## Audit transversal de la sécurité informatique de la Confédération
## Unité de pilotage informatique de la Confédération

### L'essentiel en bref

Dans ce quatrième audit transversal de la sécurité informatique de la Confédération depuis 2011, le Contrôle des finances (CDF) a examiné la mise en œuvre des mesures de protection de base des technologies de l'information. Ces mesures sont regroupées au sein d'un catalogue de 17 chapitres, édité par l'Unité de pilotage informatique de la Confédération (UPIC). Leur mise en œuvre est du ressort tant des fournisseurs (FP) que des bénéficiaires de prestations (BP), et doit être documentée. Les pratiques des sept départements, de la Chancellerie fédérale, de cinq fournisseurs de prestations et de l'UPIC ont été passées en revue. Douze applications critiques ont également été examinées. Enfin, le CDF a évalué la mise en œuvre du processus de gestion des risques liés à l'espionnage ainsi que celle des recommandations issues des audits transversaux antérieurs.

**L'examen des pratiques des bénéficiaires de prestations révèle un paysage contrasté**

La grande majorité des unités administratives (UA) examinées tiennent un inventaire actuel des applications en service. Sous l'angle de la sécurité, le CDF recommande toutefois de renoncer dans toute la mesure du possible au regroupement d'applications de moindre importance. Les documents de sécurité ne sont pas édités et actualisés pour toutes les applications. Des actions correctives sont en cours dans le sillage de l'affaire RUAG. Le CDF salue les améliorations en cours des outils permettant le contrôle des documents de sécurité. Il juge toutefois les contrôles de la mise en œuvre des mesures encore insuffisants.

Le contrôle périodique des droits d'utilisateurs est souvent négligé. Le CDF a émis des recommandations à l'attention des départements concernés. Il a en outre relevé que l'aspect de la sécurité pouvait être négligé dans le processus d'homologation des achats informatiques. Il a recommandé à l'UPIC de revoir son implication dans ces processus.

Pour une majorité des applications critiques examinées, des documents de sécurité actuels sont disponibles. Sur un plan matériel, le CDF considère que la majorité des concepts de sécurité répondent de manière appropriée aux besoins en protection. Il estime toutefois que dans un cas, les exigences en termes de confidentialité sont sous-estimées. Une solution est actuellement en cours de mise en place. Pour les trois applications recourant à la télémaintenance, les prescriptions sont respectées : Des comptes utilisateurs spéciaux sont définis, leur accès et leurs activités sont enregistrés et contrôlés. Aucune mesure d'amélioration immédiate n'est requise.

**Les pratiques des fournisseurs de prestations sont globalement satisfaisantes**

Les FP passés en revue s'impliquent activement dans l'édition et le contrôle des documents de sécurité des projets. Ils contrôlent également dans la majorité des cas la mise en œuvre des mesures de sécurité leur incombant. Ils mènent par ailleurs diverses activités d'amélioration continue en matière de sécurité. Le CDF juge la situation globalement satisfaisante.

Sur le plan de l'intégrité des systèmes, les FP ont mis en place les mesures de contrôle définies par l'UPIC. Le CDF constate toutefois que les techniques mises en œuvre diffèrent sensiblement entre fournisseurs. Il encourage l'UPIC à définir plus précisément les notions d'intégrité et d'en regrouper

les prescriptions. En outre, les solutions à mettre en œuvre pour surveiller l'intégrité des systèmes en service doivent être coordonnées avec les FP.

**La complexité croissante de la sécurité informatique**

Les exigences de la protection de base évoluent vers une complexité croissante, reflétée dans les mises à jour périodiques par l'UPIC du catalogue des mesures. Leur mise en œuvre peut poser problème. Les plateformes techniques et les applications se multiplient. Les délégués à la sécurité ne disposent cependant pas toujours du temps suffisant pour gérer les tâches requises. Le CDF voit un risque dans cette situation et recommande à l'UPIC de simplifier et d'optimiser les mesures de la protection de base là où c'est possible.

**Le contrôle de la mise en œuvre et de l'efficacité des mesures comporte des failles**

En matière de contrôle et de documentation de la mise en œuvre et de l'efficacité des mesures, la qualité des pratiques varie sensiblement. Les BP ne les documentent pas systématiquement et n'exigent pas dans tous les cas les rapports de contrôle de la part des FP.

Le CDF voit ici un manque. Il estime en outre peu efficient le système actuel de documentation du contrôle des mesures. Selon la démarche en place, les FP répondent souvent de manière redondante aux mêmes questions. Le CDF a recommandé à l'UPIC de trouver les moyens de faciliter la documentation et la confirmation périodique par les FP du contrôle de la mise en œuvre des mesures de protection.

En outre, les BP définissent rarement explicitement les responsabilités et les processus de contrôle de la mise en œuvre et de l'efficacité des mesures de protection. Le CDF juge qu'un risque réel existe que ces mesures ne soient simplement pas appliquées, faute de contrôle. Il a recommandé à l'UPIC de compléter les instructions de la protection de base. Celles-ci devraient prescrire aux départements de définir les responsabilités et les processus de contrôle.

**Le processus de gestion des risques liés à l'espionnage doit être simplifiée et clarifié**

Les UA passées en revue appliquent les nouvelles directives relatives à la méthode de gestion des risques visant à réduire les activités d'espionnage de service de renseignement (GRAES). Elles estiment que la démarche répond à un risque réel, mais qu'elle occasionne un travail trop important. Elles s'interrogent en outre sur la pertinence de certains critères d'analyse, leur pondération et sur les mesures à adopter pour les objets présentant un risque GRAES. Les UA ont pu exprimer ces objections lors des discussions en vue d'une deuxième version du processus.

Le CDF partage les réserves des départements sur l'efficacité du processus GRAES dans sa forme actuelle. [redacted] Le CDF a recommandé à l'UPIC de simplifier le processus et de clarifier les mesures à adopter pour les objets présentant un risque GRAES. La nouvelle version de la démarche pourrait s'inspirer des processus simplifiés définis dans certains départements.

**La plupart des recommandations d'audits transversaux antérieurs ont été mises en œuvre**

Le CDF constate que douze des quinze recommandations d'audits transversaux de sécurité informatique antérieurs encore ouvertes dans son système de suivi ont été mises en œuvre. Pour les trois recommandations restantes, les travaux sont en bonne voie.