der Reorganisation noch verbleibenden Gouvernanzfragen sowie der übrigen in der Empfehlung genannten Konzepte erfolgt anschliessend, sollte aber vor Ende 2022 abgeschlossen werden können. Damit wird die Empfehlung der EFK vollumfänglich umgesetzt.

7.3 Aufarbeiten der Grundlagen in den Projekten

Sowohl bei Cervin als auch bei CURIAplus fehlen die auf Projektebene abgenommenen Grundlagen. Sofern die Projekte weiterlaufen, sind diese gemäss Vorgaben fertigzustellen und qualitätsgesichert abzunehmen. Sobald die übergeordneten Grundlagen (vgl. Empfehlung Nr. 1, 2 und 4) vorliegen, müssen die Konzepte in den Projekten überarbeitet und erneut abgenommen werden.

Projekt Cervin

Empfehlung 5 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, die fehlenden Lieferergebnisse für Cervin rasch zu erstellen. Dies betrifft insbesondere die Infrastruktur für umfassende Tests, einen überarbeiteten Rahmenvertrag, Betriebs- und Wartungsverträge (inkl. SLA), fehlende Konzepte, die Prüfung der Sicherheitsanforderungen sowie vollständige Tests und formelle Abnahme. Sobald die übergeordneten Grundlagen vorliegen, müssen die Lieferergebnisse überprüft und bei Bedarf angepasst werden.

⇨ Für Details siehe Kapitel 3.1 und 3.2

Stellungnahme der Parlamentsdienste

Die Empfehlung ist angenommen.

Die in den Ausschreibungsunterlagen geforderten und noch nicht erbrachten Lieferergebnisse wurden aufgrund der im Prüfungs-Report vom Juni und November 2020 gemeldeten «fehlenden Konzepte» in die Projektplanung aufgenommen und werden per Ende März 2022 fertiggestellt sein. Die insbesondere für CURIAplus notwendig gewordene Parlnet-Testplattform steht seit August 2021 zur Verfügung. Nach der Architekturbereinigung per Ende März 2022 wird Parlnet (die im Projekt Cervin realisierte Anwendung, welche auf derselben Portalplattform aufsetzt wie CURIAplus) auch über Test-User-Accounts sowie Testdaten verfügen. Eine weitere Sicherheitsprüfung ist für April 2022 vorgesehen. Sämtliche Testfälle sind bereits seit 2020 in einem eigenen Test-Management-Tool (Zephyr) dokumentiert und werden mit jedem Release ausgebaut.

Die formelle Abnahme des Projekts erfolgt, wenn in der für April 2022 geplanten Sicherheitsprüfung keine gravierenden, hoch oder mittel eingestuften Risiken bzw. Mängel festgestellt werden. Die Parlamentsdienste gehen davon aus, dass damit die Empfehlung 5 im Mai 2022 erledigt sein wird.

Projekt CURIAplus

Empfehlung 6 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, für CURIAplus umgehend mit Unterstützung eines Sicherheitsexperten eine vollständige Gefahren- und Risikoanalyse vorzunehmen. Anschliessend sind die fehlenden Lieferergebnisse rasch fertigzustellen (Infrastruktur für umfassende Tests, Betriebskonzepte und ISDS-Konzept und deren Umsetzung). Sobald die übergeordneten Grundlagen vorliegen, müssen die Lieferergebnisse überprüft und bei Bedarf angepasst werden. Die Arbeiten sind in interdisziplinären Teams voranzutreiben.

⇨ Für Details siehe Kapitel 4.2 und 4.3

Stellungnahme der Parlamentsdienste

Die Empfehlung ist angenommen.

Wir erachten es nicht als sinnvoll, erneut eine vollständige Gefahren- und Risikoanalyse durchzuführen. Zum einen wurde die Portalplattform im Rahmen des Projekts Cervin gründlich geprüft und verbesserungswürdige Punkte sind in der Umsetzung. CURIAplus wird weitere sicherheitstechnische Überprüfungen dann vornehmen, wenn die Schnittstellenanbindungen zu den benützten Anwendungen erfolgt sind, da vorher kein Datenaustausch möglich ist.

