SOX-PRÜFUNG DER SAP-BASIS DURCH IT-ABTEILUNG AUF KNOPFDRUCK

Früher dauerte die quartalsweise vorgeschriebene SOX Basisprüfung bei Caterpillar Energy Solutions regelmäßig rund zwei Arbeitstage. Heute entsteht ein Sarbanes-Oxley Act Prüfbericht für das Management auf Knopfdruck. Der Zeitaufwand hat sich auf 30 Minuten reduziert, und zusätzlich können die SAP-Administratoren des Unternehmens viel besser einschätzen, wo Risikopotenziale bei der Vergabe von SAP-Rollen und SAP-Berechtigungen liegen.

Das ist nicht nur für die Administration der rund 1.200 eigenen SAP-Benutzer wichtig, sondern auch für die Rechtevergabe an Externe, die beim Betrieb, Support und der Weiterentwicklung des SAP-Systems helfen. Die IT-Abteilung entschied sich für den Einsatz des Tools „CheckAud® for SAP Systems“ der IBS Schreiber GmbH. Es wird bereits mit Standard-Regelwerken ausgeliefert, die zwei Mal im Jahr aktualisiert werden, und die sich von den Kunden eigenständig individualisieren lassen.

IT-Abteilung braucht sicheres SAP-System

Caterpillar Energy Solutions produziert Gasaggregate zur Stromerzeugung sowie Kraft-Wärme-Kopplungs-Anlagen und realisiert Kraftwerksprojekte. Vom Firmensitz in Mannheim aus wird das dafür notwendige SAP-System für rund 1.200 SAP-Anwender in acht Auslandsniederlassungen, diversen Servicecentern und der Zentrale in Deutschland verantwortet. Das SAP-System wird mit nahezu allen SAP-Modulen genutzt. Zudem haben auch externe Anwender einen Systemzugriff, um zwecks Support und Beratung bei verschiedenen IT-Themenstellungen zu unterstützen.

„Dabei den Überblick über die regelkonforme Rollen- und Berechtigungsvergabe zu behalten, ist wahnsinnig schwer“, erläutert Oliver Klamm, Leiter IT Application Management bei Caterpillar Energy Solutions. Da Basisprüfungen unter anderem Gegenstand von quartalsweisen SOX- und jährlichen Finanzabschlussprüfungen sind, entschied sich das Unternehmen für ein Werkzeug, das die regelmäßig anfallenden manuellen Aufwände reduzieren kann. Gleichzeitig kann der IT-Bereich sicherstellen und nachweisen, dass alle gesetzlichen und unternehmenseigenen Vorgaben eingehalten werden.

IBS Prüfen mit Konzept

Aufwand von zwei Tagen auf dreißig Minuten reduziert

„Bei den SOX-Basisprüfungen müssen wir 25 Richtlinien prüfen und erfüllen. Eine Richtlinie kann bis zu 30 SAP-Transaktionen betreffen, die ich früher manuell prüfen und mit Screenshots in einem Prüfprotokoll dokumentieren musste. In Summe dauerte alleine die Prüfung etwa zwei Arbeitstage pro Quartal“, blickt Oliver Klamm zurück. „Heute kann ich jederzeit eine Prüfung auf Knopfdruck durchführen. Sie dauert etwa 30 Minuten, und ich bekomme einen automatisierten Bericht, der das Scoring unserer 25 Prüfkriterien enthält“, freut sich Oliver Klamm.

Das Projekt: In wenigen Schritten zum Ziel

So kam es zu dieser Beschleunigung: Caterpillar Energy Solutions prüfte probehalber einmalig das Berechtigungswesen seines SAP-Systems mit CheckAud® von IBS Schreiber. Eine Standardprüfung von Systemeinstellungen und Systemparametern gegen den DSAG-Prüfleitfaden, den DSAG-Datenschutzleitfaden, HGB-, DSGVO- und andere gesetzlich verbindliche Vorgaben ist mit den mitgelieferten Standardregelwerken möglich. Über 2.500 Abfragen sind bereits vordefiniert, sie werden zwei Mal im Jahr von IBS Schreiber an Gesetzesänderungen und Neuerungen in den SAP-Systemen angepasst. Nach der Analyse der Auswertungen entschied sich Caterpillar für den Kauf der Lösung - auch eine Miete wäre möglich gewesen. In einem zweitägigen Workshop wurde der gesamte Anforderungskatalog von 25 Regelprüfungen, bei denen in Summe mehr als 100 SAP-Transaktionen betroffen sind, umgesetzt. Ergebnis des Workshops mit CheckAud® war ein Regelwerk, mit dem Caterpillar sein SAP-System permanent auf Compliance überwachen kann. Seit Abschluss der ersten Prüfung arbeitet das SAP-Anwenderunternehmen Caterpillar eigenständig mit der IBS Schreiber-Lösung. „Die mitgelieferten Regelwerke waren zur Auswahl der SAP-Basisabsicherung und als Vorlage für eigene Regeln sehr hilfreich. Wir haben gelernt, wie man eigene Regelwerke anlegen und modifizieren kann. Im ersten halben Jahr der produktiven Nutzung, haben wir - mit wenig Aufwand - bereits dreimal das Regelwerk angepasst, weil sich die Vorgaben aus den USA geändert haben“, berichtet Oliver Klamm.

