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