Audit de la rentabilité et de la sécurité de l'informatique après l'externalisation

Services du Parlement

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a vérifié la rentabilité et la sécurité de l'informatique au sein des Services du Parlement après l'externalisation des secteurs suivants: réseau, téléphonie, WIFI, serveurs des messageries et des systèmes et base de données de la plateforme de collaboration. Dans le cadre de ses évaluations et de ses constatations, le CDF fait la distinction entre le secteur informatique des *parlementaires* et celui des *Services du Parlement*.

Le changement de fournisseur a considérablement amélioré la rentabilité

En passant de l'Office fédéral de l'informatique et de la télécommunication (OFIT) à Swisscom, le changement de fournisseur a permis de baisser les frais annuels de réseau et de téléphonie prévus par l'OFIT de 3 millions à 700 000 francs au total. Les attentes ont été largement dépassées, aussi bien au niveau du transfert des prestations initiales que de leur extension. Les bases décisionnelles destinées à l'Assemblée fédérale ont été élaborées correctement et présentées avec transparence dans la proposition concernant «le partenaire commercial pour les prestations informatiques des Services du Parlement» et dans l'étude de projet sur «l'exploitation et les frais de l'infrastructure informatique de base pour l'Assemblée fédérale» du 7 octobre 2010. Cependant, il n'existe aucun calcul rétrospectif pour la mise en œuvre du modèle d'affaire. Pour prouver sa rentabilité, le CDF a dû, au moment de l'audit, regrouper tout d'abord les frais de réalisation et d'exploitation et les comparer avec les anciens coûts.

Une gouvernance appropriée dans le domaine de la sécurité informatique du Parlement est un défi

La gouvernance informatique, en tant qu'instrument destiné à fixer les conditions-cadres et à soutenir la gestion informatique à l'échelon de la direction, est peu visible dans la structure du secteur informatique des parlementaires. La responsabilité de la gouvernance informatique n'a pas été clairement attribuée. L'évaluation des risques et la détermination des exigences en matière de sécurité incombent avant tout aux domaines de l'informatique (Domaine IT) et des délégués à la sécurité informatique (Domaine DSI) des Services du Parlement. Les mesures de sécurité prises reposent principalement sur l'estimation de ces derniers. Dans le cadre du développement de nouveaux services informatiques pour les Chambres fédérales, les mesures de sécurité ont été prises en accord avec la Délégation administrative (DA). De plus, les utilisateurs – à savoir les parlementaires – acceptent mal les mesures de sécurité qui concernent directement leur utilisation des services informatiques. Dès lors, il est difficile aussi bien pour la DA que pour les Domaines IT et DSI d'imposer et de mettre en œuvre dans le secteur informatique des parlementaires des mesures techniques et organisationnelles importantes visant à renforcer la sécurité, alors qu'elles ont fait leurs preuves et sont largement répandues.

Dans le nouveau projet de loi sur la sécurité de l'information, les Services du Parlement sont explicitement mentionnés. Reste à voir dans quelle mesure cette nouvelle loi débouchera sur des compétences correspondantes, capables de faciliter la mise en œuvre de la gouvernance informatique.

La sécurité informatique sur le plan technique devrait être améliorée ponctuellement

Les Domaines IT et DSI des Services du Parlement sont conscients des impératifs de sécurité. Le Domaine IT demande régulièrement à des spécialistes externes de l'évaluer dans des secteurs sensibles. En outre, les Services du Parlement, et donc les Domaines IT et DSI, suivent le standard de la Confédération, même s'ils n'y sont pas tenus (à l'exception de la connexion du réseau du Parlement au réseau VPN de l'administration fédérale). D'une manière générale, le secteur informatique des Services du Parlement se situe à un niveau approprié. Au cours de l'audit, le CDF a encore identifié quelques écarts par rapport aux directives techniques concernant les configurations des serveurs. Dans ce domaine, il faudrait mener des contrôles plus systématiques et améliorer la surveillance.

Texte original en allemand