EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

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

Audit de surveillance financière à l'Administration fédérale des finances

CDF-16569 / prises de position incluses / 13 septembre 2016

Impressum

Adresse de commande **Bestelladresse** **Indirizzo di ordinazione** **Order address**	Contrôle fédéral des finances (CDF) Monbijoustrasse 45, CH - 3003 Berne http://www.cdf.admin.ch
Numéro de commande **Bestellnummer** **Numero di ordinazione** **Order number**	1.16569.601.00188.006
Complément d'informations **Zusätzliche Informationen** **Informazioni complementari** **Additional information**	E-Mail: info@efk.admin.ch Tél. +41 58 463 11 11
Texte original **Originaltext** **Testo originale** **Original text**	Français Französisch Francese French
Résumé **Zusammenfassung** **Riassunto** **Summary**	Français (« L'essentiel en bref ») Deutsch (« Das Wesentliche in Kürze ») Italiano (« L'essenziale in breve ») English (« Key facts »)

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 revérifier 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.

Konfiguration und Start der Benutzer- und Berechtigungsverwaltung im SAP-Bereich
Finanzaufsichtsprüfung bei der Eidgenössischen Finanzverwaltung

Das Wesentliche in Kürze

Mit dem Projekt SuPro BeBe SAP der Eidgenössischen Finanzverwaltung (EFV) sollten Prozesse und Instrumente zur Verbesserung der Kontrolle der Zugriffsberechtigungen in den SAP-Systemen der Bundesverwaltung eingeführt werden. Das Projekt wurde im Juli 2015 abgeschlossen und hat rund 2,5 Millionen Franken gekostet. Seitdem benutzen die Ämter die neuen Kontrollprozesse. Sie haben eine Bestandsaufnahme aller bei ihren Benutzerinnen und Benutzern festgestellten kritischen Berechtigungen und aller anderen Konflikte in der Funktionstrennung (SoD) gemacht und sie beseitigt. Diese Tätigkeiten, die noch bis zum 30. November 2016 dauern, sind Gegenstand der vorliegenden Prüfung der Eidgenössischen Finanzkontrolle (EFK). Insbesondere wurde überprüft, ob die Voraussetzungen für eine sichere Nutzung der Instrumente und Prozesse in den Ämtern gegeben sind.

Die EFK hat festgestellt, dass die EFV den Startvorgang in angemessener Weise verfolgt und regelmässig mit den Ämtern kommuniziert. Diese haben angekündigt, dass sie die Anpassungsfristen einhalten werden. Die EFV erarbeitet derzeit eine Studie über die Folgemassnahmen zum Projekt. Die EFK erachtet das Vorgehen als angemessen. Zudem schlägt sie der EFV vor, eine Kosten-Nutzen-Analyse für das Projekt SuPro BeBe SAP durchzuführen.

Eine insgesamt zufriedenstellende Bilanz, aber kleinere Verbesserungen sind erforderlich

Die Untersuchungen haben gezeigt, dass die Voraussetzungen für einen stabilen Betrieb der Plattform gegeben sind. Die technische Konfiguration eignet sich insgesamt für eine sichere Nutzung der Instrumente. Die EFK hat den Betreiber dennoch auf einige kleine Verbesserungsmöglichkeiten hingewiesen.

Die EFK hat festgestellt, dass die Regeln, die festlegen, was eine Verletzung ist – SoD-Konflikte oder kritische Berechtigung – während der Projektphase überprüft und validiert wurden. Die aktuelle Betriebsphase hat zur Einführung eines Prozesses zur Verwaltung und Verfolgung der Änderungen im Regelbereich geführt. Die EFK ist der Meinung, dass dieser zweckmässig ist. Sie hat jedoch festgestellt, dass gewisse Definitionen von spezifischen Transaktionen nicht präzise genug sind. Die EFK hat den betroffenen Ämtern empfohlen, diese Regeln mit Unterstützung der EFV noch einmal zu überprüfen.

Die EFK konnte zudem feststellen, dass Zusatzfunktionen – frühzeitige Erkennung von Verletzungen und Workflow – realisiert wurden, um eine angemessene Berechtigungsverwaltung zu erleichtern. Sie legt der EFV nahe, die systematische Nutzung dieser Zusatzfunktionen vorzuschreiben. Die EFK rät ihr ferner, für die Berichte zur regelmässigen Verfolgung der Verletzungen ein nicht veränderbares Format (z.B. PDF) zu verwenden. Und zu guter Letzt wurden die Definitionen und Prozesse für die Verwaltung der mindernden Kontrollen als angemessen beurteilt.

Einige wünschenswerte Ergänzungen zu den Arbeitsanweisungen der EFV

Die EFK ist der Ansicht, dass die EFV die Verwaltungseinheiten beim Startvorgang in angemessener Weise unterstützt und ihnen dafür Leitfäden und Dokumente von hoher Qualität zur Verfügung stellt. Die EFK hat der EFV dennoch empfohlen, ihre Anweisungen zur Häufigkeit der Überprüfung der Zugriffsberechtigungen, zur Freigabe der Berechtigungskonzepte der Ämter sowie zur Verfolgung der externen Nutzerinnen und Nutzer mit Änderungsberechtigung zu vervollständigen.

Originaltext in Französisch

Configurazione e avvio della gestione degli utenti e delle autorizzazioni d'accesso in SAP
Verifica della vigilanza finanziaria nell'Amministrazione federale delle finanze

L'essenziale in breve

Il progetto SAP SuPro BeBe dell'Amministrazione federale delle finanze (AFF) aveva l'obiettivo di istituire i processi e gli strumenti per migliorare il controllo delle autorizzazioni d'accesso ai sistemi SAP della Confederazione. Terminato nel luglio 2015, il progetto è costato a circa 2,5 milioni di franchi. Sulla base del progetto, le unità amministrative (UA) hanno utilizzato i nuovi processi di controllo per inventariare ed eliminare le autorizzazioni critiche e gli altri conflitti di separazione dei compiti riscontrate presso gli utenti. Tali attività, che saranno portate a termine entro il 30 novembre 2016, sono state oggetto della presente verifica svolta dal Controllo federale delle finanze (CDF), il quale ha voluto verificare in particolare se sussistono le condizioni per un utilizzo affidabile dei processi e degli strumenti adottati nelle UA.