Die beiden Konzepte ISDS-Konzept und Betriebskonzept werden laufend aktualisiert. Beide verweisen jedoch über weite Teile auf die gleichnamigen Konzepte der Portalplattform, auf der sowohl Parlnet als auch CURIAplus aufsetzen. Das ISDS-Konzept wird Ende Dezember aktualisiert und abnahmebereit sein. Das bereinigte Betriebskonzept wird spätestens Ende Februar 2022 vorliegen.

Die erste Testumgebung für den Lieferanten steht auf der Portalplattform bereits zur Verfügung. Die Testumgebung und die Integrationsumgebung der Portalplattform benötigt CURIAplus gemäss Planung erst ab März 2022. Die Integrationsumgebung ist seit langem vollständig in Betrieb und die Testumgebung im Rahmen spezifisch für CURIAplus ist im Aufbau.

Damit wird die Empfehlung der EFK weitgehend umgesetzt, eine noch weitergehende Gefahren- und Risikoanalyse des Projekts CURIAplus erachten die Parlamentsdienste aus den aufgeführten Gründen als nicht notwendig.

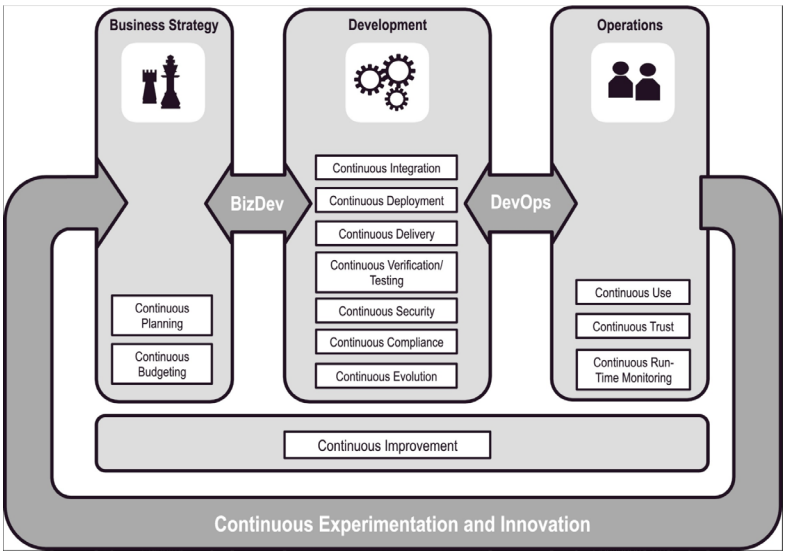
Anhang 1: Rechtsgrundlagen und parlamentarische Vorstösse

Rechtstexte
Bundesgesetz über die Bundesversammlung (Parlamentsgesetz, ParlG) vom 13. Dezember 2002 (Stand am 2. Dezember 2019), SR171.10
Verordnung der Bundesversammlung zum Parlamentsgesetz und über die Parlamentsverwaltung (Parlamentsverwaltungsverordnung, ParlVV) vom 3. Oktober 2003 (Stand am 2. Dezember 2019), SR 171.115
Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020, noch nicht in Kraft gesetzt
Parlamentarische Vorstösse
20.4260 – Zukunftsfähige Daten-Infrastruktur und Daten-Governance in der Bundesverwaltung. Motion eingereicht von der Finanzkommission des Nationalrates, 6.10.2020 Der Bundesrat beantragte am 25.11.2020 die Annahme der Motion. Von beiden Räten angenommen am 17.12.2020 und 8.3.2021.
18.3301 – Aufsicht über die Parlamentsdienste. Interpellation eingereicht von Gerhard Pfister, Nationalrat, 15.3.2018 Am 19.6.2020 abgeschrieben, weil nicht innert zwei Jahren abschliessend im Parlament behandelt.
17.4026 – Digitaler Ratsbetrieb bis 2020. Motion eingereicht von Sebastian Frehner, Nationalrat, 7.12.2017 Von beiden Räten im Jahr 2018 angenommen, damit Auftragserteilung an die Verwaltungsdelegation.
17.3640 – Papierloser Ratsbetrieb. Interpellation eingereicht von Sebastian Frehner, Nationalrat, 11.9.2017 Am 10.11.2017 vom Büro des Nationalrates beantwortet und am 15.12.2017 vom Nationalrat als erledigt eingestuft.
13.3493 – Vorwärts mit dem digitalen Parlament. Motion eingereicht von Thomas Aeschi, Nationalrat, 19.6.2013 Am 12.9.2013 vom Büro des Nationalrates beantwortet und Antrag auf Ablehnung. Am 26.9.2013 im Nationalrat angenommen, am 12.12.2013 im Ständerat abgelehnt.

