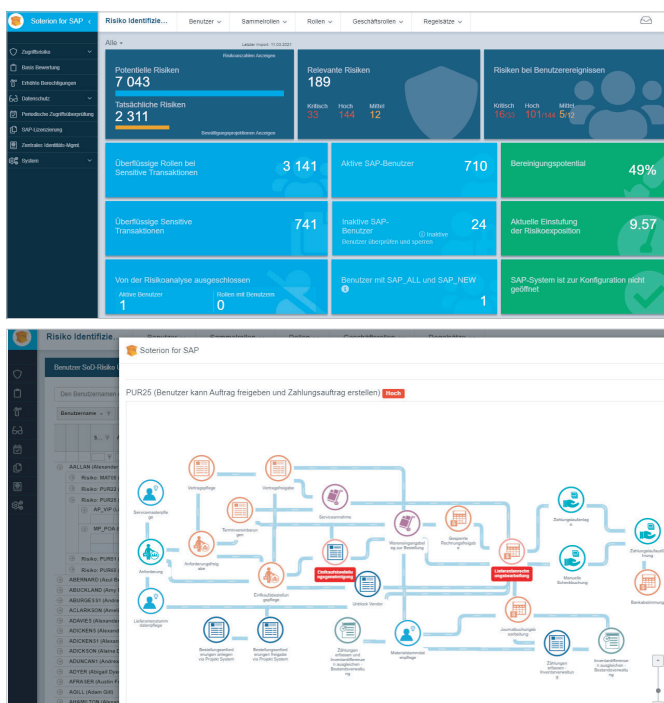


ZUGRIFFSRISIKO-MANAGER



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 Benutzertransaktion-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 displays a form titled 'Benutzer der Rolle zuordnen' (Assign user to role). The form includes fields for 'Rolle auswählen' (Role selection) with the value 'ZF_AP_PAYMENT_RUN_MINT_ALL', 'Benutzer zuordnen' (User assignment) with the value 'ADAVIES (Alexander Davies)', 'Gültig ab' (Valid from) with the date '29.07.2021', and 'Gültig bis' (Valid until) with the date '31.12.9999'. There are buttons for 'Werte Löschen' (Reset values) and 'Simulation ausführen' (Execute simulation).

Simulation

The screenshot shows the 'Simulator' interface with the 'Ergebnisse' (Results) tab active. It displays a summary section titled 'Zusammenfassung' (Summary) with a warning icon and the text 'Führt Zu Neuem Risiko' (Leads to New Risk). The summary shows the role 'ZF_AP_PAYMENT_RUN_MINT_ALL (AP - Payment Run Create and Change (FTR))' and the user 'ADAVIES (Alexander Davies)'. A risk change indicator shows a red circle with the number '6' and the word 'hoch' (high). Below the summary is a 'Detail' section titled 'Dieser Antrag verursacht neue Risiken' (This request causes new risks). It lists several risks with their descriptions and a 'hoch' (high) risk level indicator. The risks listed are: PUR47.2 (User is able to purchase unauthorized items & make payment by executing the payment run), PUR20.2 (User is able to receive/accept services & make payment by executing the payment run), PUR23.2 (User is able to approve purchase of unauthorized items & make payment by executing the payment run), FIN22 (Benutzer kann Zahlung entsperren und dann Zahlung ausführen), SL227 (Benutzer kann Kundengutschriften bearbeiten und Debitorenzahlungen erstellen), and CT_P107 (Prüfische Transaktionen FINANZWESEN: Maschinelle Zahlung / Scheckzahlungen).

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.

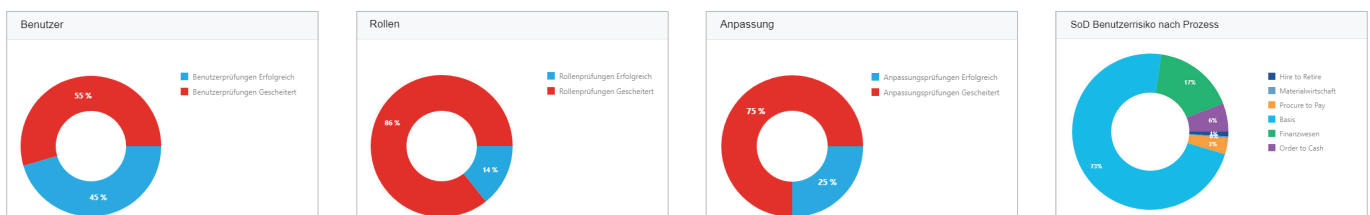
BASIS-PRÜFUNG-MANAGER



Prüfung der SAP-Basis-Konfiguration, um Konformität zu gewährleisten

Die SAP-Basis-Konfigurationen stellen auf Systemebene Kontrollen auf, um ein SAP-System abzusichern. Diese Konfigurationseinstellungen können so eingestellt werden, dass sie Ihren spezifischen Sicherheitsanforderungen entsprechen. Der Soterion Basis-Prüfung-Manager überprüft Ihre SAP-Basis-Konfiguration anhand von Regeln, die auf Industrie Best Practices basieren. Da diese Konfigurationen in der Regel Bestandteil eines jährlichen externen Audits sind, können Sie mit unserem Basis-Prüfung-Manager vorbereitet sein und es wird eine vollständige Compliance erstellt zur Vermeidung von nachteiligen Prüfungsfeststellungen.