Il CDF ha constatato che l'AFF segue in modo adeguato le attività di avvio e comunica regolarmente con le UA. Queste ultime hanno inoltre fatto sapere che le attività saranno svolte entro i termini previsti. Attualmente l'AFF sta elaborando uno studio per dare seguito al progetto. L'iniziativa è giudicata positivamente dal CDF, il quale incoraggia l'AFF a procedere anche con un'analisi dei costi e dell'utilità del progetto SAP SuPro BeBe.

Bilancio complessivamente positivo, ma con piccoli miglioramenti da apportare

Secondo le analisi effettuate, le condizioni per un'operatività stabile della piattaforma allestita sono garantite. Tuttavia, sebbene la configurazione tecnica sia complessivamente adeguata per un utilizzo affidabile degli strumenti, il CDF ha segnalato alcuni punti sui quali apportare piccoli miglioramenti.

Secondo il CDF le regole che determinano una violazione (ossia un conflitto di separazione dei compiti o un'autorizzazione critica) sono state testate e confermate durante il progetto. L'attuale fase di operatività ha portato all'introduzione di un processo di gestione e monitoraggio delle modifiche delle regole. Secondo il CDF tale processo è appropriato, ma alcune definizioni che incorporano delle operazioni specifiche sono state valutate come incerte. Il CDF ha quindi raccomandato alle UA interessate di verificare nuovamente tali punti con il sostegno dell'AFF.

Il CDF, inoltre, ha avuto modo di constatare che per facilitare la buona gestione delle autorizzazioni d'accesso in SAP sono state create delle funzioni aggiuntive, ossia l'individuazione preventiva di violazioni e il workflow. Il CDF incoraggia l'AFF a prescriverne un uso generalizzato e raccomanda l'utilizzo di rapporti in formato non modificabile (PDF) per il monitoraggio periodico delle violazioni. Infine, il CDF reputa adeguati anche le definizioni e i processi di gestione dei controlli di compensazione in caso di violazioni.

Necessità di ampliamento delle guide pratiche prodotte dall'AFF

Il CDF ha valutato come appropriato l'appoggio fornito dall'AFF alle UA nelle attività di avvio e si è espresso positivamente anche sulla qualità delle guide e dei documenti prodotti dall'AFF in proposito. È tuttavia caldeggiato il completamento delle istruzioni sulla frequenza delle revisioni delle autorizzazioni di accesso a SAP, oltre che un miglioramento del processo di conferma dei principi di autorizzazione delle UA e il monitoraggio degli utenti esterni alle UA con autorizzazione di modifica.

Testo originale in francese

Configuration and launch of SAP user management and access rights
Financial supervision audit in the Federal Finance Administration

Key facts

The aim of the SAP project SuPro BeBe of the Federal Finance Administration (FFA) was to establish the processes and the tools to improve control of access rights in the SAP systems of the Confederation. This was completed in July 2015 and had been achieved for around CHF 2.5 million. Following the completion of the project, the offices applied these new control processes. They identified and rectified the critical clearances and other conflicts in task segregation among their users. These activities which are planned up until 30 November 2016 were the subject of this audit by the Swiss Federal Audit Office (SFAO). This included verifying if the conditions for reliable use of the tools and processes deployed in the offices have been fulfilled.

The SFAO noted that the FFA adequately follows the start-up activities and is in regular contact with the offices which have announced that they would meet the compliance deadlines. The FFA is currently preparing a study on the action to be taken to the project. The SFAO deems this to be the right approach. In addition, it is encouraging the FFA to do an analysis of the costs and usefulness of the SAP SuPro BeBe project.

An overall satisfactory result but minor improvements have to be implemented

Based on the analyses made, the conditions for stable operation of the platform set up have been met. The technical configuration is broadly adequate to ensure reliable use of the tools, the SFAO nonetheless forwarded some minor points aimed at improvement to the operator.

The SFAO noted that the regulations defining what constitutes a violation – clash in the separation of tasks or critical authorisation – were tested and validated during the project. The current phase of operation led to a management process being set up and to a follow-up on the adjustments of the rules. The SFAO considers it appropriate but found that certain definitions incorporating specific transactions were obscure. The SFAO recommended to the offices concerned to double-check these rules with the support of the FFA.

Furthermore, the SFAO noted that additional functions – precautionary screening of violations and workflow – were carried out to facilitate compliant rights management. It encourages the FFA to stipulate general use. Furthermore, the SFAO recommends the use of reports in a non-modifiable format like PDF for the periodic violation follow-up. Finally, the definitions and the management processes of the compensatory controls were found to be adequate.

Some additions to the working instructions of the FFA would be beneficial

The SFAO considers the support from the FFA in the start-up activities of the administrative units to be adequate and that the guides and documents produced destined for them are of good quality. However, it recommended to the FFA to complete its instructions on the frequency of the reviews of access rights, validating the authorisation concepts of the offices as well as the follow-up of external users to the offices with change authorisations.

Original text in French

Prise de position générale de l'AFF

Die EFK hat in der Vergangenheit regelmässig das Berechtigungswesen in SAP bemängelt. Die EFV hat in der Folge grosse Anstrengungen unternommen und zusammen mit den anderen Fachämtern (EPA, BBL und ISB), den IKT (SAP) – LE und den Departementen im Rahmen eines mehrjährigen Projektes die Benutzer- und Berechtigungsverwaltung SAP in der BVerw überarbeitet und deutlich gestärkt. Die neu eingeführten Systeme und Prozesse erlauben heute eine geeignete Kontrolle der Benutzer und der diesen zugeteilten Berechtigungen. Die entsprechenden Umsetzungsarbeiten in den einzelnen VE sind noch im Gang und sollen bis Ende 2016 abgeschlossen sein. Die EFV nimmt mit Befriedigung zur Kenntnis, dass die EFK die laufenden Arbeiten und die erzielten Ergebnisse positiv beurteilt und nur geringfügige Anpassungen empfiehlt.

