SAP-Rollen und Berechtigungen

Self-Check: 11 Fragen zu Transparenz, Verantwortlichkeiten und Kontrollen

Für Verantwortliche aus SAP, IT und Fachbereich. Ohne Systemzugriff beantwortbar.

So antworten Sie: Je Frage eine Antwort. „Ja“ nur, wenn alle genannten Aspekte erfüllt und belegbar sind. „Teilweise“ bei lückenhafter, „Nein“ bei fehlender Umsetzung. „Unklar“ bei fehlendem Wissen oder Nachweis.

Rollenmodell und Verantwortlichkeiten	Ja	Teilw.	Nein	Unklar
1. Wird regelmäßig und bei wesentlichen Änderungen überprüft, ob die Rollen noch zu den Aufgaben und Zuständigkeiten passen?	☐	☐	☐	☐
2. Ist für jede Rolle klar, welchem Zweck sie dient und wer fachlich bzw. technisch dafür verantwortlich ist?	☐	☐	☐	☐
3. Werden Nutzungsdaten und der aktuelle Rollenbestand regelmäßig ausgewertet, um nicht mehr benötigte Rollen und Berechtigungen zu identifizieren und zu bereinigen?	☐	☐	☐	☐

> ***Achtung:*** *Schrittweise Erweiterungen lassen eine passende Rolle über ihren fachlichen Zweck hinauswachsen.*

Vergabe und regelmäßige Überprüfung	Ja	Teilw.	Nein	Unklar
4. Werden Rollenänderungen und Benutzerzuordnungen nachvollziehbar beantragt und durch zuständige Verantwortliche freigegeben?	☐	☐	☐	☐
5. Bestätigen die Verantwortlichen regelmäßig, dass Benutzer ihre zugewiesenen Rollen weiterhin benötigen?	☐	☐	☐	☐
6. Werden bei Aufgabenwechsel oder Austritt nicht mehr benötigte Berechtigungen zeitnah entzogen?	☐	☐	☐	☐

> ***Achtung:*** *Eine Rollenbestätigung sagt wenig aus, wenn Verantwortliche die enthaltenen Zugriffe nicht beurteilen können.*

Risiken und Kontrollen	Ja	Teilw.	Nein	Unklar
7. Haben Sie einen aktuellen Überblick über kritische Berechtigungen und Funktionstrennungskonflikte (SoD)?	☐	☐	☐	☐
8. Werden erkannte Risiken fachlich bewertet und ihre Bereinigung oder begründete Akzeptanz nachvollziehbar dokumentiert?	☐	☐	☐	☐
9. Sind für akzeptierte Risiken erforderliche Kontrollen festgelegt, deren Durchführung und Wirksamkeit regelmäßig überprüft werden?	☐	☐	☐	☐
Achtung: *Eine SoD-Trefferliste zeigt mögliche Konflikte. Welche davon tatsächlich relevant sind, erfordert eine fachliche Bewertung.*				

SoD bezeichnet unvereinbare Tätigkeiten, z. B. Lieferantenstammdaten pflegen und Zahlungen ausführen.

Transparenz und privilegierte Zugriffe	Ja	Teilw.	Nein	Unklar
10. Wissen Sie, welche Benutzer einschließlich technischer Benutzer weitreichende Rechte haben (etwa Benutzerverwaltung, Datenänderung in Produktion) und warum?	☐	☐	☐	☐
11. Werden Notfallzugriffe genehmigt, zeitlich begrenzt und nachträglich auf ihre Nutzung überprüft?	☐	☐	☐	☐
Achtung: *Bei technischen Benutzern bleiben Verantwortlichkeit und benötigter Berechtigungsumfang leicht ungeklärt.*				

Was Ihre Antworten zeigen

5 und mehr Antworten - Teilweise oder Nein: Hier bestehen nach Ihrer Einschätzung Lücken. Markieren Sie die Punkte, deren Auswirkungen Sie genauer klären möchten. Liegen Ihre Lücken vor allem beim Rollenmodell, dessen regelmäßiger Überprüfung, bei kritischen Berechtigungen oder bei weitreichenden Zugriffen, betrifft das meist das Rollenmodell selbst. Bei den übrigen Fragen fehlt eher die Steuerung eines grundsätzlich tragfähigen Modells.

5 und mehr Antworten - Unklar: Klären Sie mit den Verantwortlichen, wie der aktuelle Stand belegt werden kann.

Durchgehend Ja: Die abgefragten Aspekte sind nach Ihrer Einschätzung geregelt. Ob die tatsächlichen Berechtigungen dazu passen, bleibt gesondert zu prüfen.

Ihr nächster Schritt

Sie haben offene Punkte identifiziert? Besprechen Sie Ihren ausgefüllten Self-Check mit uns. Gemeinsam ordnen wir die Punkte ein und klären, welcher Umfang für einen SAP-Berechtigungs-Health-Check sinnvoll ist.

IHR KONTAKT

Michael Müllner
Managing Partner
T +43 (0) 676 9398 461
M michael.muellner@akquinet.de