Audit de la sécurité et de la disponibilité de l'exploitation GEVER

Chancellerie fédérale et Centre de services informatiques du Département fédéral de l'économie, de la formation et de la recherche

L'essentiel en bref

Avec le programme GENOVA, la Chancellerie fédérale (ChF) veut introduire un seul produit de gestion électronique des affaires (GEVER) pour toutes les unités de l'administration fédérale. Planifié entre novembre 2015 et septembre 2021, le programme est devisé à plus de 68 millions de francs. Le Centre de services informatiques du Département de l'économie, de la formation et de la recherche (ISCeco) assume la responsabilité principale de l'exploitation de la plateforme. Plus de 22 000 utilisateurs travaillent avec ce nouveau système en automne 2020.

Dans cette révision, le Contrôle fédéral des finances (CDF) évalue si, sous l'angle de la sécurité et de la disponibilité, les mesures mises en œuvre au niveau de l'exploitation sont adéquates. Il examine aussi si le passage du statut de projet au statut d'exploitation est réglé et si le suivi des points en suspens est assuré. Enfin, cet audit effectue un suivi de quatre recommandations de révisions antérieures.

Le CDF est parvenu à une conclusion globalement satisfaisante, bien que l'architecture complexe du système impose des exigences élevées à l'exploitation et qu'un travail important doit encore être accompli.

Les exigences de sécurité sont définies, mais la démarche n'est pas entièrement aboutie

L'architecture de la solution est complexe, plusieurs intervenants sont impliqués dans son exploitation. Leurs prérogatives sont clairement définies, ils jugent la collaboration satisfaisante. Les postes de spécialistes sont pourvus, l'exploitation peut être considérée comme stable, le développement des incidents est favorable. Les processus de conduite, de planification et d'exploitation sont définis au sein de l'ISCeco. Un audit interne du fonctionnement de l'exploitation a été mené, d'autres sont prévus. Pour le CDF, les définitions de l'organisation, de la conduite et des processus de l'exploitation sont appropriées. Les exigences de sécurité au niveau de la solution technique et de l'exploitation sont documentées. Les risques résiduels sont reconnus et acceptés. Le CDF a toutefois constaté que la mise en œuvre de la protection de base n'est pas complètement documentée.

Du côté des bénéficiaires de prestations, le CDF n'a pas examiné de façon approfondie le statut des démarches de sécurité. Il a cependant trouvé un cas où la répartition des tâches entre département et offices n'était pas clairement réglée. Le CDF demande ici un nouvel effort de communication.

Protection de l'accès et de l'intégrité : des mécanismes appropriés et quelques points à finaliser

La plateforme GEVER est installée dans le nuage privé (« private cloud ») de l'administration fédérale hébergé à l'Office fédéral de l'informatique et de la télécommunication (OFIT). Elle est utilisée au sein du réseau informatique protégé de la Confédération. L'authentification à deux facteurs est assurée par le service TIC standard eIAM[1]. Les utilisateurs se voient assigner le système de leur département et des autorisations limitant les opérations et objets auxquels ils peuvent accéder. Un nombre limité d'administrateurs est défini, aux niveaux applicatif et technique. Les mécanismes en place sont globalement appropriés. Le CDF a toutefois constaté que les contrôles annuels des listes d'utilisateurs privilégiés n'étaient pas encore opérationnels.

Une solution du Groupement défense assure la confidentialité des documents jusqu'au niveau CONFIDENTIEL. Le règlement d'utilisation proscrit par contre le traitement des documents de niveau SECRET et le système bloque la définition d'un document dans cette catégorie de classification. Le risque de saisie de données sensibles dans les métadonnées subsiste et est reconnu par le donneur d'ordre.

Le processus de gestion des changements en place à l'ISCeco définit de manière adéquate les étapes à suivre (demande, validation, exécution, tests). En revanche, les changements ne sont pas systématiquement répertoriés dans toutes les composantes du système. Le CDF n'a donc pas pu contrôler l'efficacité du processus de gestion des changements. Des outils contrôlent régulièrement l'intégrité des serveurs. Des mécanismes de hachage[2] sont disponibles sur la plateforme, mais pas encore utilisés. Le CDF a demandé de clarifier ce point.

Gestion de la continuité : la démarche n'est pas entièrement aboutie

Pour répondre aux besoins accrus en termes de disponibilité du système, l'infrastructure est conçue de manière redondante dans des centres de calcul séparés. Les tests ont montré que les bascules fonctionnent en cas de défaillance. Un système de surveillance des composantes de la plateforme est en place à l'ISCeco, des alertes sont émises et des tickets d'incident sont automatiquement générés en cas de grave dysfonctionnement. Ceux-ci sont alors traités selon les procédures en vigueur. Le CDF souligne que des composantes ne sont pas sous le contrôle de l'ISCeco. Celui-ci doit alors s'appuyer sur d'autres fournisseurs de prestations pour la résolution des incidents.

Sur le plan de la gestion de la récupération, le CDF constate que des aspects ne sont pas encore documentés. Diverses mesures sont certes définies, des sauvegardes régulières et des tests de restauration sont effectués, mais il manque une vue d'ensemble structurée dans ce domaine (« policy »). Des scénarios de défaillance, des plans de récupération actuels et des tests de reconstruction plus étendus doivent également être préparés.

La transition vers l'organisation permanente est réglée

Diverses activités et instances sont définies pour traiter la transition vers le statut d'exploitation. Des groupes de travail aux niveaux du pilotage, de la conduite et de l'exécution se réunissent régulièrement et impliquent les différents acteurs concernés. Le transfert de

[1] Service TIC standard de gestion de l'identité et des accès, géré par l'UPIC.
[2] Fonction cryptographique utilisée à des fins de vérification.

connaissance est ainsi facilité. Des listes de suspens sont gérées à ces niveaux. Le CDF estime que ces mécanismes sont adéquats, même s'il attend quelques incertitudes liées à la reprise des fonctions de l'UPIC par la Chancellerie fédérale dès janvier 2021.

Les recommandations émises précédemment par le CDF sont largement mises en œuvre.