Die EFV verdankt explizit die konstruktive Mitarbeit und Unterstützung aller Beteiligten bei diesen aufwändigen Arbeiten. Im Ergebnis werden die Qualität und die Ordnungsmässigkeit des Rechnungswesens der BVerw verbessert. Ein weiterer Ausbau bzw. Projekte im Berechtigungswesen SAP wird die EFV aus verwaltungsökonomischen Gründen nur mit Zurückhaltung, Augenmass und bei hoher Dringlichkeit angehen.

Wir danken der EFK für die effiziente, sachliche und kompetente Durchführung der Prüfungsarbeiten und für die Gelegenheit zur Stellungnahme.

Table des matières

1 Mission et déroulement de l'audit

1.1 Contexte

Le projet SAP SuPro BeBe de l'Administration fédérale des finances (AFF) visait à mettre en place les processus et les systèmes permettant une amélioration du contrôle des droits d'accès dans les systèmes SAP de la Confédération. L'objectif était d'identifier les droits d'accès critiques et les violations de la séparation des tâches, et de les supprimer pour les utilisateurs concernés ou d'y remédier par des contrôles compensatoires. Dans un premier temps, la gestion des droits d'accès des processus de support – finances et comptabilité, ressources humaines et logistique – a été considérée. Le projet a mis en œuvre à cet effet un système de contrôle, le module Access Right Analysis (ARA) de la plateforme SAP GRC de l'éditeur SAP AG. Les processus définis ont fait par la suite l'objet d'un déploiement dans les offices de la Confédération. Le projet, terminé en juillet 2015, a été réalisé pour une enveloppe d'environ 2,5 millions de francs.

Suite à ce projet, les offices de la Confédération ont procédé au démarrage des nouveaux processus de contrôle des droits d'accès. Ils ont également effectué une revue et diverses corrections des droits d'accès de leurs utilisateurs SAP. En parallèle, l'AFF a suivi ce démarrage. Elle a défini 18 mesures d'amélioration de divers aspects des processus et des systèmes mis en place, dont 10 ont déjà été mises en œuvre. Ces activités ont pour terme prévu le 30 novembre 2016. Le schéma suivant montre le calendrier des activités.

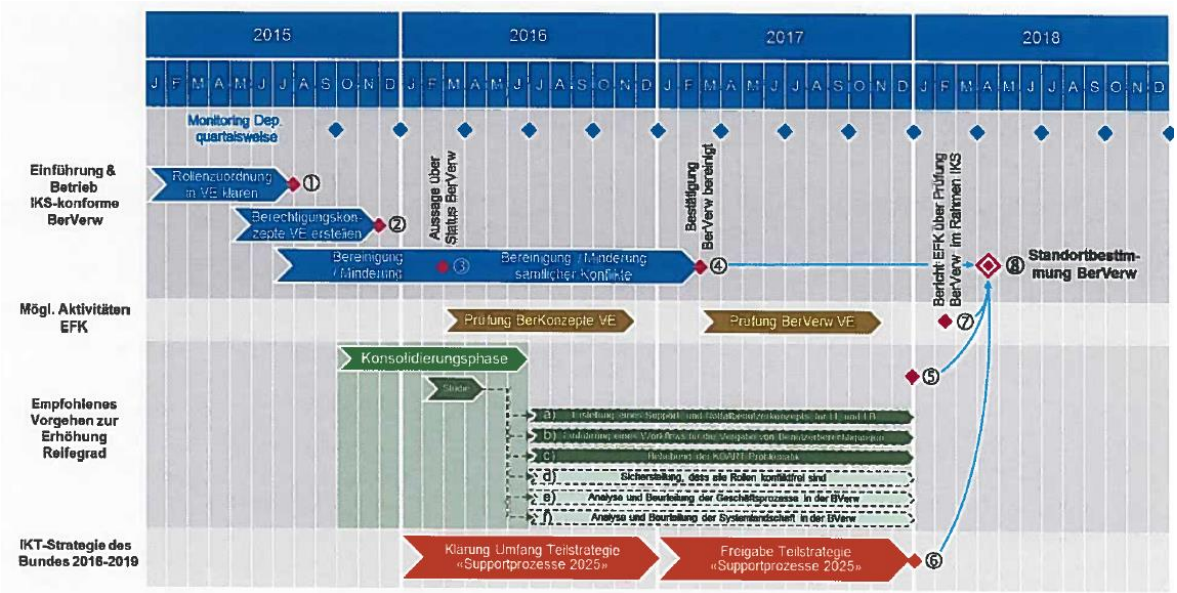

Fig. 1 : Feuille de route du projet SuPro BeBe et des activités annexes

1.2 Objectifs et questions d'audit

L'audit du Contrôle fédéral des finances (CDF) a eu pour objectif de vérifier que les conditions pour une utilisation efficace des outils de contrôle des droits d'accès sont réunies.

Compte tenu de l'analyse de risques du CDF, les questions suivantes ont été traitées pour répondre à l'objectif d'audit :

- Le projet SAP SuPro BeBe a-t-il été mis en œuvre correctement sur le plan technique, de manière à atteindre les objectifs fixés ?
- Les conditions pour une exploitation stable de la plateforme sont-elles réunies ?
- Les concepts d'autorisation des unités administratives sont-ils appropriés ?
- Y a-t-il des raisons de penser que certaines unités administratives n'auront pas terminé à temps les activités de démarrage?
- Des mesures sont-elles prévues pour calculer l'impact et la rentabilité de la mise en œuvre du projet SAP SuPro BeBe ?