Der Basis-Prüfung-Manager besteht aus einer Reihe von Prüfungen, die gegen Ihr SAP-System ausgeführt werden können. Die Ergebnisse werden entweder als bestanden oder als nicht bestanden markiert, mit der Option, die nicht bestandene Ergebnisse zu mäßigen. Beispiele von typischen Prüfungen sind:



Parametereinstellungen (RSPARAM)

- ✓ Kennwortlänge, -ablauf und -komplexität
- ✓ Einschränkung der Mehrfachanmeldung
- ✓ Untersuchung der Tabellenprotokollierung

Rollekontrollen

- ✓ Rollen, die zwar im Produktion System liegen, aber den Benutzern nicht zugeordnet sind
- ✓ Rollen, die im Produktion System angelegt oder geändert wurden
- ✓ Rollen mit Transaktionsplatzhaltern

Benutzerkontrollen

- ✓ Benutzer, die Entwicklerschlüssel im Produktion System haben
- ✓ Testbenutzer, die im Produktion System arbeiten
- ✓ Benutzer, die SAP-Standardrollen im Produktion System haben

| Regel-Identifikator | Name | Beschreibung | Aktiviert | Ergebnis |
|---------------------|---|--|-----------|---------------|
| C.100 | Inadequate Parameter (RSPARAM) settings | Identify inadequate parameter (RSPARAM) settings | ✓ | ✗ Gecheitert |
| C.102 | Non productive Company codes | Identify non productive Company Codes | ✓ | ✗ Gecheitert |
| C.104 | Prohibited Passwords | Identify prohibited passwords (from table USR40) | ✓ | ✗ Gecheitert |
| C.106 | SCC4 Client Settings | SCC4 Client Settings | ✓ | ✓ Erfolgreich |
| C.107 | List of critical tables being logged (esp T000) | List of tables that should be logged | ✓ | ✗ Gecheitert |
| C.114 | List of locked transaction codes | List of transactions that should be locked | ✓ | ✗ Gecheitert |
| C.117 | Custom programs without authorization group | Identify custom programs that have not been assigned to an authorization group | ✓ | ✗ Gecheitert |
| C.118 | Custom tables without authorization group | Identify custom tables that have not been assigned to an authorization group | ✓ | ✓ Erfolgreich |

ERHÖHTE- BERECHTIGUNGS-MANAGER



Genehmigung sensibler Zugänge in einer sicheren und strukturierten Umgebung

Von Zeit zu Zeit benötigen Kunden temporären oder Notfallzugang für einen begrenzten Zeitraum – oft auch „Firefighter“-Zugang genannt. Unsere neue Funktion ermöglicht Ihnen dies mühelos und unter Einhaltung der Audit-Anforderungen. Der Erhöhte-Berechtigungen-Manager von Soterion genehmigt sensiblen Zugang in einem automatisierten Workflow-gesteuerten Prozess und ermöglicht Ihrem Managementteam eine strukturierte Überprüfung aller Tätigkeiten, die während des Zeitraums für den Zugang mit erhöhten Berechtigungen ausgeführt wurden.

Unser Vorgang

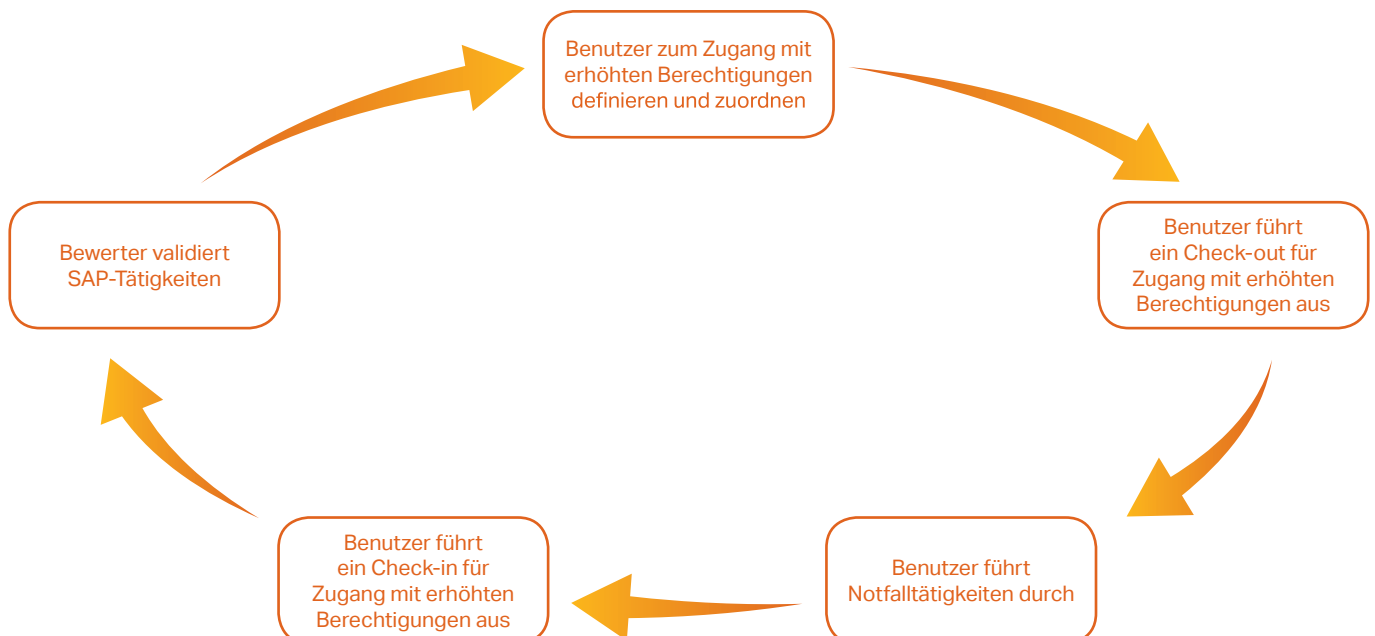
Der Erhöhte-Berechtigungen-Manager kann an Ihre spezifische Geschäftsumgebung angepasst werden. Erhöhte Zugangsberechtigungen können entweder einer Rolle oder einem SAP-Benutzer genehmigt werden.

Rollen mit erhöhten Berechtigungen

Eine vorgenehmigte SAP-Benutzer-ID kann bei der Durchführung eines Check-outs mit umfangreichen Zugriffsrollen versehen werden. Der jeweilige SAP-Benutzer verwendet seine SAP-Benutzer-ID, um die erforderlichen Aktivitäten in SAP durchzuführen.

