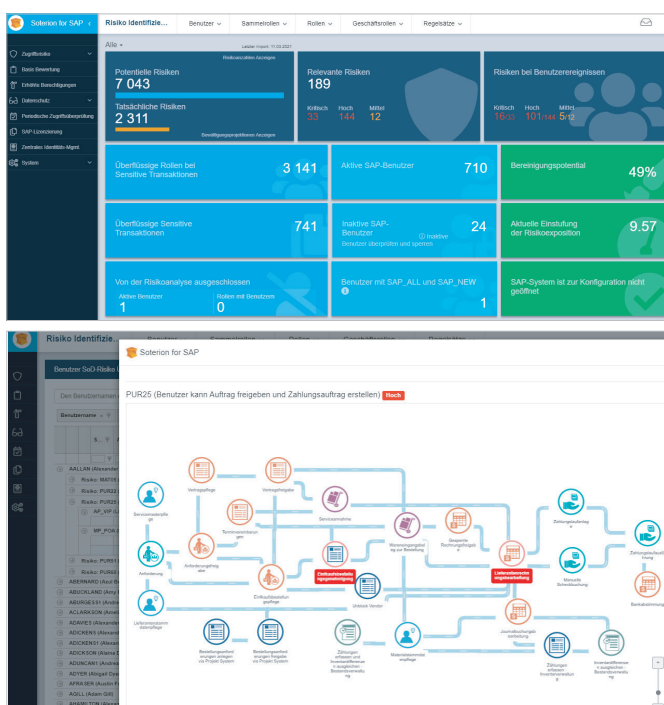


# ZUGRIFFSRISIKO-MANAGER



## Zugriffsrisiko-Manager: Risiko identifizieren



Gewinnen Sie Einblick in Ihre SAP-Zugriffsrisiken mit geschäftsfreundlicher Berichterstattung.

### SAP-Zugriffsrisiko-Analyse – Transaktionsnutzung miteinbezogen

Soterion für SAP analysiert Benutzerberechtigungen und unterscheidet zwischen den potentiellen und den tatsächlichen Zugriffsrisiken mittels Einbeziehung der historischen Transaktionsnutzungsdaten des Benutzers.

### Geschäftsfreundliche SAP-Zugriffsrisiko Berichterstattung

Soterion für SAP ermöglicht es der Organisation, Daten aus allen Blickwinkeln zu betrachten, indem sie eine Drag & Drop-Funktionalität zum Gruppieren und Filtern verwendet. Grafische Übersichten zeigen die Zugriffsrisikolandschaft der Organisation, inkl. Hochrisikobereiche, in Bezug auf Risikotoleranz und den Grad der Risikobereitschaft. Berichterstattung über SAP-Zugriffsrisiken auf Abteilungsebene erleichtert die Bestimmung der Eigentumsverantwortung.

### Berichterstattung über Geschäftsprozessflüsse

Ergänzende Geschäftsprozessflussdiagramme liefern mehr Kontext zum Zugriffsrisiko und wandeln die technische GRC-Sprache in eine geschäftsfreundliche Sprache um, um eine bessere Entscheidungsfindung zu gewährleisten.

## Zugriffsrisiko-Manager: Bereinigen

SAP-Zugriffsrisiken beseitigen ohne nennenswerte Betriebsunterbrechung, mithilfe leistungsstarker Datenanalyse.

### Auflösungskonzentrierte Gap-Analyse-Berichterstattung

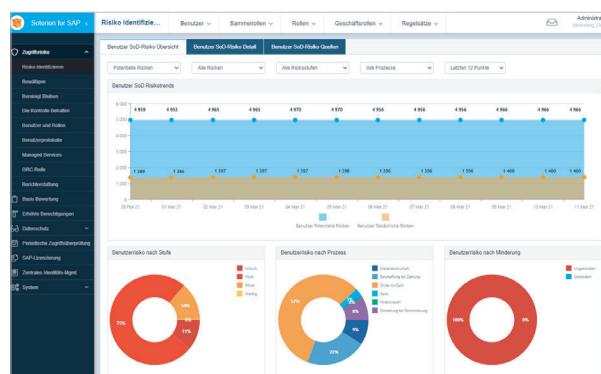
Soterion für SAP führt eine Gap-Analyse durch, um das potentielle SAP-Zugriffsrisiko von dem tatsächlichen SAP-Zugriffsrisiko in Ihrem Berechtigungsumfeld zu unterscheiden. Das Identifizieren und Auflösen von diesem überflüssigen Zugriff gilt als erster Schritt zur Steuerung Ihrer SAP-Berechtigungslandschaft. Überflüssiger Benutzerzugriff kann dann ohne Betriebsunterbrechung beseitigt werden, was es dem Unternehmen ermöglicht, sich auf das tatsächliche Zugriffsrisiko zu konzentrieren. Überflüssige Benutzerzugriffe tragen typischerweise zu 80% der Zugriffsrisiken in einem SAP-System bei.