1.3 Etendue de l'audit et principes

L'audit des aspects « métier » a été mené du 25 avril au 10 juin 2016 par MM. Stéphane Kury et André Stauffer (responsable de révision). L'audit de l'exploitation et de la configuration technique de la plateforme a été conduit par la société Ernst and Young SA (EY) pendant la même période.

Les travaux d'audit de l'exploitation se sont concentrés sur l'évaluation de la définition des contrôles informatiques généraux mis en place pour la plateforme SAP GRC.

Pour finaliser cet audit, le CDF et EY ont eu recours aux méthodes suivantes :

- des interviews de spécialistes de diverses unités administratives :
    - l'Office fédéral de l'informatique et des télécommunications (OFIT) pour les questions d'exploitation et de configuration technique
    - l'AFF pour les aspects « métier » de la configuration de la plateforme SAP GRC
    - l'Administration fédérale des douanes (AFD), le Secrétariat Général du Département de l'environnement, des transports, de l'énergie et de la communication (DETEC), et le Centre de services en matière de finances du Département fédéral des finances (DFF) pour le jugement des activités de démarrage ;
- des analyses documentaires (instructions, procédures, rapports, etc.) ;
- des observations des valeurs de paramètres de la configuration technique de la plateforme SAP GRC.

Le jugement des activités de démarrage repose sur des documents et des assertions recueillis au sein de trois unités administratives, choisies en fonction du risque qu'elles représentent en termes de conformité de la gestion des droits d'accès SAP (volume ou étendue des droits). Les constats tirés sont mentionnés à titre d'illustration et ne sauraient refléter la situation de manière représentative.

1.4 Documentation et entretiens

Les informations et documents requis ont été fournis rapidement et de manière compétente par les spécialistes concernés. Le CDF remercie l'ensemble des personnes impliquées dans cet audit pour leur disponibilité et leur collaboration.

2 Avancement des activités de démarrage et suite des événements

2.1 Le suivi par l'AFF des activités de démarrage est adéquat

L'AFF effectue un suivi régulier des activités de démarrage dans les unités administratives. Elle pointe le nombre de conflits par unité, édite des rapports de synthèse de l'avancement et discute régulièrement des progrès avec les départements au sein du « Fachgruppe Compliance ». L'AFF apporte par ailleurs un soutien méthodologique aux unités administratives qui en font la demande.

L'objectif au 30 novembre 2016 est de n'avoir plus aucune violation de droits non compensée par un contrôle. Le nombre de violations non compensées a diminué de manière sensible depuis le début des activités de démarrage. Les unités ont par ailleurs annoncé qu'elles tiendraient le délai.

De l'avis du CDF, l'AFF suit l'avancement des activités de démarrage de manière efficace.

2.2 Mettre en regard des coûts et des effets

Le CDF note que les offices sondés mettent en avant la transparence accrue apportée par les nouveaux systèmes et processus mis en œuvre dans la gestion et le contrôle des droits d'accès SAP. Dans leur perception, le risque d'accès non autorisé ou de fraude a diminué.

Le projet SAP SuPro BeBe a encouru des coûts inférieurs à 5 millions de francs. Il n'est de ce fait pas considéré comme un grand projet informatique au sens des directives du Conseil fédéral concernant les projets informatiques de l'administration fédérale et le portefeuille informatique de la Confédération. Il n'est ainsi pas soumis à l'obligation de planifier et d'exécuter un calcul de rentabilité de projet („Kosten-Nutzen-Analyse"). Le CDF estime pourtant qu'un tel calcul fait partie des bonnes pratiques en matière de gestion de projet. Il encourage vivement l'AFF à tenter l'exercice pour le projet SAP SuPro BeBe, ce d'autant plus que d'autres activités annexes sont prévues (intégration des fonctions des spécialistes informatiques ou d'autres systèmes SAP dans le périmètre d'analyse). Leur coût additionné aux dépenses déjà encourues pourrait dépasser le montant minimum évoqué plus haut.

2.3 Le détail de la suite des événements est en cours d'élaboration

Le projet SAP SuPro BeBe avait produit une feuille de route globale des activités et des projets à mener après son terme. Sur cette base, l'AFF élabore actuellement une étude visant à préciser les étapes suivantes de manière détaillée, à en fixer les priorités, les échéances et les ressources nécessaires.

Parmi les thèmes pressentis, on compte notamment :

- les systèmes SAP à intégrer dans le périmètre d'analyse de SAP GRC
- les fonctions « métier » à intégrer dans le périmètre d'analyse de SAP GRC, notamment les fonctions liées aux processus informatiques (utilisateurs de support, de paramétrage, gestionnaires des droits d'accès, administrateurs systèmes, développeurs, etc.)
- le déploiement de fonctions et d'outils complémentaires dans les offices (notamment : workflow).

Le CDF a ainsi pu constater que les réflexions sont en cours à l'AFF sur la suite des événements dans le domaine de la gestion conforme des droits d'accès des systèmes SAP. Il juge la démarche appropriée et prendra connaissance avec intérêt de l'étude de l'AFF.

3 Exploitation et configuration technique de la plateforme SAP GRC

3.1 L'examen de l'exploitation n'a pas révélé de problèmes significatifs

Les spécialistes d'EY ont pu constater que l'exploitation du système SAP GRC se fait selon les mêmes modalités que les autres systèmes SAP hébergés à l'OFIT. En particulier, l'attribution de droits étendus à des utilisateurs de SAP GRC est réglée selon le même processus et soumise aux mêmes validations que pour les autres systèmes SAP.

La plateforme étant soumise aux mêmes contrôles, le CDF n'a pas de raison de penser que la stabilité de l'exploitation soit compromise.

