Eine neue GRC-Ära für SAP-Kunden

Der Weg in die Zukunft: **Soterions Erkenntnisse und Prognosen**

soterion

Für Unternehmen, die mit SAP arbeiten, stehen neue Herausforderungen an. Eine wachsende Zahl von Unternehmen geht auf S/4HANA über, denn die Upgrade-Frist rückt rasch näher. Nach Schätzungen einer Quelle haben rund 22.000 Kunden S4 lizenziert und etwa zwei Drittel von ihnen haben die Implementierung abgeschlossen.

Die Umstellung auf S4 bringt viele Vorteile in Bezug auf Geschwindigkeit, Flexibilität und Analysefähigkeit mit sich, aber sie steigert auch die Komplexität. Dieser Sprung nach vorne ist mehr als eine einfache Software-Aktualisierung. Er stellt eine erhebliche Verlagerung in der Art und Weise dar, wie Unternehmen ihre Daten angesichts der raschen Weiterentwicklung der Geschäftsprozesse sichern.

Wie bei vielen großen digitalen Transformationsprojekten ist die Sicherheit klassischerweise in den Hintergrund getreten, da sich Unternehmen auf die Konfiguration und Aufrechterhaltung geschäftskritischer Prozesse konzentrieren.

Der Bedarf an robuster Sicherheit ist unbestreitbar. Die Zahl der Sicherheitsvorfälle hat in den letzten zehn Jahren deutlich zugenommen, einschließlich Cyberangriffen und Datenbetrug. Daten aus einer Studie des Weltwirtschaftsforums von 2023 zeigen, dass 43 Prozent der Geschäftsführer es für wahrscheinlich halten, dass ihr eigenes Unternehmen in den nächsten zwei Jahren spürbar von einem Cyberangriff betroffen sein wird.

Diese Art von Angriffen kann nicht nur den Ruf schädigen, sondern auch erhebliche finanzielle Folgen haben. In einem Bericht des Cybercrime Magazine von 2020 wird prognostiziert, dass die weltweite Cyberkriminalität bis 2025 jährlich 10,5 Billionen US-Dollar kosten wird – exponentiell mehr als der Schaden, der durch Naturkatastrophen entsteht, und profitabler als der weltweite Handel mit sämtlichen illegalen Drogen von Bedeutung.

Die zunehmende Strenge der SAP-Prüfungen stellt eine zusätzliche Herausforderung dar. Die Aufsichtsbehörden ergreifen immer strengere Maßnahmen, um die Befolgung der Vorschriften zu gewährleisten. Das erhöht den Druck auf die Unternehmen, ihre SAP-Umgebung ordnungsgemäß zu sichern und strikte Maßnahmen in Bezug auf Governance, Risiko und Compliance (GRC) einzuführen.

Dieser zunehmende Druck hat eine neue GRC-Ära eingeläutet. Eine Ära, in der die Verwaltung von SAP-Umgebungen voraussichtlich komplexer als je zuvor sein wird. Für Führungskräfte, die in diesem zunehmend komplexen Umfeld die Nase vorn haben wollen, ist es unerlässlich, die Dynamik zu verstehen und künftige Entwicklungen vorauszusehen.

In diesem Bericht stellen wir vier zentrale Erkenntnisse und Prognosen vor, die unserer Meinung nach die Zukunft von GRC für Unternehmen mit SAP prägen werden.

Soterions Prognosen für die Zukunft von GRC in SAP

Prognose 1:

Der Mangel an qualifizierten SAP-Sicherheitsressourcen kann das Risiko erhöhen

Die erwartete Zunahme der SAP-Sicherheitskomplexität in Verbindung mit einem weltweiten Fachkräftemangel kann Unternehmen einem erhöhten Risiko aussetzen, da sie Schwierigkeiten haben, ausreichend qualifizierte SAP-Sicherheitsressourcen zu finden.

Prognose 2:

Das Streben nach Standardgeschäftsprozessen wird zu einer Ausweitung des Zugangs führen

Im Zuge des Drängens auf die Einführung von Standardgeschäftsprozessen und vordefinierten Rollen könnten Unternehmen gezwungen sein, Benutzern mehrere Rollen zuzuweisen. Die Folge ist eine Ausweitung des Zugriffs, wodurch sich das Unternehmensrisiko erhöht.