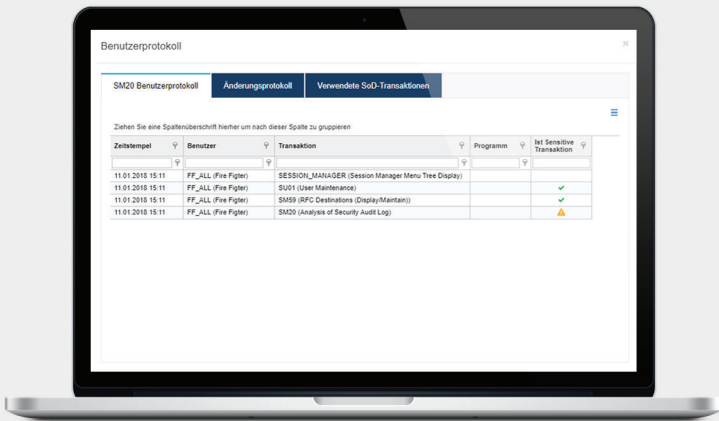
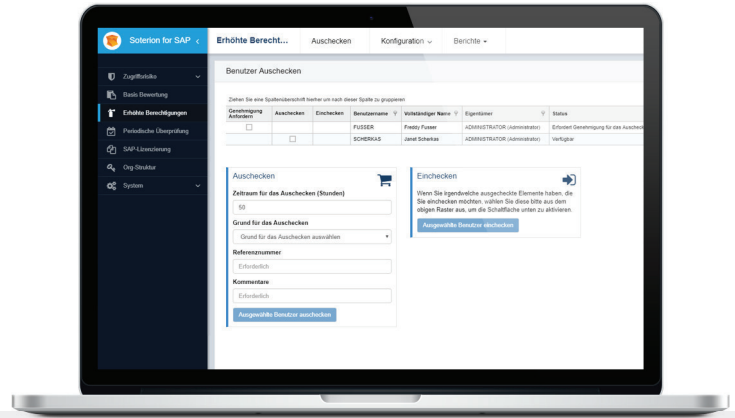
SAP-Benutzer mit erhöhten Berechtigungen

Ein SAP-Benutzerkonto mit dem erforderlichen umfangreichen Zugang wird freigeschaltet und das Kennwort an einen vorgenehmigten SAP-Benutzer gesendet. Mit dem entsprechenden SAP-Benutzerkonto werden die notwendigen Tätigkeiten in SAP durchgeführt.



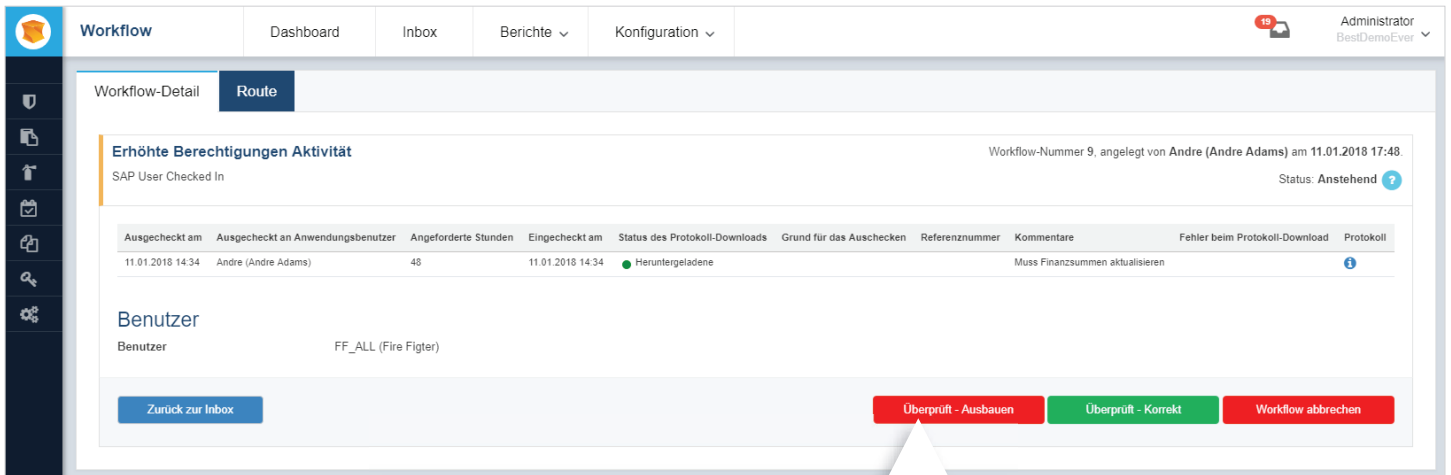
Check-out von erhöhten Zugangsberechtigungen

Wenn ein Benutzer ein Check-Out durchführt, wird ihm für einen definierten Zeitraum die erhöhte Zugangsberechtigung zugewiesen, damit er die erforderlichen Notfalltätigkeiten durchführen kann. Nach Abschluss des Vorgangs kann der Benutzer ein Check-in des Zugangs mit erhöhten Berechtigungen ausführen. Als Alternative erfolgt das Check-in automatisch, sobald die zugeordnete Frist abgelaufen ist.



Bewertung der erhöhten Zugangsberechtigungstätigkeiten

Alle Änderungen in SAP werden protokolliert und zur Überprüfung in den Soterion Erhöhten-Berechtigungen-Manager heruntergeladen. Alle ausgeführten Transaktionen und alle sensiblen Felder, die geändert wurden, können überprüft werden. Alle sensiblen Transaktionen, die ausgeführt wurden (Aufgabentrennung/ SOD oder Kritische Transaktionen) werden ebenfalls für die Berücksichtigung des Prüfers hervorgehoben.



Der Prüfer kann die vom Benutzer mit Zugang zu erhöhten Berechtigungen ausgeführten Tätigkeiten bestätigen. Die Workflow-Aktivität kann bei Rückfragen als **Review - Folgeaktivität** gekennzeichnet werden.

