Eine neue GRC-Ära für SAP-Kunden

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

soterion

Unternehmen, die SAP im Einsatz haben, stehen vor ganz neuen Herausforderungen
Immer mehr Unternehmen migrieren auf S/4HANA, denn die Frist zum Upgrade rückt allmählich näher Schätzungen zufolge haben etwa 22.000 Kunden bereits eine S/4 Lizenz, aber nur ein Drittel davon hat jedoch die Migraton abgeschlossen.

Während die Migration auf S/4HANA viele Vorteile mit sich bringt wie etwa Geschwindigkeit, Flexibilität und Analysefähigkeit, nimmt aber auch gleichzeitig die Komplexität deutlich zu. Dieser Sprung nach vorne ist weit mehr als ein einfaches Software-Upgrade. Er bedeutet eine grundlegende Neuaufstellung/Ausrichtung wie Organisationen ihre Daten sichern, und zwar angesichts sich rasant/schnell verändernder Geschäftsprozesse.

Bei vielen großen SAP-Projekten ist die Sicherheit in den Hintergrund geraten, weil man sich hauptsächlich auf die Konfiguration und Stabilität geschäftskritischer Prozesse konzentriert hat.

Der Bedarf an robuster Sicherheit ist unbestreitbar. Die Zahl der Sicherheitsvorfälle hat in den letzten zehn Jahren deutlich zugenommen, einschließlich Cyberangriffen und Datenbetrug. Einer Studie des Weltwirtschaftsforums von 2023 zufolge halten es 43 Prozent der Geschäftsführer für wahrscheinlich, dass ihr eigenes Unternehmen in den nächsten zwei Jahren Opfer eines Cyberangriffs wird.

Während solche Angtriffe zu Rufschädigungen führen können, verursachen diese in aller Regel auch erhebliche finanzielle Schäden. In einem Bericht des Cybercrime. Magazine von 2020 wird prognostiziert, dass die weltweite Cyberkriminalität bis 2025 jährlich 10,5 Milliarden 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-Audits 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, Risk und Compliance (GRC) einzuführen.

Diese neuen Erfordernisse haben eine neue GRC-Ära eingeleitet Eine Ära, in der das Management von SAP-Prozessen immer komplexer wird. Für Führungskräfte, die in diesem zunehmend komplexen Umfeld die Nase vorn haben wollen, ist es zunerlässlich, die Dynamik zu verstehen und künftige Entwicklungen vorauszusehen.

An dieser Stelle präsentieren wir Ihnen 4 wichtige Erkenntnisse und Prognosen vor, von denen wir glauben, dass sie für Unternehmen, die SAP im Einsatz haben, künftig außerordentlich bedeutsam werden.

Soterions Prognosen für die Zukunft von GRC in SAP

Prognose 1:

Der Mangel an qualifizierten Sicherheitspersonal wird aller Wahrscheinlichkeit nach die Risiken 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 standardisierten Geschäftsprozessen wird zu einer deutlichen Zunahme unberechtigter Systemzugriffe 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 zunehmender Cloud-Nutzung vermischen sich die Verantwortlichkeiten und die Risikoübernahme wird unscharf

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

Prognose 4:

Der Aufstieg des hybriden IAM/GRC-Modells

Bei der Vorteilsabwägung zwischen IAM- und GRC-Lösungen werden immer mehr Unternehmen ein Hybridmodell in Betracht ziehen, dass die Stärken beider Systeme miteinander verbindet.

Prognose 1:

Der Mangel an qualifizierten Sicherheitspersonal wird aller Wahrscheinlichkeit nach die Risiken erhöhen

Die Verwaltung von SAP-Berechtigungen ist eine anspruchsvolle und komplexe Aufgabe. Sie erfordert sowohl ein fortgeschrittenes technisches Know-How als auch ein tiefgreifendes Verständnis der Systemdetails. Die Ausbildung zum kompetenten SAP-Sicherheitsadministrator dauert Jahre. Mit der zunehmenden Komplexität, S/4HANAProzesse zu managen, müssen Unternehmen möglicherweise ihre Sicherheitsanstrengungen verdoppeln, um ihre Aufgaben zu bewältigen.

Angesichts erheblicher Veränderungen im S/4 Sicherheitsmanagement könnte es sein, dass viele erfahrene SAP-Sicherheitsfachleute in der Nähe des Renten alters, sich nicht mehr mit den neuen, technischen Herausforderungen befassen Wollen. Eine mögliche Folge wäre der Verlust an hoch qualifizierten Fachkräften Damit stehen Unternehmen vor der Aufgabe, neue Mitarbeiter einzustellen 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 Fachkräfte gibt, die dafür in Frage kommen. Wenn es um spezialisierte Fähigkeiten wie die Verwaltung von SAP-Berechtigungen geht, ist der Qualifikationsrückstand/Ausbildungsrückstand sogar noch größer.

Der Übergang zur Remote-Arbeit wie etwa Home Office hat den Mangel an SAP-Sicherheitsfachkräften weiter verschärft. Die herkömmlichen Trainingsmaßnahmen vor Ort (am Arbeitsplatz) haben sich als der beste Weg zur Vermittlung von Fach Know-How erwiesen. Durch Remote Arbeit wird dieser Trainingsprozess jedoch verkompliziert und 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. Das Erfordernis einer effizienten Berechtigungsadministration kann weniger erfahrene Administratoren dazu verleiten, großzügiger Zugangsrechte zu vergeben, um Arbeitsunterbrechungen zu vermeiden. Das kann zu Systemausfällen, Ineffizienz und Frustration am Arbeitsplatz führen.