Prognose 3:

Mit der zunehmenden Cloud-Nutzung verschwimmen die Eigentumsverhältnisse und die Risiko-Exposition

Die zunehmende Nutzung von Drittanbieter-Cloud-Lösungen verursacht Mehrdeutigkeiten in Bezug auf das Zugriffsrisiko, und der Vorstoß in die SAP-Cloud wirft Fragen zum Eigentum und zur Verwaltung der Sicherheit auf.

Prognose 4:

Der Aufstieg des hybriden IAM/GRC-Modells

Bei der Abwägung der Vorteile von IAM- und GRC-Lösungen werden immer mehr Unternehmen ein Hybridmodell in Betracht ziehen, das die Stärken beider Systeme nutzt.

Prognose 1:

Der Mangel an qualifizierten SAP-Sicherheitsressourcen kann das Risiko erhöhen

Die Verwaltung von SAP-Berechtigungen ist eine anspruchsvolle und komplexe Aufgabe. Sie erfordert fortgeschrittene technische Fähigkeiten und ein tiefreichendes Verständnis der Systemkomplexität. Die Ausbildung zum kompetenten SAP-Sicherheitsadministrator dauert Jahre. Mit der erwarteten Zunahme der Komplexität bei der Verwaltung von S/4HANA müssen Unternehmen möglicherweise ihre Sicherheitsressourcen verdoppeln, um diese Aufgabe gut zu bewältigen.

Angesichts der erheblichen Veränderungen im Sicherheitsmanagement in S4 sind viele erfahrene SAP-Sicherheitsexperten, die sich dem Ende ihrer Karriere nähern, möglicherweise nicht geneigt, diese neuen Ansätze zu übernehmen. Die potenzielle Folge wäre der Verlust von Spitzenkräften. Damit stehen Unternehmen vor der Aufgabe, neue Mitarbeiter zu rekrutieren und auszubilden – eine beträchtliche Herausforderung angesichts des vorherrschenden massiven globalen Fachkräftemangels.

In einem McKinsey-Bericht von 2021 wurde festgestellt, dass weltweit 87 Prozent der Unternehmen Qualifikationslücken haben oder in einigen Jahren mit Lücken rechnen. Ein weiterer Bericht, veröffentlicht von der globalen Unternehmensberatungsfirma Korn Ferry, kommt zu dem Ergebnis, dass bis 2030 mehr als 85 Millionen Stellen unbesetzt bleiben könnten, weil es nicht genügend qualifizierte Personen gibt, die dafür in Frage kommen. Wenn es um spezialisierte Fähigkeiten wie die Verwaltung von SAP-Berechtigungen geht, ist die Qualifikationslücke sogar noch größer.

Der Übergang zur Fernarbeit hat den Mangel an SAP-Sicherheitsressourcen weiter verschärft. Die herkömmliche Schulung vor Ort hat sich als der effizienteste Weg zur Entwicklung von Fähigkeiten erwiesen. Durch Remote Work wird dieser Schulungsprozess jedoch in die Länge gezogen. Folglich sehen sich viele Unternehmen dazu veranlasst, den Wert von Investitionen in die Ausbildung von Hochschulabsolventen zu überdenken. Zudem schreckt die Unvorhersehbarkeit des heutigen Arbeitsmarktes – auf dem Arbeitnehmer ihre neu erworbenen Fähigkeiten leicht anderswo anbieten können – viele Unternehmen davon ab, in die Weiterbildung zu investieren. Dieser Fachkräftemangel wird vermutlich mehrere Folgewirkungen haben. Ein ineffizient verwalteter Zugang kann Unternehmen einem größeren Risiko aussetzen, da weniger erfahrene Administratoren möglicherweise einen unnötig breiten Zugang gewähren, um Arbeitsabläufe nicht zu blockieren. Das kann zu Systemausfällen, Ineffizienz und Frustration am Arbeitsplatz führen.

Angesichts dieser Herausforderungen gehen wir davon aus, dass es für eine beträchtliche Anzahl von Unternehmen schwierig sein wird, die benötigten qualifizierten SAP-Sicherheitsressourcen zu finden. Um eine angemessene Zugriffskontrolle aufrechtzuerhalten, müssen diese Unternehmen möglicherweise alternative Support-Modelle in Betracht ziehen, beispielsweise Outsourcing oder Managed Services. Wir erwarten in den kommenden Jahren eine deutliche Verschiebung hin zu diesen Modellen, da die Unternehmen bemüht sein werden, die zunehmende Komplexität der SAP-Sicherheit in der S/4HANA-Ära zu bewältigen.