PERIODISCHE- ZUGRIFFSÜBERPRÜFUNG- MANAGER



Ausrichtung Ihrer GRC-Fähigkeiten an Ihren Geschäftszielen

Die periodische Überprüfung Ihres SAP-Benutzerzugriffs, wobei die damit verbundenen Risiken und notwendigen Kontrollen analysiert bzw. überprüft werden, richtet Ihre GRC-Kapazität an Ihren individuellen Unternehmenszielen aus. Dieser Prozess wird sowohl die Einsicht in Ihre GRC-Umgebung erheblich verbessern als auch eine Prüfung und gesetzliche Verpflichtung darstellen in

Eine ausgereifte GRC-Fähigkeit umfasst die regelmäßige Überprüfung des Zugriffs, der Risiken und Kontrollen eines Benutzers.

Der Periodische-Zugriffsüberprüfung-Manager bietet eine Plattform, auf der Benutzerzugriffsüberprüfungen in einer einfachen, Workflow-gesteuerten Web-Umgebung von Geschäftsbenutzern durchgeführt werden können, während externe Regelsatz- und Kontrollüberprüfungen erleichtert werden. Der Periodische-Zugriffsüberprüfung-Manager von Soterion sorgt für zentrale Kontrolle aber auch dezentralisierte Verwaltung während des gesamten Benutzerzugriffsüberprüfungprozesses

Überprüfung des Regelsatzes

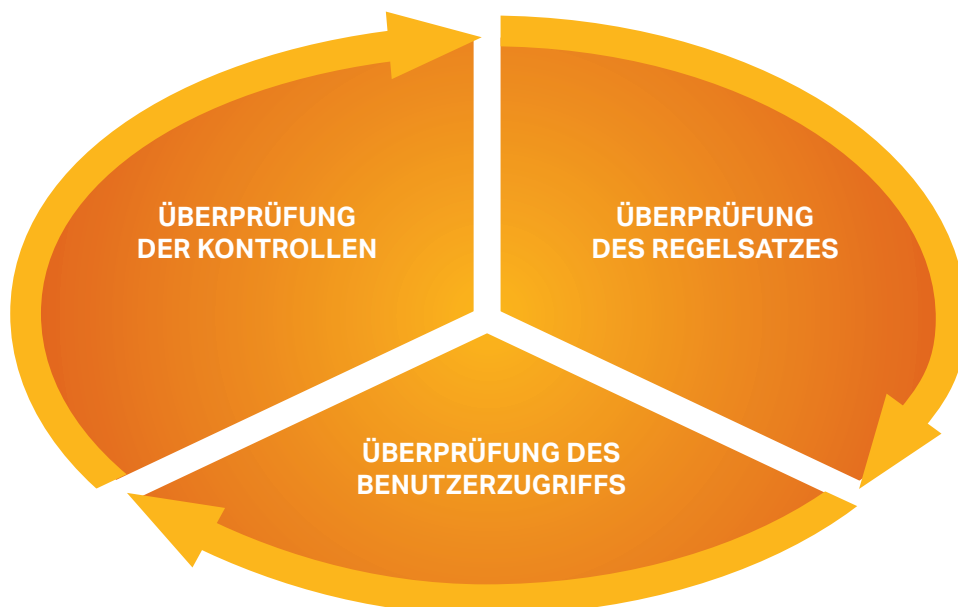
Durch die regelmäßige Überprüfung und Aktualisierung Ihres Risikoregelsatzes wird sichergestellt, dass er in einem sich wandelnden Geschäftsumfeld weiterhin relevant bleibt.

Überprüfung der Kontrollen

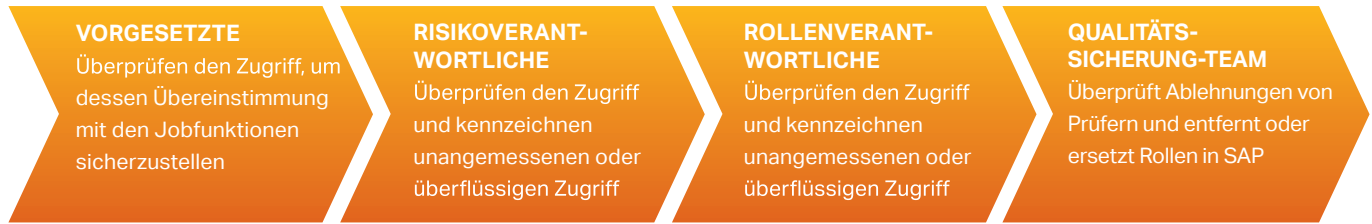
Durch regelmäßige Überprüfungen wird die Effizienz Ihrer Kontrollmaßnahmen kontinuierlich optimiert, indem Lücken in der Kontrolleffektivität identifiziert werden.

Überprüfung des Benutzerzugriffs

Überprüfen Sie Ihre SAP-Benutzerzugriffszuordnungen, um sicherzustellen, dass alle Zuordnungen weiterhin relevant sind. Neuzertifizierung des Benutzerzugriffs erfolgt durch Identifizierung und Entfernung redundanter und überflüssiger Zugriffe.

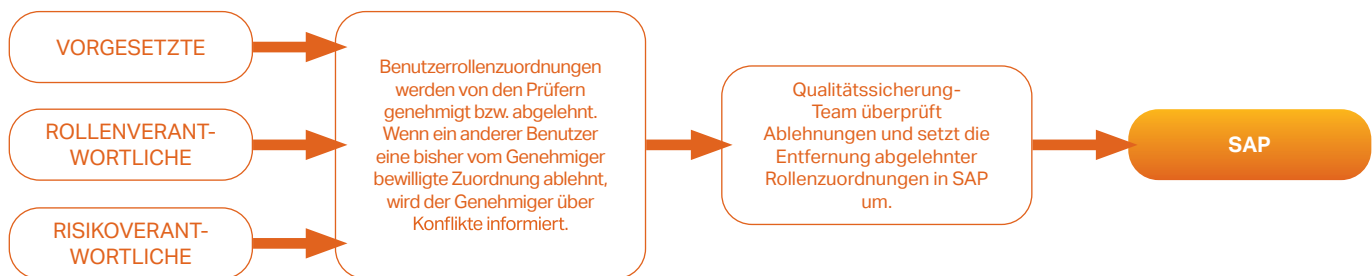


Wer ist an einer Überprüfung beteiligt?