### SAP-Zugriffsrisiko Bewältigungsprojektion

Die Risiko-Bewältigungsprojektion Ansicht schätzt ab, in welchem Maße Ihre SAP-Berechtigungslösung mittels der Methodik von Soterion für SAP bereinigt werden kann. Die Bereinigungsmaßnahmen konzentrieren sich zunächst auf die Beseitigung des ungenutzten Zugriffs, der zu Risiken beiträgt, was erhebliche Risikosanierungen mit minimalen Auswirkungen auf das Geschäft gewährleistet.

### Risiko-Bereinigungsassistenten

Die Assistenten zur Risikobereinigung bieten klare, fokussierte und schrittweise Vorschläge zur Beseitigung von Zugriffsrisiken, von der Entfernung überflüssiger Zuordnungen bis hin zur Aufteilung von Rollen auf der Grundlage von Rollenverwendungsanalysen.



## Bereinigen: Benutzerrisiko-Übersicht

Der Großteil des Zugriffsrisikos in einer SAP-System wird durch Funktionen, die einem Benutzer zwar zugeordnet sind, aber nicht genutzt werden, verursacht. Mit der Gap-Analyse-Funktionalität von Soterion für SAP können Sie Ihre Berechtigungslösung an den wirklichen Aktivitäten der Benutzer im System ausrichten und sich auf das tatsächliche Zugriffsrisiko in Ihrer SAP-Umgebung konzentrieren.

## Zugriffsrisiko-Manager: Bereinigt bleiben

Simuliert "Was-wäre-wenn" - Szenarien, vor Änderungen in SAP durchgeführt werden – Genehmigung erfolgt über Workflow.

### Simulationen der Zuweisungen und "Was-wäre-wenn" - Analyse

Soterion für SAP ermöglicht die Simulation von SAP-Berechtigungsänderungen vor sie in SAP durchgeführt werden. Durch die Einbindung von Benutzertransaktions-Nutzungshistorie ist das Unternehmen in der Lage, bessere Zugriffsrisikoentscheidungen zu treffen. Die Änderungskontrolle gewährleistet die geschäftliche Genehmigung von Berechtigungsänderungen sowie die Risikoauswirkung.

### Vorkonfigurierter Regelsatz, der vollständig benutzerdefinierbar ist

Soterion für SAP wird mit einem vorkonfigurierten Zugriffsrisiko-Regelsatz bereitgestellt, der auf Best Practices in allen Branchen basiert ist. Der Regelsatz ist leicht anpassbar, um den spezifischen Bedürfnissen eines Unternehmens entsprechen zu können.

### Kontrollen zur Risikominderung

Die einzigartige Gap-Analyse-Funktionalität von Soterion für SAP ermöglicht es dem Unternehmen, sich auf die Minimierung der tatsächlichen SAP-Zugriffsrisiken zu konzentrieren. Der Geschäftsbetrieb kann den Status der identifizierten Risiken grafisch einsehen. Die Kontrollenbibliothek ist ein zentrales Repository für Kontrollen zur Risikominderung, das es dem Unternehmen ermöglicht, Zugriffsrisiken durch Standardkontrollen und Workflow-Funktionen einfach und effektiv zu minimieren.

The screenshot shows the 'Simulator' interface with three tabs: 'Typ', 'Simulation-Auswahl', and 'Ergebnisse'. The 'Simulation-Auswahl' tab is active. It features a form titled 'Benutzer der Rolle zuordnen' with the following fields: 'Rolle auswählen' (set to 'ZF\_AP\_PAYMENT\_RUN\_MINT\_ALL'), 'Benutzer zuordnen' (set to 'ADAVIES (Alexander Davies)'), 'Gültig ab' (set to '29.07.2021'), and 'Gültig bis' (set to '31.12.9999'). There are buttons for 'Werte Löschen' and 'Simulation ausführen'.

Simulation

The screenshot shows the 'Simulation Ergebnisse' view. It displays a summary table with columns for 'Rolle', 'Benutzer', and 'Risikoänderung'. The role is 'ZF\_AP\_PAYMENT\_RUN\_MINT\_ALL (AP - Payment Run Create and Change (FTR))' and the user is 'ADAVIES (Alexander Davies)'. The risk change is '6 hoch'. Below the summary, there is a 'Detail' section titled 'Dieser Antrag verursacht neue Risiken' listing several risks with their descriptions and 'hoch' severity levels.

Simulation Ergebnis

## Bereinigt bleiben: Zuweisung-Simulator

Stellen Sie sicher, dass die SAP-Berechtigungslösung auch in Zukunft bereinigt bleibt, indem Sie die Zuordnungen simulieren, bevor Sie diese Änderungen im SAP System vornehmen. Der Zuweisung-Simulator von Soterion für SAP erkennt, ob durch diese Änderungen neue SAP-Zugriffsrisikoverstöße entstehen werden. Diese Änderungen können per Workflow zur Genehmigung versendet werden, so dass das neue Risiko vom Unternehmen akzeptiert wird, aber auch damit Prüfprotokolle für Änderungen und Risiken erstellt werden können.