Prognose 2:

Das Streben nach Standardgeschäftsprozessen wird zu einer Ausweitung des Zugangs führen

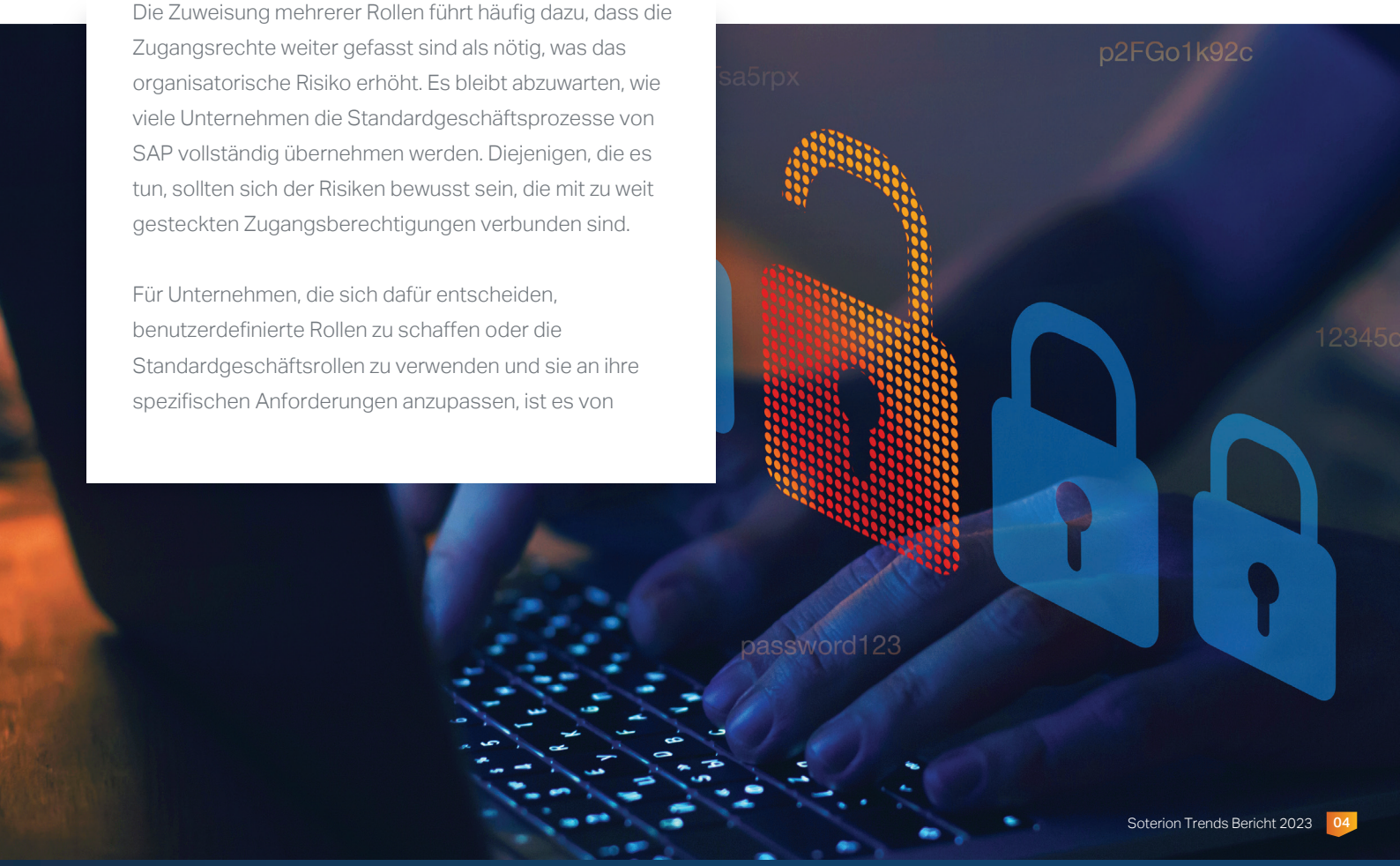
Das jüngste Drängen von SAP zur Einführung von Standardgeschäftsprozessen, und insbesondere wenn Implementierungspartner empfehlen, die vordefinierten Geschäftsrollen von SAP zu verwenden, stellt eine bedeutsame Verlagerung in der SAP-Landschaft dar. Diese Standardrollen zielen darauf ab, die Implementierung und den Support zu straffen, aber sie haben den Nachteil, dass sie unangemessenen, weitreichenden Benutzerzugang verschaffen, der das Unternehmen einem unnötigen Betrugsrisiko aussetzt.