Jede gewünschte Kombination von Vorgesetzten, Risikoverantwortlichen und Rollenverantwortlichen kann Benutzerrollenzuordnungen genehmigen oder ablehnen im Kontext eines bestimmten Risikoszenarios. Geschäftsbutzer können von jedem internetfähigen Gerät aus teilnehmen. Der Administrator hat Zugang zu einer grafischen Ansicht des Gesamtfortschritts aller Prüfer. Anfragen und Streitigkeiten können effektiv reguliert werden, und Geschäftsbutzer werden regelmäßig per E-Mail auf dem Laufenden gehalten.

Der Überprüfungsprozess



Ein Überprüfungssatz ist eine Schattenkopie der Benutzerzugriffslandschaft in SAP zum Zeitpunkt der Erstellung. Jeder Überprüfungssatz enthält außerdem eine Liste der Verantwortlichen und Genehmigern für Benutzer, Risiken und Rollen.

Prüfer können Genehmigungen und Ablehnungen von Benutzerrollen durchführen

Eine automatisierte E-Mail vom Administrator fordert alle relevanten Benutzer auf, am Überprüfungsprozess teilzunehmen, indem sie sich einfach von einem beliebigen internetfähigen Gerät aus in ihren Überprüfungsposteingang einloggen und die in der E-Mail angegebene URL verwenden.

Beim Einloggen wird dem Benutzer ein Posteingang angezeigt, der die Rollenzuordnungen und die damit verbundenen Risiken in separaten Registerkarten detailliert darstellt.

Der Benutzer kann Rollenzuordnungen genehmigen oder ablehnen und bei Bedarf Kommentare hinzufügen.

Der Benutzer kann die zuvor von ihm genehmigten oder abgelehnten Zuordnungen einsehen (und zurücknehmen). Der Benutzer hat Zugriff auf die Anzeige und Behebung von Zuordnungen, wenn Konflikte bestehen, d. h. Zuordnungen, die zuvor genehmigt wurden, aber von einem anderen Benutzer abgelehnt wurden.

Periodische Zug...

Überprüfung Inbox: ESTEYN (Emilia Steyn) | Überprüfung | Annual User Access Review 2021

Überprüfung Inbox

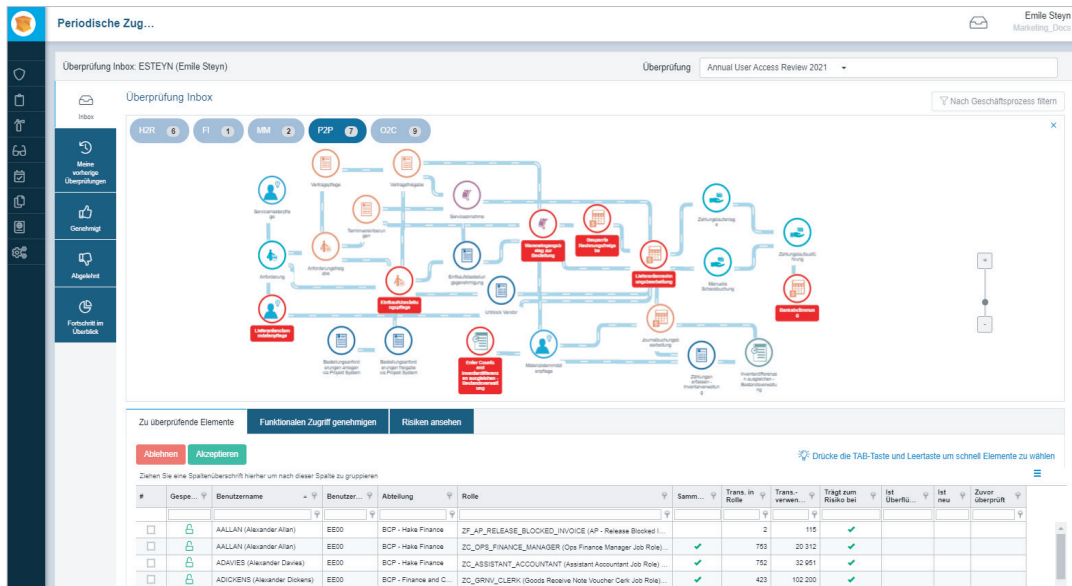
Zu überprüfende Elemente | Fundamentale Zugriff genehmigen | Risiken ansehen