Anhang 2: Abkürzungen

APPF	Ausschuss zur Vorbereitung des mittelfristigen Projektportfolios
ABE	Ausschuss zur IKT-Bedarfsevaluation
BinfV	Bundesinformatikverordnung
EFK	Eidgenössische Finanzkontrolle
ISB	Informatiksteuerungsorgan des Bundes
ISDS	Informationssicherheits- und Datenschutz
ISG	Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz)
QRM	Qualitäts- und Risikomanager oder Qualitäts- und Risikomanagement
Schuban	Schutzbedarfsanalyse
SLA	Service Level Agreement
VDTI	Verordnung über die digitale Transformation und die Informatik

Anhang 3: Glossar

BizDevOps	Bei BizDevOps übernimmt ein integriertes, cross-funktionales sich selbst organisierendes Team aus kompetenten Geschäftsvertretern, Softwareentwicklern und Betriebsvertretern die Verantwortung für eine fachliches Produkt bzw. einen Service. Die Unternehmensstrategie wird gleichermassen berücksichtigt wie die IT-Strategie und Technologie-Trends.  (Quelle Text: Dr. Christoph Schulz, www.palladio-consulting.de; Quelle Grafik: The Journal of Systems and Software April 2015, Brian Fitzgerald und Klaas-Jan Stol, Seite 181)
Cervin (Projekt)	Informatikprojekt «Digitale Arbeitsplattform für die Bundesversammlung» der Parlamentsdienste zur Ablösung von Intranet/Extranet der Parlamentsdienste. Dies ist lediglich ein erster Schritt. Schlussendlich sollen viel weitergehende Anforderungen erfüllt werden: «Eine zentrale, digitale Arbeitsplattform, die alle geschäfts- und supportrelevanten Prozesse sowie die dafür benötigten Funktionen, orts- und geräteunabhängig, auf einer webbasierten Plattform abbilden bzw. zur Verfügung stellen kann. Das dynamische Aggregieren von Inhalten unterschiedlicher Quellsysteme garantiert jederzeit einen umfassenden und aktuellen Informationsstand.»[9]
Cervin/Parlnet (Anwendung)	Die vom Projekt Cervin implementierte Anwendung heisst Parlnet. Aktuell werden vom Projekt weitere Komponenten erstellt.

[9] «Pflichtenheft zum Projekt (18208) 101 «Cervin» – Digitale Arbeitsplattform für die Bundesversammlung», Seite 8

CURIAplus	Informatikprojekt der Parlamentsdienste, mit dem die bestehenden CURIA-Anwendungen und die Datenbank ersetzt werden sollen. Der parlamentarische Betrieb im Zusammenhang mit der Kommissions- und Sessionsarbeit soll gesamtheitlich in einer Grundausstattung digitalisiert werden.[10]
Denial of Service (DOS)	Ein Denial-of-Service-Angriff ist eine mutwillig herbeigeführte Überlastung eines Internetdienstes (beispielsweise einer Webseite), sodass dieser nicht mehr verfügbar ist.
HERMES	eCH-0054: HERMES Projektmanagement-Methode HERMES ist die Projektmanagement-Methode für Informatik, Dienstleistung, Service und Geschäftsorganisationen und wurde von der schweizerischen Bundesverwaltung entwickelt. Die Methode steht als offener Standard vom Verein eCH allen zur Verfügung. Aktuell gilt HERMES 5.1. (Quelle: www.hermes.admin.ch)
Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)	Das ISDS-Konzept bildet die Grundlage für die Festlegung der Massnahmen für die Informationssicherheit und den Datenschutz. Es zeigt die (Rest-)Risiken auf, die mit dem Betrieb des IT-Systems und der Organisation verbunden sind. Es beschreibt das Notfallkonzept. Gemäss der «Richtlinie Informationssicherheit in Projekten» der Parlamentsdienste muss das ISDS-Konzept gegen Ende der Konzeptphase erstellt sein (inkl. Risikoanalyse). Die Prüfung/Abnahme muss mit dem Phasenabschluss Konzept erfolgen. Die Umsetzung des ISDS-Konzeptes muss während der Realisierung erfolgen und vor der Einführung in die Produktion abgenommen werden. (Quellen: www.hermes.admin.ch sowie «Richtlinie Informationssicherheit in Projekten»)
Personas	Eine Persona ist ein Modell aus dem Bereich der Mensch-Computer-Interaktion. Die Persona stellt einen Prototyp für eine Gruppe von Nutzern dar, mit konkret ausgeprägten Eigenschaften und einem konkreten Nutzungsverhalten. Personas werden im Anforderungsmanagement von Computeranwendungen verwendet. Für eine geplante Computeranwendung wird analysiert, welcher Nutzerkreis diese Anwendung später nutzen wird. Dazu werden, anhand von Beobachtungen an realen Menschen, einige fiktive Personas geschaffen, die stellvertretend für den grössten Teil der späteren tatsächlichen Anwender stehen sollen. (Quelle: Wikipedia)

