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