Abnehmen | Approbieren

Zeigen Sie mir Systembenutzer Rollen um nach Bedarf Spalte zu gruppieren

| Grp | Benutzername | Benutzerg. | Abteilung | Rolle | Sensitivität | Trans. in Risk | Trans. - Bewertung | Risikozust. Risk |
|-----|--------------------------|------------|-----------------|--|--------------|----------------|--------------------|------------------|
| ✓ | AALLAN (Alexander All) | 0010 | BCP - Intern F. | 2F_SF_RELEASE_BLOCKED_INVOICE (AP - Release Blocked Invoice) | ✓ | 2 | 100 | ✓ |
| ✓ | AALLAN (Alexander All) | 0010 | BCP - Intern F. | 2C_SFPE_FINANCE_MANAGER (Cpe Finance Manager Job Role) | ✓ | 760 | 20.000 | ✓ |
| ✓ | ADONIS (Alexander Donis) | 0010 | BCP - Intern F. | 2C_ACCOUNT_ACCOUNTANT (Account Accountant Job Role) | ✓ | 162 | 50.000 | ✓ |
| ✓ | ADONIS (Alexander Donis) | 0010 | BCP - Intern F. | 2C_SERV_GLENN (Global Resource Note User/Car Job Role) | ✓ | 433 | 100.000 | ✓ |
| ✓ | ADONIS (Alexander Donis) | 0010 | BCP - Intern F. | 2C_SERV_GLENN (Global Resource Note User/Car Job Role) | ✓ | 139 | 4.000 | ✓ |
| ✓ | ADONIS (Alexander Donis) | 0010 | BCP - Intern F. | 2C_SERV_GLENN (Global Resource Note User/Car Job Role) | ✓ | 403 | 14.000 | ✓ |
| ✓ | AMR1 (Amelia May) | 0010 | BCP - Intern F. | 2F_SF_PRRV_DOC (AP - Print Document) | ✓ | 1 | 177 | ✓ |
| ✓ | AMR1 (Amelia May) | 0010 | BCP - Intern F. | 2C_FINANCE_GLENN (Finance Clerk Job Role) | ✓ | 400 | 24.000 | ✓ |
| ✓ | AMTHOLD (Andreas H) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 139 | 5.000 | ✓ |
| ✓ | AMTHOLD (Andreas H) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 132 | 97 | ✓ |
| ✓ | AMTHOLD (Andreas H) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 12 | 97 | ✓ |
| ✓ | AMTHOLD (Andreas H) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 433 | 20.000 | ✓ |
| ✓ | AMTHOLD (Andreas H) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 139 | 5.000 | ✓ |
| ✓ | BOLARI (Boris Clark) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 7 | 897 | ✓ |
| ✓ | BOLARI (Boris Clark) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 1 | 1.000 | ✓ |
| ✓ | BOLARI (Boris Clark) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 403 | 27.000 | ✓ |
| ✓ | BOLARI (Boris Clark) | 0010 | BCP - Intern F. | 2C_SF_PRRV_DOC (AP - Print Document) | ✓ | 403 | 20.000 | ✓ |

Soterion wandelt die technische GRC-Sprache in eine für Ihre Geschäftsbenutzer verständliche Sprache um



Der Periodische-Zugriffsüberprüfung-Manager von Soterion bietet den Geschäftsbenutzern (Prüfern) die Möglichkeit, ihre Prüfung nach Geschäftsprozessablauf durchzuführen. Wenn Ihre Organisation SAP-Rollen hat, die entweder keine gute Namenskonvention haben, d.h. wenn der SAP-Rollenname die Funktion der Rolle nicht beschreibt, oder wenn die SAP-Rollen groß sind und viele Aktivitäten enthalten, führt dies oft dazu, dass Prüfer nicht wissen, welcher Zugriff in den SAP-Rollen enthalten ist.

Soterion ermöglicht es den Prüfern, ihre Prüfung nach Geschäftsprozessablauf durchzuführen. Alle hervorgehobenen Schritte im Geschäftsprozessfluss zeigen den Zugriff an, der den SAP-Benutzern des Überprüfers zugewiesen wurde.

Durch Auswahl der Geschäftsprozessschritte filtert Soterion, welche SAP-Rollen diesen Zugriff ermöglichen und welche SAP-Benutzer diesen SAP-Rollen zugewiesen wurden.

Die Geschäftsprozessfluss-Funktionalität von Soterion reduziert den Aufwand für die Durchführung einer Benutzerzugriffsprüfung erheblich und spart der Organisation Zeit und Geld.

SOTERION SAP-LIZENZIERUNG-MANAGER



Optimieren Sie Ihre Ausgaben und halten Sie Ihre Compliance ein, indem Sie Ihr SAP-Lizenzmanagement aktiv steuern

SAP-Lizenzmanagement ist ein erfolgskritisches Element bei der Erstellung einer kosteneffizienten und revisionssicheren Strategie für ein effektives Software Asset Management. Der SAP-Lizenzierung-Manager von Soterion bietet Ihnen die notwendigen Einsichten zur Anpassung Ihrer SAP-Lizenzvereinbarung an die spezifischen Anforderungen Ihres Unternehmens, um ein optimales Vertragsmanagement und vollständige Compliance sicherzustellen und gleichzeitig ungeplante und überflüssige Kosten zu reduzieren.

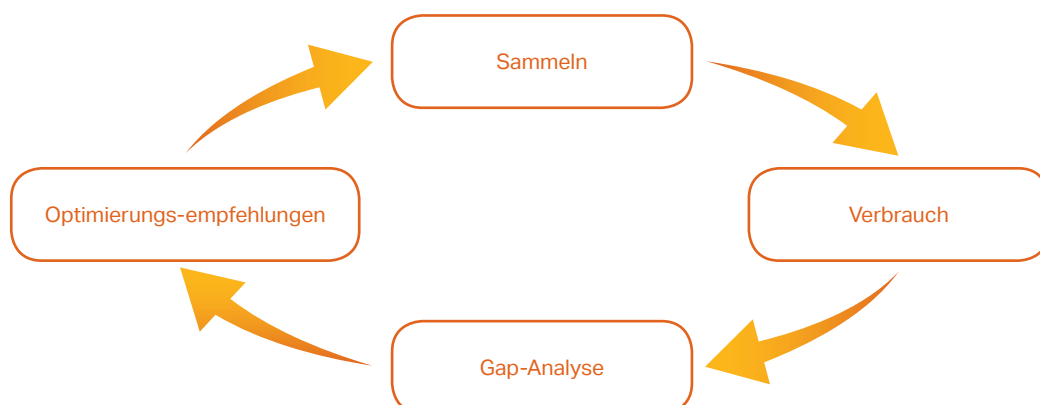
Unser Hintergrund

Unsere spezialisierte Erfahrung und unser umfassendes Verständnis von Vor-SAP-Lizenzaudits stellen sicher, dass unsere Kunden nicht nur die Produktivität und die Kosten im Auge behalten können, sondern auch die Regelung der SAP-Lizenz Einhaltung.