In der Realität sind Unternehmen keine Gebilde mit Einheitsgröße. Da jedes Unternehmen seine spezifischen Bedürfnisse und Arbeitsabläufe hat, ist es unwahrscheinlich, dass eine Standardrolle das richtige Maß an Zugang gewährt. Um potenzielle betriebliche Engpässe zu vermeiden, werden den Benutzern oft mehrere Geschäftsrollen zugewiesen, damit sie den erforderlichen Zugriff für alle ihre Aufgaben haben. Dieser Ansatz hat jedoch seine Tücken.

Die Zuweisung mehrerer Rollen führt häufig dazu, dass die Zugangsrechte weiter gefasst sind als nötig, was das organisatorische Risiko erhöht. Es bleibt abzuwarten, wie viele Unternehmen die Standardgeschäftsprozesse von SAP vollständig übernehmen werden. Diejenigen, die es tun, sollten sich der Risiken bewusst sein, die mit zu weit gesteckten Zugangsberechtigungen verbunden sind.

Für Unternehmen, die sich dafür entscheiden, benutzerdefinierte Rollen zu schaffen oder die Standardgeschäftsrollen zu verwenden und sie an ihre spezifischen Anforderungen anzupassen, ist es von entscheidender Bedeutung, sich vor dem Übergang zu S/4HANA mit einem soliden Rollendesign abzusichern. Leider wird bei vielen Projekten erst in einem späten Stadium die Sicherheit berücksichtigt, was zu übereilten und potenziell fehlerhaften Anordnungen führt. In einem Live-Umfeld kann die Änderung des Benutzerzugangs schwierig und störend sein. Daher ist es ratsam, vor der Umstellung den SAP-Zugang und die Prozesse genau zu definieren.

Dieser proaktive Ansatz wird vermutlich einige Nacharbeiten erfordern, zum Beispiel die Transaktionscodes für Lieferanten- und Kundenstamm mit Geschäftspartnern zu ersetzen und den Fiori-Zugang zu integrieren. Die Vorteile einer gut geplanten, sicheren Zugangskontrolle in S/4HANA überwiegen jedoch bei weitem die vorübergehenden Unannehmlichkeiten dieser Nacharbeit. Entscheidend ist, dass Sicherheitsmaßnahmen zusammen mit der Migration geplant werden und nicht als Nachgedanke.



Prognose 3:

Mit der zunehmenden Cloud-Nutzung verschwimmen die Eigentumsverhältnisse und die Risiko-Exposition

Es gab eine Zeit, in der Unternehmen, die SAP einsetzten, alle ihre Abläufe mit einem einzigen System verwalten konnten. Mit der zunehmenden Komplexität von Unternehmen und der rasanten Verbreitung von technologischen Lösungen setzen viele jedoch auf einen Best-of-Breed-Ansatz. Bei dieser Strategie wird eine Vielzahl von Lösungen in die SAP-Umgebung integriert, um spezifische Funktionalitäten zu erweitern.

Beispielsweise werden SAP- Funktionalitäten durch Cloud-basierte Lösungen ersetzt, wie etwa HCM durch SuccessFactors oder Procurement durch Ariba. Oder Sie entscheiden sich dafür, Teile von SAP durch Cloud-Plattformen wie Workday oder Coupa zu ersetzen. Diese Lösungen haben jede ihre eigenen Sicherheitskonzepte, was ihre Verwaltung zu einer Herausforderung macht.

Viele Zugangskontrolllösungen sind leider nicht in der Lage, für diese Cloud-Lösungen eine umfassende Analyse des Zugangsrisikos durchzuführen. Folglich haben Unternehmen möglicherweise kein klares Bild von ihrer Risikoexposition. Es ist unerlässlich, dass die Sicherheitsteams mit den Sicherheitsprotokollen für alle integrierten Lösungen vertraut sind und über genügend Ressourcen verfügen, um sie effektiv zu verwalten. Bemühen Sie sich um eine Lösung für die Zugangskontrolle, die in der Lage ist, eine Analyse des Zugangsrisikos für die in Ihrem Unternehmen eingesetzten Cloud-Lösungen durchzuführen.