3.2 Quelques détails de la configuration technique peuvent être optimisés

Les spécialistes d'EY ont jugé que la configuration technique des systèmes SAP GRC permet une utilisation fiable des fonctionnalités de contrôle des droits d'accès. Ils ont néanmoins identifié et consigné divers points de détail susceptibles d'être améliorés. Ces points ont été transmis à l'OFIT pour discussion et pour traitement. L'AFF en a été informée.

Le CDF a par ailleurs pu constater qu'un programme d'interface mis à disposition par SAP pour le chargement de rôles dits „AM" ne fonctionnait pas depuis mai 2015. Les corrections livrées à ce jour par l'éditeur n'ont pas permis de résoudre le problème et un ticket d'assistance est encore en suspens chez SAP. Les données concernées par cette erreur ne sont toutefois pas de première importance et une solution de secours acceptable a été mise en œuvre. Le CDF encourage l'OFIT à poursuivre ses contacts avec l'éditeur du logiciel en vue de la résolution du problème.

4 Aspects « métier » de la configuration de la plateforme SAP GRC

4.1 Le processus de définition et de modification des règles est approprié

Le système SAP GRC se base sur un ensemble de règles d'analyse qui définissent ce qui constitue une violation – conflit de séparation des tâches ou autorisation critique.

L'ensemble des règles mis en œuvre dans le cadre du projet SAP SuPro BeBe a été repris du contenu standard mis à disposition par SAP avec la plateforme GRC. Ce contenu, qui couvre un grand nombre de violations, a été ensuite adapté et complété par des spécialistes externes et internes aux besoins particuliers de la Confédération. Pendant le projet, chaque unité administrative a pu tester que l'ensemble de règles défini couvraient ses risques. Par la suite, les responsables de la compliance (AFF) et du projet SAP SuPro BeBe ont pu valider l'ensemble des règles.

Le système SAP GRC étant maintenant productif, un processus pour gérer les modifications apportées à l'ensemble des règles définissant les exceptions est mis en place. Tous les changements

demandés sont testés, évalués pour approbation et documentés par la responsable de la Compliance. Tous les changements réalisés par rapport à l'ensemble des règles validé à la fin du projet sont en outre consignés dans une liste à cet effet. La traçabilité des modifications est ainsi assurée.

Le CDF estime que les activités de définition et de validation pendant le projet ont permis de produire une version satisfaisante de l'ensemble des règles. Par ailleurs, celui-ci continue d'être complété et corrigé au fur et à mesure de l'évolution de la couverture de SAP GRC ou de la découverte d'inexactitudes. Le CDF juge appropriées les méthodes de suivi des modifications apportées à l'ensemble des règles.

4.2 Certaines règles intégrant les transactions spécifiques sont à revérifier

Le CDF a noté que les transactions spécifiques des unités administratives ont été prises en considération pendant le projet SAP SuPro BeBe. Les violations en lien avec ces transactions spécifiques ont donc été incluses dans l'ensemble des règles défini. Les spécialistes d'EY ont constaté que quelques violations ont été définies de manière potentiellement incomplète : la règle intègre le contrôle du lancement de la transaction mais pas celui des objets d'autorisation détaillés contenus dans la transaction (par exemple détail des unités administratives dans lesquelles l'utilisateur peut exécuter la transaction). La liste des définitions incriminées a été remise à l'OFIT et à l'AFF pour analyse et pour traitement.

Le CDF a par ailleurs pris note que l'AFF a inventorié d'autres règles définies de manière incomplète (niveau transaction, mais sans niveau objet d'autorisation), et compte les compléter. De l'avis du CDF, ces corrections doivent intervenir rapidement pour éviter d'éventuels impacts pendant la période de démarrage.

En outre, le représentant de l'Administration fédérale des douanes (AFD) a signalé des incertitudes sur quelques définitions de règles incorporant des transactions spécifiques à son domaine, notamment dans l'assignation des transactions aux identifiants de fonctions („Funktions-ID"). Les règles incriminées doivent être revérifiées.

Recommandation 1 (priorité 2):

Le CDF recommande à l'Administration fédérale des douanes de revérifier avec l'appui de l'Administration fédérale des finances les définitions incertaines des règles liées à ses transactions spécifiques (liens aux „Funktions-ID") et de communiquer les éventuelles corrections à leur apporter.

Prise de position de l'AFD:

Einverstanden; Die Abteilung Finanzen der EZV prüft zusammen mit der EFV bei den VE-spezifischen Transaktionen, welche einer Funktions-ID zugewiesen sind, ob diese IKS-relevant sind.

- Wenn keine IKS-Relevanz: Mittels CR wird beantragt, die VE-spezifische Transaktion aus der zugewiesenen Funktions-ID zu entfernen, damit sie kein Risiko mehr darstellt. Demzufolge wird sie im BRW deaktiviert.
- Wenn IKS-Relevanz: Die EZV analysiert zusammen mit der EFV, ob die VE-spezifische Transaktion der korrekten Funktions-ID und dem korrekten Risiko zugewiesen ist. Ist dem nicht so, wird mittels CR eine Berichtigung beantragt.

4.3 Des outils additionnels facilitent une gestion conforme des droits d'accès

Le CDF a pu constater la mise en œuvre de fonctionnalités supplémentaires dans le module d'assignation des rôles aux utilisateurs. Ces outils additionnels, qui ont pour but de faciliter une gestion conforme des droits d'accès des utilisateurs, sont les suivants :

- Simulation : la fonction permet la détection préventive des violations issues d'une modification d'assignation de rôles.
- Workflow : la fonction permet de forcer la séparation des tâches entre la personne qui attribue le rôle et celle qui valide et documente les agents ayant procédé à ces activités.

Ces deux fonctions ont été développées et testées pendant le projet SAP SuPro BeBe et sont disponibles à l'utilisation. La simulation est utilisable immédiatement, le workflow présuppose des activités de configuration par les unités administratives, notamment la définition des agents. Les manuels d'utilisation décrivent en détail les modalités de l'utilisation de ces deux fonctions.