Kernpunkte

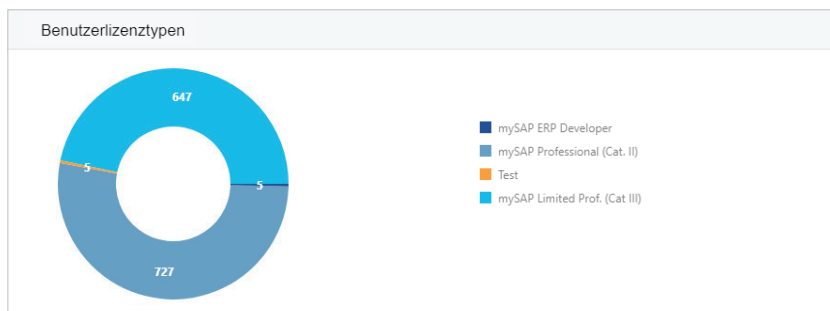
Unser Vorgehen

- ✓ **Sammeln (Stückliste)**
SAP-Lizenzvereinbarungen zusammentragen und mit der SAP-Lizenzstückliste vergleichen.
- ✓ **Verbrauch**
Konfiguration und Nutzung verschiedener Lizenzkategorien bestimmen.
- ✓ **Gap-Analyse**
Verbrauchfiguren mit der Stückliste vergleichen und feststellen, ob sie innerhalb der Lizenzgrenzwerte liegen, um ungeplante Mehrkosten zu vermeiden.
- ✓ **Optimierungsempfehlungen**
Ermitteln von Optimierungsmöglichkeiten anhand der tatsächlichen Nutzung von Lizenzkategorien. Dazu gehören Aktivitäten wie das Sperren oder Verfallen ruhender Benutzerkonten.



SAP-Lizenzkategorien gliedern sich typischerweise in folgende Bereiche:

- ✓ Benannte Benutzer (einschließlich indirekter Nutzung)
- ✓ Stammsätze
- ✓ Durchsatz
- ✓ Hardware



Benutzerlizenz Optimierungsempfehlungen

Benutzerpflege

- ✓ Inaktive Benutzer
- ✓ Gesperrte Benutzer und nicht abgelaufene
- ✓ Noch nie angemeldete Benutzer

Benutzerklassifizierung

- ✓ Uneinheitliche Klassifizierung der Benutzer wird von SAP als höhere Lizenzkategorie angesehen. Benannte SAP-Benutzerlizenzen müssen über die verschiedenen SAP-Systeme hinweg abgeglichen werden.
- ✓ Nicht klassifizierte Benutzer werden von SAP im Rahmen des jährlichen Lizenzaudits als Professional-Lizenztyp (High-End-Kategorie) eingestuft.

45

GESPERRTE ABER NICHT ABGELAUFENE BENUTZER
 Diese Benutzer sind zwar gesperrt, sind aber nicht durch Änderung des "Gültig bis" - Datums abgelaufen. Ein gesperrter, aber nicht abgelaufener Benutzer gilt als aktiver SAP-Benannte-Benutzer.

612

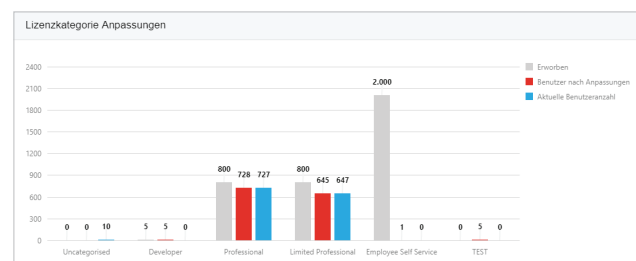
NOCH NIE ANGEMELDETE BENUTZER
 Diese Benutzer haben sich noch nie am SAP-System angemeldet. Überlegen Sie, ob diese Konten gesperrt und abgelaufen werden könnten.

Empfehlungen zur Anpassung der Benutzer-Lizenzkategorie

Die Grafik fasst die Umklassifizierungsempfehlungen nach Nutzung zusammen.

Da es in der SAP-Standardversion nicht möglich ist, die Nutzungsdaten der SAP-Benutzer in den Klassifizierungsprozess einzubeziehen, folgen die meisten SAP-Mandanten der SAP-Lizenzklassifikationsmethodik, die auf Rollenzuordnungen basiert ist. Diese Methodik kann erfolgreich angewendet werden, wenn die spezifischen SAP-Rollen, die den Benutzern zugewiesen werden, gut auf das abgestimmt sind, was die Benutzer in SAP tatsächlich tun.

Untersuchungen zeigen jedoch, dass SAP-Benutzer durchschnittlich nur 20% der ihnen zugeordneten Funktionalität nutzen, was zu einer unnötigen Zuweisung von höheren SAP-Lizenzkategorien an die Mehrheit der Benutzer führt (80%).



In Zukunft

Der Soterion SAP-Lizenzierung-Manager verwendet seine Datenbank als Repository für zukünftige SAP-Lizenzüberprüfungen, wodurch Sie weniger Zeit und Ressourcen für die Wartung Ihrer SAP-Lizenzen benötigen.

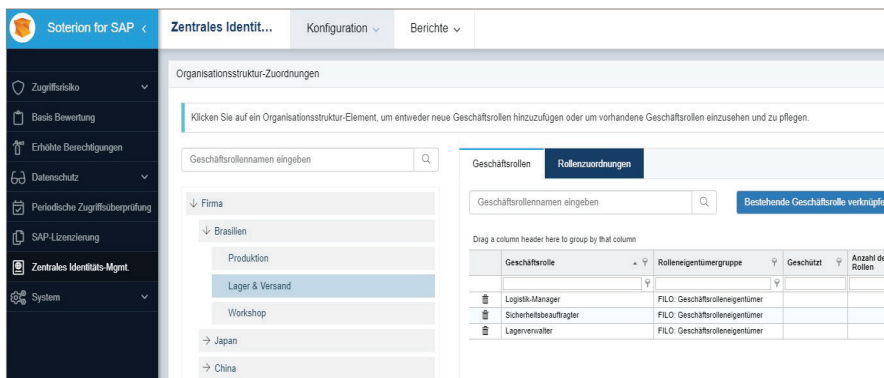
Darüber hinaus können Sie mit unserer Lösung Verträge, Dokumente und Notizen speichern, um Ihre SAP-Lizenz-Compliance nachzuweisen und so die Anzahl der Beratungstage bei zukünftigen SAP-Lizenzaudits zu minimieren.