Dies ist nicht die einzige Herausforderung im Zusammenhang mit der Cloud. Die Initiative von SAP, Kunden über das SAP-Programm Rise für den Umstieg auf Cloud-Hosting zu gewinnen, erhöht diese Komplexität noch weiter. Kunden können wählen, ob sie ihre SAP-Systeme in einer privaten Cloud, zum Beispiel einem Hyperscaler wie AWS oder Azure, oder in der SAP-eigenen öffentlichen Cloud hosten lassen.

Diese Verlagerung auf das Cloud-Hosting bringt zwar Skalierbarkeit, Leistung und Kostenvorteile mit sich, aber es führt auch zu Unklarheiten in Bezug auf die Verantwortung für verschiedene Tätigkeiten.

Diese Verlagerung auf das Cloud-Hosting bringt zwar Skalierbarkeit, Leistung und Kostenvorteile mit sich, aber es führt auch zu Unklarheiten in Bezug auf die Verantwortung für verschiedene Tätigkeiten.

We foresee significant challenges and potential disputes Wir sehen erhebliche Herausforderungen und potenzielle Auseinandersetzungen zwischen SAP und Kunden über die Verantwortlichkeiten in diesem Bereich voraus. Während wir darauf warten, dass SAP weitere Klarheit über Rollen und Verantwortlichkeiten schafft, sollten Sie sich vergewissern, dass Sie verstehen, wer welche Tätigkeiten ausführt, um sicherzustellen, dass angemessene Sicherheitsmaßnahmen abgedeckt sind, wenn Sie sich für das SAP-Programm Rise entscheiden.

Prognose 4:

Der Aufstieg des hybriden IAM/GRC-Modells

Im komplexen Ökosystem von SAP-Umgebungen stehen Lösungen für das Identitäts- und Zugangsmanagement (IAM) sowie für Governance, Risiko und Compliance (GRC) im Mittelpunkt des Interesses. Unternehmen sind darauf bedacht, die Rolle und den potenziellen Wert der einzelnen Lösungen zu verstehen.

IAM-Lösungen wurden entwickelt, um eine Identität in einer IT-Umgebung zu verwalten und den Joiner-Mover-Leaver-Prozess zu erleichtern. Diese Lösungen integrieren mehrere Systeme und ihr Versprechen bestand darin, frühere Herausforderungen bei der Bereitstellung zu lösen und die Prozesse für das Onboarding und die Bereitstellung von Benutzern zu beschleunigen. Zwar brachten sie tatsächlich erhebliche Effizienzgewinne mit sich, doch ein entscheidendes Element fehlte. Den meisten IAM-Lösungen fehlt die Fähigkeit, den SAP-Zugang auf einer detaillierten oder technischen Ebene zu analysieren, also bis hinunter zum SAP-Berechtigungsobjekt oder -feld. IAM-Lösungen eignen sich zwar hervorragend für die Gewährung von Zugangsrechten, doch häufig sind sie unzureichend, wenn es darum geht, die Risikoauswirkungen der zugewiesenen SAP-Rollen zu bewerten.

Für Unternehmen, die SAP einsetzen, sind detaillierte Zugangsrisikofähigkeiten unabdingbar. Geschäftsanwender treffen Entscheidungen mit begrenzten Risikoinformationen. Wenn Ihr Unternehmen beispielsweise die jährliche Überprüfung des SAP-Benutzerzugangs mit einer IAM-Lösung durchführte, entschieden die Prüfer lediglich anhand des Rollennamens, ob eine SAP-Rolle für Benutzer geeignet war. Es wurden keine Informationen über die Nutzung oder die Auswirkungen des mit dieser Rolle verbundenen Zugangsrisikos hervorgehoben, da IAM nicht in der Lage ist, diese detaillierten Informationen auf die gleiche Weise wie eine GRC-Lösung anzuzeigen.