[10] Projektbeschreibung aus dem monatlichen Projektstatus-Rapport

Projektleiter (PL)	In den Parlamentsdiensten ist der PL der Hautpverantwortliche für ein Projekt. In der Regel wird er von einem IT-Projektleiter und einem Fach-Projektleiter unterstützt. PL sind in der Einheit «Innovation & Fachanwendungen» angesiedelt.
Qualitäts- und Risikomanager (QRM)	Der QRM unterstützt den Auftraggeber mit einer unabhängigen Beurteilung des Projekts. Er gibt Empfehlungen für Massnahmen zur Erreichung der Projektziele ab, hat aber keine eigene Entscheidungskompetenz. Hinweis: Die Rolle des QRM muss gem. HERMES nicht zwingend besetzt werden. Insbesondere ist der QRM verantwortlich für • die Beurteilung der Einhaltung der Vorgaben (Weisungen, Richtlinien) • die Beurteilung des Vorgehens und der Ergebnisse des Projektmanagements, der Projektorganisation und der Zusammenarbeit im Projekt • die umfassende Beurteilung der Prozesse der Projektsteuerung, -führung und -abwicklung bei allen Projektpartnern • die Beurteilung der Projektergebnisse aus qualitativer Sicht • die Beurteilung des Projektstands und der Prognosen • die Beurteilung der Risiken • die Empfehlung von Massnahmen zum Umgang mit Risiken und zur Erreichung der Projektziele • die transparente Berichterstattung an den Auftraggeber. (Quelle: https://www.hermes.admin.ch)
Schutzbedarfsanalyse (Schuban)	Mit der Schuban werden die Anforderungen an die Informationssicherheit und den Datenschutz erhoben. Zeigt die Schuban, dass ein erhöhter Schutz nötig ist, muss eine vertiefte Risikoanalyse durchgeführt und ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) verfasst werden. Gemäss der «Richtlinie Informationssicherheit in Projekten» der Parlamentsdienste muss die Freigabe der Schuban zu Beginn der Initialisierung erfolgen. (Quelle: https://www.hermes.admin.ch sowie «Richtlinie Informationssicherheit in Projekten»)

Verwaltungsdelegation	Der Verwaltungsdelegation obliegt die oberste Leitung der Parlamentsverwaltung. Sie befasst sich mit sämtlichen Fragen im Zusammenhang mit der Haushaltsführung, dem Personalmanagement, der Sicherheit, der Informatik und der Infrastruktur des Parlaments. Ausserdem übt die VD die Oberaufsicht über die Parlamentsdienste. (Quelle: www.parlament.ch)
Verordnung über die digitale Transformation und die Informatik (VDTI)	Die VDTI schafft die rechtliche Grundlage für die departementsübergreifende Organisation der Bundesverwaltung im Hinblick auf die digitale Transformation und die Lenkung der Informations- und Kommunikationstechnologie (IKT). Die VDTI ersetzt die bisherige Bundesinformatikverordnung (BinfV). (Quelle: Bundeskanzlei)

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).