SAP-Sicherheitsüberwachung und IKS

Sie wollen sich für die interne Revision wappnen oder proaktiv auf den nächsten Besuch des Wirtschaftsprüfers vorbereiten? In jedem Fall sollten Sie die Ordnungsmäßigkeit ihres SAP-Systems und die korrekte Umsetzung ihres SAP-Sicherheitskonzepts sicherstellen und überwachen.

Stetig ändernde Anforderungen aus den Fachbereichen sorgen für eine Dynamik im System und erschweren eine kontinuierliche Überprüfung der konzeptionellen Compliance-Vorgaben aus dem Berechtigungskonzept. Mit der Etablierung eines internen Kontrollsystems decken sie Mängel auf und erkennen so frühzeitig Sicherheitsprobleme, um ihr SAP-System proaktiv zu schützen.

Mit unserem Service zur Überwachung von SAP-Sicherheitsvorgaben implementieren wir ein internes Kontrollsystem (IKS) und ermöglichen Ihnen die Gesamtheit ihrer SAP-Sicherheitsvorgaben zentral zu überprüfen.

UNSERE DIENSTLEISTUNG – SCHRITT FÜR SCHRITT

1. **Vorbereitungen und Analyse der bestehenden Sicherheitsrichtlinien**
   - Vorbereitende Maßnahmen am SAP-System und Implementierung des Security Architects
   - Analyse und Reflektion der bestehenden Sicherheitsrichtlinien
   - Überarbeitung und Definition neuer Maßnahmen und Aufnahme eventueller Vorgaben aus dem Audit
2. **Implementierung der Sicherheitsrichtlinien und Customizing des Security Architects**
   - Pflege und Customizing der Sicherheitsrichtlinien im Security Architect
   - Optional: Einrichtung und Implementierung einer zentralen Überprüfung über die komplette Systemlandschaft
   - Optional: Automatisierte periodische Überprüfung mit E-Mail-Benachrichtigung
3. **Abschließende Aufgaben**
   - Einweisung/Schulung zur Bedienung des Security Architects
   - Erstellen einer Abschlussdokumentation und Übergabe

XAMS-WEBINARE

Get clean – stay clean!
Erfahren Sie in unseren kostenlosen Webinaren mehr über die produktive Testsimulation mit XAMS während des normalen Arbeitsablaufes!

ITing quality

SAP-Sicherheitsüberwachung und IKS

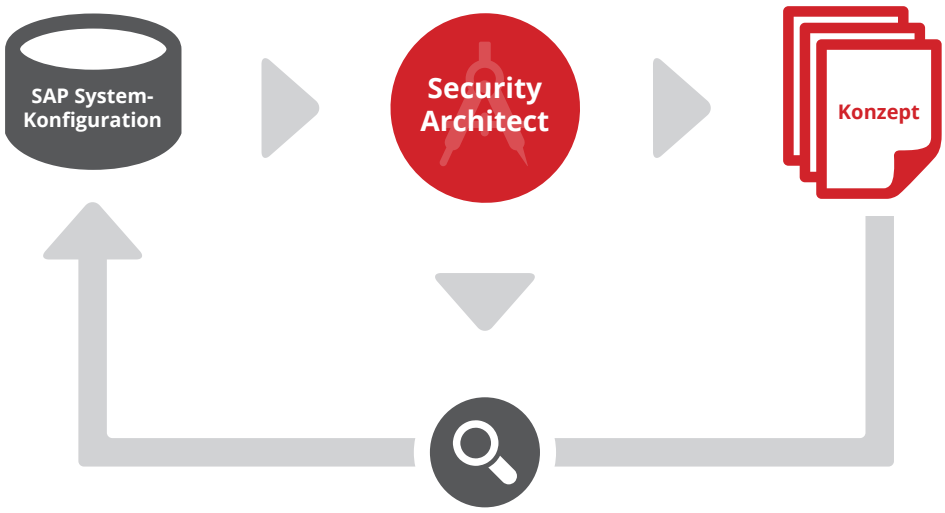
CHECK-MODE – AUFBAU EINES IKS MIT DEM SECURITY ARCHITECT

Mit dem Security Architect werden Best Practice Vorlagen für ein Sicherheitskonzept ausgeliefert, die leicht an Kundenbedürfnisse angepasst oder um diese erweitert werden können. Das Konzept kann direkt aus dem System heraus generiert werden. Im Umkehrschluss können wir ihre gewünschte oder bereits bestehende Systemkonfiguration im Security Architect abbilden.

So können bereits bestehende Systemvorgaben wie Systemparameter, kritische Profile, Mandanteneinstellungen u.v.m. im Security Architect hinterlegt und fortan automatisch überprüft werden.

Die Überprüfung erfolgt über den sogenannten Check-Mode im Security Architect und kann ebenfalls von einem Zentralsystem (z.B. Solution Manager) für alle angeschlossenen Systeme durchgeführt werden. Die einheitlichen Prüfungsergebnisse können revisionskonform gespeichert werden und geben Ihnen die Möglichkeit ihren Soll-Zustand des Systems mit dem derzeitigen Ist-Zustand zu vergleichen.

Unsere Berater analysieren die Ist-Situation und optimieren ihre Sicherheitsvorgaben mithilfe des Security Architects effizient und gemäß Best Practice Empfehlungen, die sich unter anderem am DSAG-Prüfleitfaden orientieren.



AUF EINEN BLICK:

- Ein automatisiertes internes Kontrollsystem, das dauerhaft ihren Systemzustand überwacht
- Erhöhung der Sicherheit und Einhaltung von Compliance-Vorgaben durch die Kontrolle von Sicherheitsvorgaben und dem regelmäßigen Abgleich des Soll-Zustandes mit dem Ist-Zustand
- Die Möglichkeit systemspezifische Sicherheitsvorgaben zentral von einem System zu kontrollieren

Weiterführende Informationen & Webinare unter **www.xiting.ch**

SAP Silver Partner

Tel: +49 7656 9888 155
Email: info@xiting.de

Tel: +41 43 422 8803
Email: info@xiting.ch

Tel: +44 1454 838785
Email: info@xiting.uk.com

Tel: +1 (813) 9022226
Email: info@xiting.us