ZENTRALER IDENTITÄTSMANAGER



Geschäftsrollen

Mit dem Konzept der Geschäftsrolle können Sie mehrere Geschäftsziele ansprechen.



Eine Geschäftsrolle ist ein Datencontainer für eine Gruppe von SAP-Einzelrollen, die aus mehreren SAP-Systemen stammen können.

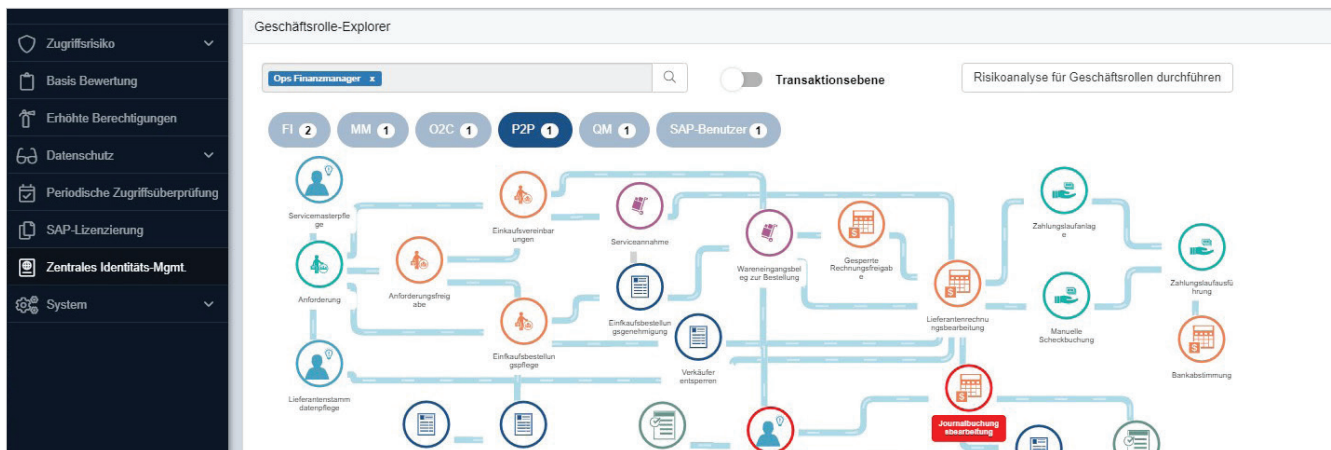
Eine Geschäftsrolle ähnelt einer SAP-Sammelrolle mit den zusätzlichen Vorteilen:

- Eine Geschäftsrolle ist flexibler, da Benutzern Teilrollen zugewiesen werden können.
- SAP-Einzelrollen aus mehreren SAP-Systemen können in die Geschäftsrolle aufgenommen werden.

Das Geschäftsrollenkonzept betrifft mehrere wichtige GRC-Geschäftsziele. Dazu gehören:

- Effizienzsteigerung des Bereitstellungsprozesses (Joiner - Mover - Leaver) sowie Reduzierung des für die Durchführung einer Benutzerzugriffsüberprüfung erforderlichen Aufwands.
- Standardisierung von Job-Funktionen in der gesamten Organisation zur Reduktion der Komplexität.
- Verbessern Sie die Risikoverantwortung des Unternehmens, indem Sie den SAP-Zugriff auf eine geschäftsfreundlichere Weise darstellen.

Geschäftsrollen sind mit Abteilungen in der Organisationsstruktur verknüpft, um die Suche nach dem angemessenen Zugriff für SAP-Benutzer zu vereinfachen.



Die Funktionalität der Soterion Geschäftsrolle zeigt den in der Geschäftsrolle enthaltenen SAP-Zugriff mithilfe einer Visualisierungstechnik an, die die technische GRC-Sprache in eine geschäftsfreundlichere Sprache umwandelt.

Alle von einer Geschäftsrolle durchführbaren Aktionen werden im Geschäftsprozessfluss (rot) hervorgehoben, was es den Geschäftsrolleigentümern erleichtert, fundierte Entscheidungen zu treffen.

Zentrale Benutzerverwaltung

Die Zentrale Benutzerverwaltung von Soterion ermöglicht die Benutzerverwaltung in SAP-Nicht-Produktionssystemen (DEV, QAS). Damit werden der Supportaufwand und die damit verbundenen Kosten für die Verwaltung von Benutzerzugängen in SAP-Nicht-Produktionssystemen reduziert.

SAP-Verteilungskonfiguration

Verteilung SAP-System hinzufügen Verbindungen testen Globale Konfiguration

Ziehen Sie eine Spaltenüberschrift hierher um nach dieser Spalte zu gruppieren

| Typ | Beschreibung | Systemide... | SAP-Installationsnummer | Anwendungsserver | Instanznu... | Kunde | Sprache | umfeld |
|-----|------------------------|--------------|-------------------------|------------------|--------------|-------|---------|--------|
| 1 | Produktionssystem | PRD | 1234567 | 123.123.123 | 0 | 100 | DE | PRD |
| 1 | Qualitätssicherung 100 | QA | 987654321 | 321.321.321 | 0 | 100 | DE | QA |
| 1 | Qualitätssicherung 200 | QAS | 987654322 | 213.213.213 | 1 | 200 | DE | QA |
| 1 | Entwicklung Testen | DEV | 987654330 | 123.321.654 | 1 | 120 | DE | DEV |
| 2 | CRM Qualitätssicherung | CRQ | 987654340 | 123.321.432 | 0 | 100 | DE | PRD |

Konfiguration für verteilte SAP-Systeme

Erstellung von Benutzern

Kennworrücksetzungen

Rollenzuordnung

Benutzersperre

Abbrechen Speichern

Soterion bietet dem Administrator die erweiterte Entscheidungsfreiheit, welche Funktionen in den verschiedenen Vertriebssystemen ausgeführt werden können.