Nebeneffekt: Bessere Risikoeinschätzung bei Rollen und Berechtigungen

Besonders wertvoll war für Oliver Klamm die Lernkurve zum SAP-Berechtigungswesen und unbekannteren SAP-Transaktionen, insbesondere auch durch die umfassenden Dokumentationen der Regeln. Heute kann die Unternehmens-IT - nach eigenen Angaben - die Risiken bei der Vergabe von Berechtigungen an Interne und Externe viel besser abschätzen, hat höhere Transparenz zu den vorgefertigten SAP-Rollen und vergibt Berechtigungen von vornherein restriktiver. Im Projektverlauf konnten daraufhin viele Berechtigungen eingeschränkt werden, weil sie nicht notwendig waren - oder mussten eingeschränkt werden, da die Prüfung ergab, dass beispielsweise Kombinationen nicht erlaubt sind.

Ergebnis: SOX-Prüfung auf Knopfdruck

Von den mehr als 2.500 mitgelieferten CheckAud® Prüfabfragen betreffen über 100 Prüfabfragen kritische Berechtigungskombinationen in Purchase-to-Pay- und Order-to-Cash-Prozessen, der Logistik und der Finanzbuchhaltung, um die Funktionstrennung zu gewährleisten. Jede SoD-Prüfabfrage (Segregation of Duties) enthält detaillierte Aussagen zu betriebswirtschaftlichen, handelsrechtlichen, IT-sicherheitsspezifischen und datenschutzrechtlichen Risiken. Bezüglich der Systemeinstellungen wird beispielsweise geprüft, ob es Entwicklerschlüssel oder „SAP_ALL"-Berechtigungen im Produktivsystem gibt und ob System und Mandant gegen Änderungen gesperrt sind. Ferner wird geprüft, ob alle Systemparameter den Vorgaben entsprechen. Wenn Oliver Klamm heute eine CheckAud®-Prüfung startet, bekommt er eine Übersicht der SAP-Berechtigungen und detaillierte Risikobeschreibungen. Für jeden Prüfbereich und für das SAP-Gesamtsystem werden Risiko-Scores berechnet und als Dashboard dargestellt. „In komplexen SAP-Systemlandschaften sind auch systemübergreifende oder mandantenübergreifende Prüfungen nötig und möglich", ergänzt Lisa Niekamp vom Anbieter IBS Schreiber. „In besonders sicherheitskritischen oder sehr dynamischen SAP-Landschaften kann sogar eine kontinuierliche Auditierung aktiviert werden, um bei Änderungen potenzielle Risiken schnell zu erkennen und zu beheben."

Compliant bleiben: Regelwerk mit Content Service

Die Komplexität des SAP-Berechtigungswesens steigt kontinuierlich, da der Hersteller viele Innovationen und Änderungen in die SAP-Lösungen bringt. Auch die gesetzlichen Vorgaben unterliegen einem kontinuierlichen Wandel. Für CheckAud® wird ein Updateservice angeboten, damit ständig aktualisierte Regelwerke genutzt werden können, die diese Änderungen berücksichtigen. Durch eine Partnerschaft mit SAP haben übrigens alle „SAP Access Control"-Kunden die Möglichkeit, die IBS Schreiber Regelwerke und den zugehörigen Content Service zu nutzen. Sie können damit die eigenen Regelwerke im „SAP Access Control" mit dem CheckAud®-Katalog von über 2.500 vorgefertigten Prüfabfragen ergänzen und die Absicherung der SAP-Basis und der Geschäftsprozesse verbessern. Die Belange der Fachbereiche, die in der Regel die Hauptverantwortung für die Compliance der Geschäftsprozesse tragen, werden durch den Einsatz von CheckAud® unterstützt. In vielen Unternehmen nutzt auch die Revision das Produkt, weil für qualitative Prüfungen ständig aktuelles und gleichzeitig tiefgehendes Expertenwissen notwendig ist. Mit der kontinuierlichen Pflege der Regelwerke bekommen IT-Abteilungen und Revisoren dieses Wissen prüfungsfertig geliefert.

Fazit

„Der mit IBS Schreiber durchgeführte CheckAud®-Workshop hat sich besonders rentiert. Unser Know-how, die Transparenz und die Sensibilität zum SAP-Berechtigungswesen hat sich dadurch deutlich verbessert", fasst Oliver Klamm die Projektarbeit zusammen. „Den Einsatz der Lösung und einen derartigen Workshop würde ich anderen Unternehmen unbedingt empfehlen." Oliver Klamm sieht für Caterpillar Energy Solutions die quartalsweise Zeitersparnis, den internen Know-how-Aufbau zur SAP-Sicherheit und die automatisierten Reports auf Knopfdruck als Hauptvorteile der Lösung.

CheckAud®
for SAP Systems

IBS Schreiber GmbH · www.ibs-schreiber.de

IBS Schreiber GmbH
International Business Services for Auditing and Consulting
Zirkusweg 1 | 20359 Hamburg
Fon: +49 40 69 69 85-82 | Fax: +49 40 69 69 85-31
sales@ibs-schreiber.de | www.ibs-schreiber.de