

## Configuration et démarrage de la gestion des utilisateurs et des droits d'accès SAP

Audit de surveillance financière à l'Administration fédérale des finances

### L'essentiel en bref

---

Le projet SAP SuPro BeBe de l'Administration fédérale des finances (AFF) visait à mettre en place les processus et les outils pour une amélioration du contrôle des droits d'accès dans les systèmes SAP de la Confédération. Terminé en juillet 2015, il a été réalisé pour quelque 2,5 millions de francs. A la suite de ce projet, les offices ont utilisé ces nouveaux processus de contrôle. Ils ont inventorié et remédié aux autorisations critiques et autres conflits de séparation de tâches constatés chez leurs utilisateurs. Prévues jusqu'au 30 novembre 2016, ces activités ont fait l'objet du présent audit du Contrôle fédéral des finances (CDF). Il s'agissait notamment de vérifier si les conditions d'une utilisation fiable des outils et des processus déployés dans les offices sont réunies.

Le CDF a constaté que l'AFF suit les activités de démarrage de manière adéquate et communique régulièrement avec les offices. Ceux-ci ont annoncé qu'ils tiendraient les délais de mise en conformité. L'AFF élabore actuellement une étude sur les suites à apporter au projet. Le CDF juge la démarche appropriée. Il encourage en outre l'AFF à procéder à une analyse des coûts et de l'utilité du projet SAP SuPro BeBe.

#### **Un bilan globalement satisfaisant, mais des améliorations mineures à mettre en œuvre**

Selon les analyses effectuées, les conditions pour une exploitation stable de la plateforme mise en place sont réunies. La configuration technique est globalement adéquate pour une utilisation fiable des outils, le CDF a néanmoins transmis quelques points d'amélioration mineurs à l'exploitant.

Le CDF a noté que les règles définissant ce qui constitue une violation – conflit de séparation de tâches ou autorisation critique – ont été testées et validées pendant le projet. La phase actuelle de l'exploitation a conduit à la mise en place d'un processus de gestion et de suivi des modifications des règles. Le CDF le juge approprié, mais il a constaté que certaines définitions incorporant des transactions spécifiques étaient incertaines. Le CDF a recommandé aux offices concernés de réviser ces règles avec l'appui de l'AFF.

Par ailleurs, le CDF a pu constater que des fonctions additionnelles – détection préventive de violations et workflow – ont été réalisées pour faciliter la gestion conforme des droits d'accès. Il encourage l'AFF à en prescrire l'usage généralisé. De même, le CDF préconise l'usage de rapports en format non modifiable de type PDF pour le suivi périodique des violations. Enfin, les définitions et processus de gestion des contrôles compensatoires ont été jugés adéquats.

#### **Quelques compléments aux instructions de travail de l'AFF sont souhaitables**

Le CDF juge adéquat le soutien de l'AFF aux activités de démarrage des unités administratives et estime que les guides et documents produits à leur attention sont de bonne qualité. Il a toutefois recommandé à l'AFF de compléter ses instructions sur la fréquence des revues de droits d'accès, la validation des concepts d'autorisation des offices, ainsi que le suivi des utilisateurs extérieurs aux offices avec droit de mutation.