Da das Bewusstsein für diese Problematik wächst, gehen wir davon aus, dass immer mehr Unternehmen ein hybrides IAM/GRC-Modell in Betracht ziehen werden, bei dem Geschäftsrollen in der GRC-Lösung definiert werden. Dieser Ansatz macht Zugangsrisiken und Nutzungsinformationen sichtbar und ermöglicht es den Inhabern von Geschäftsrollen, fundierte Entscheidungen über den Inhalt und die Zusammensetzung der Rolle zu treffen.

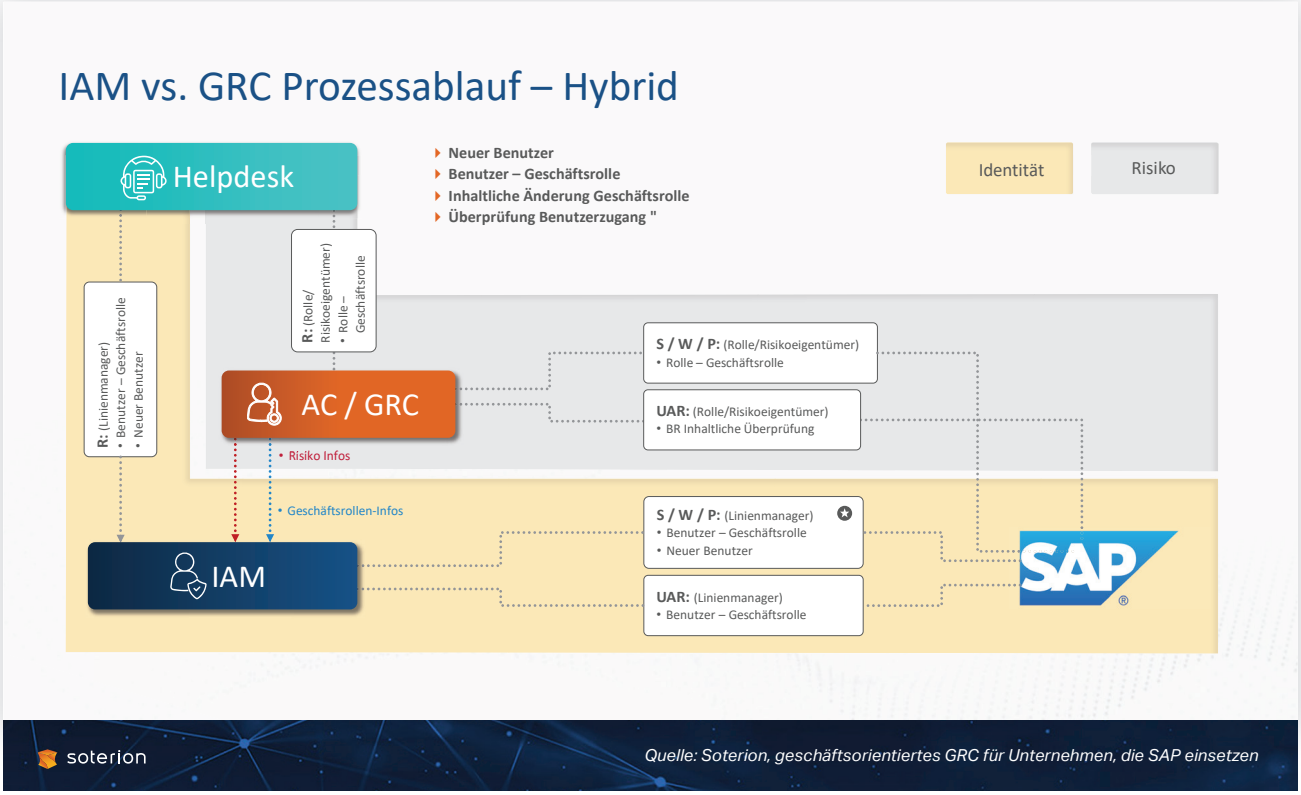
Es liegt auf der Hand, dass sowohl GRC- als auch IAM-Lösungen wichtige Aufgaben erfüllen. Die Verknüpfung der beiden Lösungen hat sich in der Praxis jedoch als schwierig erwiesen, da sich ihre Funktionen überschneiden. Auszuwählen, welche der beiden Lösungen die einzelnen Funktionen wie Workflow, Bereitstellung und Benutzerzugang übernimmt, ist ein entscheidender Faktor für den Erfolg ihrer kombinierten Nutzung.