A l'heure actuelle, la fonction de workflow a été déployée dans 11 unités administratives. L'étude en cours d'élaboration par l'AFF sur la suite des événements prévoit de prescrire l'utilisation de la fonction de workflow par toutes les unités administratives. Le financement de son déploiement restant à charge des offices, des questions de financement des travaux pourraient devoir être réglées au préalable.

Le CDF estime que ces fonctionnalités additionnelles permettent une réduction bienvenue des risques liés à la gestion des assignations de rôles aux utilisateurs. Il salue par ailleurs les intentions de l'AFF d'en prescrire l'utilisation à tous les offices, qu'il ne manquera pas de vérifier lors de ses prochaines révisions du compte d'état dès 2017.

4.4 L'utilisation de rapports d'analyse non modifiables doit être préconisée

Dans le cadre de leur revue périodique des droits d'accès, les offices produisent des rapports tirés de SAP GRC afin de documenter l'état des violations pour leurs utilisateurs. Le CDF a constaté que plusieurs formats sont possibles pour ces rapports, Excel ou PDF. Pour le travail opérationnel de gestion des droits d'accès et leur correction, les rapports sous format Excel sont particulièrement adaptés, car ils permettent un traitement des données et leur sélection.

Pour l'édition et la conservation des rapports périodiques de vérification, le CDF estime le format Excel peu approprié à cause du risque que des violations ne soient effacées dans les documents. Certes, un processus de réconciliation pour s'assurer qu'aucune modification non permise ne puisse être effectuée existe. Une comparaison des totaux entre la liste et le rapport généré en ligne dans SAP GRC est en effet possible. Néanmoins, pour simplifier le processus de reporting, le CDF recommande l'utilisation de rapports sous format PDF.

Recommandation 2 (priorité 3):

Le CDF recommande à l'AFF de préconiser aux unités administratives l'emploi d'un format non modifiable (PDF) pour l'édition et la conservation des rapports périodiques des violations tirés de SAP GRC.

Prise de position de l'AFF:

Die Compliance Managerin wird in ihrem Auftrag der jährlichen Risikoanalyse an die Berechtigungsverantwortlichen VE darauf hinweisen, dass die Berichterstattung an den IKS-Beauftragten ebenfalls eine PDF Auswertung der Berichte SAP GRC enthalten muss. Die Berichtsvorlage „IKS-Jahresbericht Berechtigungsverantwortlicher" wird dementsprechend angepasst.

4.5 Quelques points de configuration spécifique définis par des variantes

Hormis les définitions de règles portant sur les transactions spécifiques (voir plus haut), quelques éléments de configuration ont été mis en place par les unités administratives. Il s'agit de variantes d'exécution des rapports définies à l'aide de la fonctionnalité standard disponible dans les systèmes SAP. Ces variantes ont été créées et testées lors des ateliers de formation des utilisateurs de SAP SuPro BeBe.

Le CDF juge le procédé approprié et n'a pas connaissance d'autres éléments de configuration spécifique qui auraient été définis pour les offices.

4.6 La gestion des contrôles compensatoires est appropriée

Dans les cas où les droits d'accès critiques ne peuvent pas être retirés des rôles, ou si la séparation des tâches ne peut pas être assurée, les unités administratives doivent mettre en œuvre des contrôles compensatoires. L'AFF a élaboré des recommandations à l'attention des offices ainsi qu'une liste des contrôles possibles. Elle a décrit le processus de l'exécution des contrôles compensatoires et les responsabilités des divers intervenants.

L'AFF prescrit que les contrôles compensatoires utilisés pour atténuer un risque doivent être définis par chaque unité administrative dans la matrice de contrôle sous la responsabilité du chargé du système de contrôle interne. L'exécution des contrôles est ainsi intégrée dans les activités de surveillance définies au sein du système de contrôle interne.

Les contrôles compensatoires ont été définis de manière générique dans SAP GRC. Les spécialistes d'EY ont relevé que certains paramètres permettant de limiter le choix des contrôles compensatoires possibles dans une situation donnée (par exemple en fonction du processus) n'ont pas été définis. L'AFF rétorque que d'autres mécanismes sont en place pour limiter le choix d'un contrôle compensatoire face à un risque donné, et ce en fonction de l'unité administrative. Ainsi, seuls deux risques compensatoires peuvent être choisis par unité administrative (un pour les séparations de tâches, un pour les droits critiques). Le risque soulevé par EY semble donc être réduit par ce mécanisme, dont le CDF n'a toutefois pas pu tester l'efficacité.

Au vu de la gestion séparée des matrices de contrôles (systèmes de contrôle interne) et des contrôles compensatoires (SAP GRC), le CDF juge adéquates la définition et la gestion de ceux-ci dans SAP GRC. Des définitions plus ciblées des contrôles compensatoires pourraient être entreprises en cas de mise en œuvre du module de contrôle de processus (Process Control) de SAP GRC.

4.7 Les activités visant au contrôle des utilisateurs privilégiés doivent se poursuivre

Les utilisateurs privilégiés (utilisateurs de support, d'urgence, de customizing) ne faisaient pas partie du périmètre du projet SAP SuPro BeBe. Ils ne font donc pas pour l'instant l'objet d'analyses de violations dans SAP GRC, mais bénéficient généralement de droits d'accès étendus dans les systèmes SAP.

Sur demande du CDF, l'AFF a élaboré des lignes directrices régissant la gestion des utilisateurs privilégiés des fournisseurs de prestations (OFIT et Base d'aide au commandement). Selon la feuille de route de l'AFF, l'OFIT doit élaborer un guide et un concept de gestion des droits d'accès des utilisateurs de support et d'urgence. La mise en œuvre des processus et contrôles correspondants est prévue d'ici à fin 2017. Ces activités concernent les utilisateurs privilégiés des fournisseurs de prestations, mais pas ceux éventuellement définis chez les bénéficiaires de prestations. L'AFF prévoit de traiter ce point dans l'étude en cours d'élaboration. L'OFIT mène également diverses activités en vue de la définition et mise en place de contrôles des utilisateurs privilégiés. Des documents de travail et une analyse de l'opportunité de l'utilisation d'outils de gestion des droits privilégiés sont notamment en cours d'élaboration. L'AFF suit ces activités.

