Kurzübersicht
Messe München GmbH,
Berechtigungen im SAP-System

Überblick zum Prüfungsgegenstand
Gerade die Geschäftsprozesse in der Finanzbuchhaltung werden immer stärker an den SAP-Funktionalitäten ausgerichtet. Da es sich bei der SAP Software um eine erweiterte betriebswirtschaftliche Anwendung handelt, kommt der Zugriffssicherheit rund um die Finanzbuchhaltung eine besondere Bedeutung zu.

Zielsetzung der Prüfung
Unsere Prüfung trägt dazu bei, dass
- bei der Berechtigungskonzeption und -umsetzung ein angemessenes und wirtschaftlich vertretbares Internes Kontrollsystem (IKS) vorhanden ist;
- ein Berechtigungskonzept vorhanden ist;
- die erteilten Berechtigungen im Produktivsystem notwendig sind;
- erforderliche Funktionstrennungen im SAP vorhanden sind.

Prüfungsergebnisse (Zusammenfassung)
- Die Berechtigungskonzeption der MMG ist dokumentiert.
- Das Notfallkonzept ist dokumentiert. Im System ist ein Notfallbenutzer eingerichtet, der den empfohlenen Anforderungen entspricht. Das Anmelden des Notfallbenutzers am 18.03.2013 war dem Grunde nach gerechtfertigt, jedoch sind die Vorgaben zur Dokumentation des Vorgangs nicht eingehalten.
- Den temporären Notfallbenutzer - nach Notfallkonzept zulässig - bewerten wir kritisch.
- Die gesetzeskritischen Sammelprofile SAP_ALL, SAP_NEW und S_A.SYSTEM identifizierten wir bei zwei technischen Dialogbenutzern als nicht zulässig. Ferner hatte sich in der Vergangenheit ein SAP-Administrator das Sammelprofil SAP_ALL mehrfach selbst zugewiesen und wieder entfernt, obwohl ein Notfallbenutzer existiert. Auch eine externe Firma verfügte kurzzeitig über das gesetzeskritische Profil SAP_ALL.
- Es sind Benutzer mit maximal kritischen Berechtigungen im System vorhanden, womit der Buchungsstoff über den ordnungsgemäßen Rahmen hinaus verändert werden kann. Die sehr restriktive Vergabe dieser Berechtigungen ist noch nicht vollständig umgesetzt.
- Obwohl die Rechteausprägung im FI-Bereich grundsätzlich geordnet ist, stellten wir Benutzer fest, deren Berechtigungen über den tatsächlichen Aufgabenbereich hinausgehen. Die kritischen Berechtigungen lassen sich im Wesentlichen zurückführen auf:
  - Rollenkollision und daraus kumulierende Berechtigungen,
  - abweichende Ausprägung eines Berechtigungsobjekts, welches die Rolle verändert hat und
  - Abteilungswechsel von Benutzern sowie vorübergehende Vertretungsfälle.

  Nicht korrekt sind ferner die sehr umfassenden FI-Berechtigungen für zwei externe Firmen und die SAP-Administratoren.
- Die MMG hat für den FI-Bereich kritische Rechtekombinationen in einer Unverträglichkeitsmatrix definiert (Funktionstrennungen). Die praktische Umsetzung der Unverträglichkeitsmatrix erfolgte bisher noch nicht so, wie im Konzept beschrieben. Im System stellten wir einzelne Benutzer mit Unverträglichkeiten fest. Zudem verfügten drei Benutzer mit den Rechten für *Bankverbindungsdaten pflegen, Fakturieren* und *Zahlen* über eine besonders risikorelevante Kombination, die zu Schwachstellen im internen Kontrollsystem führt.

Empfehlungen auf der Basis der Prüfungsergebnisse (Zusammenfassung)
- Der Einsatz des Notfallbenutzers sollte - wie im Notfallkonzept festgelegt - dokumentiert werden.

- Die Regelung zum temporären Notfallbenutzer sollte aus dem Berechtigungskonzept entfernt werden, da ein regulärer Notfallbenutzer existiert.
- Bezüglich der Rechteausprägung im SAP-System hat die SAP-Administration bereits während der Prüfung auf unsere Hinweise und Empfehlungen reagiert und sofort Anpassungen vorgenommen. Unsere Hinweise betrafen im Wesentlichen:
  - die gesetzeskritischen Sammelprofile, über die nur der Notfallbenutzer als Dialogbenutzer verfügen darf,
  - die maximal kritischen Berechtigungen, die nur sehr restriktiv vergeben werden dürfen,
  - die FI-Berechtigungen, die dem jeweiligen Aufgabenbereich des Benutzers entsprechen müssen.

  Die SAP-Administration hat uns auch zeitnah über deren Umsetzung informiert. Dadurch ist bereits ein wesentlicher Teil unserer Prüfungsfeststellungen erledigt. Auf zusätzliche Empfehlungen haben wir in diesen Punkten verzichtet.
  In Einzelfällen waren jedoch unsere Empfehlungen nicht sofort umsetzbar, aufgrund der hohen Komplexität der Berechtigungsvergabe und aus ressuorcentechnischen Gründen, was wir nachvollziehen können. Hier sollten noch Anpassungen erfolgen.
- Zusätzlich sollten die Fachbereiche an ihre Meldepflicht beim Abteilungswechsel von Benutzern erinnert werden. Ergänzend ist eine regelmäßige Abstimmung zwischen SAP-Administration und den Fachbereichen über die Rollenzuordnung je Benutzer möglich.
- Für das Umsetzen der Unverträglichkeitsmatrix muss der Fachbereich noch entscheiden, ob er künftig Ausnahmen zulässt und wenn ja, die Einzelfälle genehmigen und die Benutzer dokumentieren. Für Unverträglichkeiten mit der Berechtigung *Debitoren* bzw. *Kreditoren Zahlen* sollten, aufgrund ihrer Risikorelevanz, generell keine Ausnahmen zugelassen werden. Das SAP-System sollte regelmäßig auf Unverträglichkeiten geprüft werden.

Stellungnahme der geprüften Organisationseinheit (Zusammenfassung)
Die MMG folgt unseren Ergebnissen und Empfehlungen. In der Schlussbesprechung zum Berichtsentwurf wie auch in der Stellungnahme zum AGAM-Bericht erläuterte sie umfassend ihre Lösungsansätze und geplanten Maßnahmen. Sie beabsichtigt in allen Punkten eine sehr zeitnahe Umsetzung. Hierzu hat sie eine Risikobewertung durchgeführt und zeitliche Umsetzungsprioritäten mit ein bzw. zwei Monaten, bei einer Maßnahme mit drei Monaten, festgelegt.

Der Rechnungsprüfungsausschuss übernimmt die Prüfungsergebnisse und trägt die Empfehlungen des Revisionsamts mit.