Prognose 4:

Das Aufkommen des hybriden IAM/GRC-Modells

Das hybride Modell kann eine der folgenden Formen annehmen:

- **Hybrid 1:** Verwendung der GRC-Lösung für alle sich überschneidenden Funktionen für die SAP-Systeme und die IAM-Lösung für alle Nicht-SAP-Systeme.
- **Hybrid 2:** Verwendung der GRC-Lösung für die Definition der SAP-Geschäftsrollen und die IAM-Lösung für die Bereitstellung dieser Rollen und die Überprüfung des Benutzerzugangs (auf Geschäftsrollenebene).



Es ist von entscheidender Bedeutung, alternative Ansätze für die Bereitstellung von Zugangsrechten gründlich zu untersuchen, insbesondere durch die Erkundung des Potenzials von Azure AD und SAP Identity Provisioning (IPS).

Schlussfolgerung

Die ständig wachsende Komplexität von SAP-Umgebungen macht deutlich, wie wichtig zukunftsorientierte Sicherheitsstrategien sind. Mit dem bevorstehenden Übergang zu S/4HANA ist es besonders wichtig, die Sicherheit von der Peripherie in den Mittelpunkt der Projektplanung und -ausführung zu rücken.

Die Umstellung auf S/4HANA stellt nicht einfach nur ein Upgrade dar, sondern Verschiebungen von seismischen Ausmaßen in Betrieb und Kontrolle. Indem vor dem Upgrade die Rollen überprüft werden, kann ein erheblicher Teil der Vorarbeit bereits im Voraus geleistet werden. Außerdem muss unbedingt sichergestellt werden, dass alle Richtlinien und Verfahren auf dem neuesten Stand und in der Praxis Ihres Unternehmens verankert sind.

Ebenso wichtig ist es, die Geschäftsanwender über ihre Aufgaben und Pflichten im Zusammenhang mit der Einhaltung der Vorschriften aufzuklären und eine Kultur des Sicherheitsbewusstseins und der Verantwortung zu schaffen.

Die Anpassung Ihres Regelsatzes an die spezifischen Anforderungen Ihres Unternehmens ist ein weiterer unabdingbarer Aspekt. Anstatt sich mit dem gebrauchsfertigen Standard-Regelsatz Ihres Anbieters von Zugangskontroll- oder GRC-Lösungen zu begnügen, können Sie die Genauigkeit und Relevanz für Ihr Unternehmen erhöhen, indem Sie ihn darauf zuschneiden.

Mit diesen Schritten können Sie die nach dem Upgrade erforderlichen Nacharbeiten erheblich reduzieren. Die Schaffung einer soliden Sicherheitsgrundlage vor der Umstellung verhindert außerdem, dass Sie sich während des Projekts um Ressourcen und Budgets drängeln müssen.

Voraussicht, Vorbereitung und kontinuierliche Anpassung sind erforderlich, um die Zukunft von SAP-Umgebungen zu meistern. Wenn Sie der Sicherheit in Ihrer strategischen Planung heute Priorität einräumen, sind Sie gut gerüstet, um die komplexen Herausforderungen von morgen zu meistern.

Mit Zuversicht die Zukunft von GRC navigieren

Soterion ist darauf spezialisiert, Unternehmen, die SAP einsetzen, bei der Optimierung ihrer Prozesse in Bezug auf Governance, Risiko und Compliance (GRC) zu unterstützen. Wir verstehen die einzigartigen Möglichkeiten und Herausforderungen, denen sich die meisten Organisationen gegenübersehen, wenn es um ihre GRC-Fähigkeiten geht.

Viele fühlen sich von der SAP-GRC-Software und ihrer scheinbaren Komplexität und den Kosten überwältigt und eingeschüchtert und zögern daher, den Prozess überhaupt zu beginnen. Andere haben möglicherweise das Gefühl, dass sie nicht den vollen Nutzen ihrer SAP-GRC-Software zu sehen bekommen.

Wir haben eine Reihe von Nischen-GRC-Tools entwickelt, um unsere Kunden dazu zu bringen, GRC als echten Nutzen und nicht als Belastung zu sehen. Unser Team von Fachberatern ist weltweit für Sie da. Wir sind darauf spezialisiert, den GRC-Prozess zu entmystifizieren, zu vereinfachen und zu beschleunigen.

BUCHEN SIE NOCH HEUTE EINE DEMO