Le CDF continue de considérer le contrôle des utilisateurs privilégiés de tous les offices comme un axe de travail prioritaire. Les processus d'activation et de désactivation des droits étendus, et les modalités du suivi des utilisateurs en bénéficiant, doivent être décrits, mis en œuvre et contrôlés.

Le CDF salue les activités entreprises à cet effet mais encourage l'AFF à poursuivre ses travaux en vue d'une gestion contrôlée de ces utilisateurs et en suivra l'avancement. Par ailleurs, il poursuivra de manière renforcée ses revues des utilisateurs privilégiés dans le cadre des audits des comptes annuels et des contrôles informatiques généraux.

5 Démarrage dans les unités administratives

5.1 Le soutien de l'AFF aux activités de démarrage est adéquat

Un guide de mise en œuvre de l'AFF et ses annexes décrivent l'organisation et les processus à mettre en place en relation avec la gestion conforme des droits d'accès SAP. L'AFF a en outre organisé des ateliers pour assurer la bonne compréhension par les offices des éléments de l'organisation nécessaire. Enfin, un canal de communication avec le « Fachgruppe Compliance » et la responsable de la Compliance complète la palette des aides disponibles pour la mise en place de l'organisation et des processus requis.

Le CDF a constaté dans les trois unités administratives approchées que l'organisation préconisée par l'AFF a été mise en place. La liste centrale tenue par l'AFF des responsables d'autorisations a été complétée en conséquence. Les processus modèles décrits par l'AFF sont utilisés pour la gestion et le contrôle des droits d'accès SAP pour le périmètre convenu.

Les unités administratives sondées possèdent des collaborateurs connaissant la thématique des droits d'accès dans l'environnement SAP et ont les compétences nécessaires pour procéder aux activités de démarrage. Elles ont jugé que la formation suivie était utile, et que les documents mis à disposition par l'AFF sont compréhensibles et facilement accessibles. Ils leur permettent d'assumer correctement leur tâche.

Le CDF juge adéquat le soutien de l'AFF aux activités de démarrage des unités administratives. Il l'encourage à poursuivre sa communication sur les plateformes à disposition pour l'échange d'expériences entre les intervenants des différents offices.

5.2 Des revues plus fréquentes favorisent un contrôle efficace des violations

Le CDF a constaté que les unités administratives sont en cours de correction des conflits de droits d'accès constatés pour leurs utilisateurs. Cette étape, nommée remédiation initiale, est comprise dans les activités de démarrage. Le délai est fixé au 30 novembre 2016 et l'AFF pointe périodiquement le nombre de conflits encore non résolus par unité administrative.

Pour la résolution des conflits, les options sont les suivantes :

- correction de l'assignation d'un rôle à un utilisateur (retrait de l'assignation)
- mise en œuvre de contrôles compensatoires
- correction du rôle occasionnant le conflit (en dernier recours, puisque la mise en conformité des rôles a déjà été effectuée pendant le projet).

Après cette phase de résolution initiale, une revue périodique annuelle des droits d'accès des unités administratives avec rapport à l'attention de l'AFF est prescrite. Les départements ont la latitude de procéder à une analyse plus fréquente, à usage interne. L'AFF recommande un rythme trimestriel pour ces revues internes, mais ne les prescrit pas.

Aucun délai maximum n'est prescrit par l'AFF pour la résolution d'un conflit constaté lors d'une revue. Les unités administratives sondées partent du principe que les conflits constatés sont à corriger le plus rapidement possible. La mise en œuvre de la fonction de simulation permet dans tous les cas de notifier immédiatement l'apparition d'un conflit suite à une modification des assignations. Une identification préventive des conflits est ainsi facilitée.

Le CDF considère que les outils pour un traitement rapide des conflits sont disponibles. Il insiste en outre sur l'utilité de revues régulières et rapprochées des droits d'accès. De son point de vue, des revues trop espacées favorisent le risque qu'une violation ne soit détectée que plusieurs mois après son apparition, notamment si la fonction de simulation n'est pas utilisée. Pendant cette période, un utilisateur pourrait effectuer des transactions non autorisées. De plus, l'exécution du contrôle compensatoire, afin d'assurer qu'aucune activité illicite n'a été entreprise, devra couvrir une plus longue période et demandera plus d'efforts.

Recommandation 3 (priorité 3):

Le CDF recommande à l'AFF de préconiser aux unités administratives la mise en œuvre dès novembre 2016 de revues trimestrielles des droits à usage interne aux départements.

Prise de position de l'AFF:

Die Compliance Managerin wird der Fachgruppe Compliance empfehlen, die quartalsweise Berichterstattung über die IKS-konforme Berechtigungsverwaltung SAP auch nach der Bereinigungsphase weiterhin quartalsweise in das IKS-Reporting einfliessen zu lassen.

5.3 Un minimum à préconiser pour les concepts d'autorisation

Un concept des rôles d'autorisation SAP a été élaboré par l'AFF et décrit les rôles standards définis dans le domaine NRM („Neues Rechnungsmodell Bund"), notamment les règles régissant leur design et la convention de nommage.

En sus, l'AFF préconise l'édition par les unités administratives de concept d'autorisations spécifiques, sous la conduite du responsable des autorisations. L'AFF met à disposition un modèle dont les offices peuvent s'inspirer et qu'ils compléteront avec les points spécifiques qu'ils jugeront nécessaires. L'AFF ne teste ni ne valide les concepts des unités administratives.

Les unités administratives sondées ont toutes élaboré leur propre manuel des autorisations, se basant partiellement sur le modèle fourni par l'AFF. Dans ces unités, les documents sont soumis à un processus de validation interne, et sont mis à jour en général une fois par année. Le CDF n'a pas vérifié la qualité de ces manuels, mais prévoit de les passer en revue dans le cadre de la révision annuelle des comptes des offices.

Le CDF estime utile la mise à disposition par l'AFF d'un modèle pour les concepts d'autorisation. Constatant néanmoins que certains offices ont des versions obsolètes de ces documents, le CDF est d'avis que l'AFF devrait préconiser aux offices une validation formelle et une révision annuelle des concepts d'autorisation SAP.

Recommandation 4 (priorité 3):

Le CDF recommande à l'AFF de préconiser aux unités administratives une validation formelle et une mise à jour annuelle des concepts d'autorisation SAP.

Prise de position de l'AFF:

Die Compliance Managerin wird in ihrem Auftrag der jährlichen Risikoanalyse an die Berechtigungsverantwortlichen der VE darauf hinweisen, dass die Berechtigungskonzepte der VE aktuell gehalten werden müssen. Die Berichtsvorlage „IKS-Jahresbericht Berechtigungsverantwortlicher" wird angepasst indem die explizite Bestätigung der Aktualisierung abgefragt wird.

5.4 Un suivi plus systématique des utilisateurs extérieurs aux offices est requis

Le CDF a constaté que certains utilisateurs ont des droits de mutation dans un office, alors qu'ils sont extérieurs à cet office. Il s'agit par exemple des spécialistes du Centre de services en matière de finances du Département fédéral des finances (DFF) ou du support. En tant que propriétaires de leurs données, les offices concernés doivent pouvoir répertorier ces utilisateurs extérieurs dans le cadre de leur revue annuelle des droits d'accès. Dans sa configuration actuelle, le système SAP GRC ne permet pas l'édition de telles listes, celles-ci sont disponibles sur demande auprès de l'OFIT.
Les instructions de l'AFF relatives aux revues annuelles de droits d'accès doivent être complétées pour incorporer le suivi des utilisateurs externes aux offices.

Recommandation 5 (priorité 2) :

Le CDF recommande à l'AFF de compléter les instructions relatives aux revues annuelles de droits d'accès avec rapport. Afin d'assurer l'intégralité de ces revues, l'édition de la liste des utilisateurs extérieurs à un office avec droits de mutation dans ce dernier doit être prescrite.

Prise de position de l'AFF: Die Compliance Managerin wird ihren Auftrag der jährlichen Risikoanalyse an die Berechtigungsverantwortlichen der VE ergänzen und die Überprüfung der mutierenden Benutzer in den VE zusätzlich verlangen. Die Berichtsvorlage „IKS-Jahresbericht Berechtigungsverantwortlicher“ wird dementsprechend angepasst.

6 Entretien final

Les résultats de la révision ont été discutés le 15.7.2016. Y ont pris part le vice-directeur en charge de la division Finances et comptabilité à l'AFF, le responsable de la section Bases et pilotage des processus ainsi qu'une collaboratrice de l'unité Gestion des processus et tenue des comptes à l'AFF et, du côté du CDF, le responsable de centre de compétences 4 et le responsable de mandat.

Les résultats spécifiques à l'Administration fédérale des douanes ont été discutés le 21.7.2016 avec un groupe sous la direction de la vice-directrice en charge de la division principale Ressources à l'AFD.

Les personnes représentant l'AFF et l'AFD acceptent les recommandations émises par le CDF.

Le CDF remercie l'attitude coopérative et rappelle qu'il appartient aux directions d'office, respectivement aux secrétariats généraux, de surveiller la mise en œuvre des recommandations.

CONTROLE FEDERAL DES FINANCES

Annexe 1 : Bases légales

Directives du Conseil fédéral concernant les projets informatiques de l'administration fédérale et le portefeuille informatique de la Confédération

Loi sur le Contrôle des finances (LCF, RS 614.0)

Loi sur les finances (LFC, RS 611.0)

Ordonnance sur les finances (OFC, RS 611.01)

Ordonnance sur l'informatique dans l'administration fédérale (OIAF, RS 172.010.58)

Annexe 2 : Abréviations, glossaire, priorité des recommandations du CDF

Abréviations:

AFD	Administration fédérale des douanes
AFF	Administration fédérale des finances
CDF	Contrôle fédéral des finances
DETEC	Département fédéral de l'environnement, des transports et de l'énergie
EY	Ernst & Young, société de révision
OFIT	Office fédéral de l'informatique et des télécommunications

Glossaire:

ARA	Access Right Analysis, module du logiciel SAP GRC permettant l'analyse des droits d'accès attribués dans des systèmes SAP
Fachgruppe Compliance	Groupe de travail mené par l'AFF et traitant de questions en relation avec la conformité des processus de travail
NRM	« Neues Rechnungsmodell Bund » nouveau modèle de gestion de la Confédération, notamment dans les domaines financier et comptable
SAP	Logiciel de gestion utilisé à la Confédération, couvrant notamment la gestion des finances, de la logistique et des ressources humaines
SAP AG	Société éditrice du logiciel de gestion SAP
SAP GRC	SAP Governance, Risk and Compliance. Logiciel de contrôle de la gouvernance du risque et de la conformité édité par SAP AG
SAP SuPro BeBe	Projet de la Confédération visant à la mise en place d'une gestion conforme des utilisateurs et des droits d'accès des systèmes SAP pour les processus de support

Priorité des recommandations du CDF:

Le CDF priorise ses recommandations en se fondant sur des risques définis (1 = élevés, 2 = moyens, 3 = faibles). Comme risques, on peut citer par exemple les cas de projets non-rentables, d'infractions contre la légalité ou la régularité, de responsabilité et de dommages de réputation. Les effets et la probabilité de survenance sont ainsi considérés. Cette appréciation se fonde sur les objets d'audit spécifiques (relatif) et non sur l'importance pour l'ensemble de l'administration fédérale (absolu).