Infolge dieser Herausforderungen kann es für viele Unternehmen schwierig werden, qualifizierte SAP Fachkräfte im Bereich der SAP Berechtigungsadministration zu finden. Um einen angemessenen Berechtigungszugang zu gewährleisten, müssen alternative Maßnahmen und Lösungen wie etwa Outsourcing oder Managed Services in Betracht gezogen werden. In den kommenden Jahren wird eine deutliche Entwicklung hin zu neuen Ansätzen und Lösungen erwartet, um die zunehmende Komplexität der SAP-Sicherheit in einer S/4HANA Welt zu bewältigen.

Prognose 2:

Das Streben nach standardisierten Geschäftsprozessen wird zu einer deutlichen Zunahme unberechtigter Systemzugriffe führen

Die aktuelle Forderung von SAP standardisierte Geschäftsprozesse einzusetzen und insbesondere die Tatsache, dass SAP Implementierungspartner empfehlen, vordefinierte Business Rollen einzusetzen, bedeutet eine wesentliche Veränderung der SAP Welt. Mit solchen Standardrollen soll die Implementierung und Administration so schlank wie möglich gestaltet werden, allerdings gewähren sie gleichzeitig einen ungemessen großzügigen Benutzerzugriff, der ein hohes Bertrugsrisiko zur Folge hat.

Unternehmen sind in der wirklichen Welt keine Gebilde mit Einheitsgröße. Jedes Unternehmen hat seine spezifischen Anforderungen und Arbeitsprozesse. Daher ist es wenig wahrscheinlich, dass Standardrollen die passende Lösung sein werden. Um mögliche Betriebsunterbrechungen zu vermeiden, erhalten SAP User gleich mehrere Business-Rollen, damit sie Berechtigungszugriffe für alle denkbaren Aufgaben haben. Diese Vorgehensweise hat jedoch erhebliche Nachteile.

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 standardisierten Geschäftsprozesse von SAP vollständig übernehmen werden. Sofern dieser Weg verfolgt wird, sollte man sich der damit verbundenen Risiken in vollem Umfang bewusst sein.

Ob man sich nun für benutzerdefinierte Rollen oder für standardisierte Business-Rollen entscheidet, wird es bei einer S/4HANA Migration unabdingbar sein, im Vorfeld ein solides Rollendesign zu erstellen.

Leider werden in vielen Projekten erst in einem späteren Stadium solche Sicherheitsfragen berücksichtigt, was häufig zu übereilten und fehlerhaften Implementierungen führt. In einem Live-System können solche Änderungen des Benutzerzugriffs sehr störend sein und zu Unterbrechungen der Abläufe führen. Daher sollten bereits vor einer Migration alle Zugangsrechte und Prozesse präzise definiert sein.

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

Prognose 3:

Mit zunehmender Cloud-Nutzung vermischen sich die Verantwortlichkeiten und die Risikoübernahme wird unscharf

Ursprünglich konnten Unternehmen ihre Abläufe in einem einzigen SAP-System verwalten. Mit wachsender Komplexität und der rasanten Verbreitung technologischer Lösungen kam im zunehmenden Maße ein Best-of-Breed-Ansatz zum Einsatz. Diese Strategie hatte zur Folge, dass viele Lösungen in die SAP Umgebung integriert wurden, um wichtige Funktionalitäten zu erweitern.

So wurden SAP- Funktionalitäten durch Cloud-basierte Lösungen ersetzt, wie etwa HCM durch SuccessFactors oder Procurement durch Ariba. Oder Teile von SAP werden durch Cloud-Plattformen wie Workday oder Coupa zu ersetzt. Jede dieser Lösungen hat ihr eigenes Sicherheitskonzept, was die SAP-Administration vor zusätzliche Herausforderungen stellt.

Viele Berechtigungskontrolllösungen sind leider nicht in der Lage, für diese Cloud-Lösungen eine umfassende Analyse des Zugangsrisikos durchzuführen. Ein klares Bild der Risikoexposition eines Unternehmens wird dadurch zunehmend schwierig. Das Sicherheitsteams muss mit den Sicherheitsprotokollen aller integrierten Lösungen vertraut gemacht werden und über genügend Ressourcen verfügen, um diese effektiv zu verwalten. Eine Lösung zur Zugangskontrolle muss eine Analyse des Zugangsrisikos durch die Cloud-Lösungen unbedingt berücksichtigen.

Dies ist nicht die einzige Herausforderung durch eine Cloud-Anbindung. SAPs Bestrebungen, Kunden über das SAP-Programm Rise für ein Cloud-Hosting zu gewinnen, erhöht diese Komplexität noch weiter. Kunden können wählen, ob sie ihre SAP-Systeme in einer privaten Cloud, etwa einem Hyperscaler wie AWS oder Azure, oder in der SAP-eigenen öffentlichen Cloud hosten lassen.

Diese Verlagerung in die Cloud erhöht zwar die Skalierbarkeit und Performance und bringt Kostenvorteile, führt aber auch zu unklaren Zuordnungen bezüglich der jeweiligen Verantwortlichkeiten.

Erhebliche Herausforderungen und potenzielle Auseinandersetzungen zwischen SAP und ihren Kunden sind aus unserer Sicht bei Fragen der Verantwortungszuordnung vorprogrammiert. 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 Sicherheitsmaßnahmen abgedeckt sind, wenn Sie sich für SAP-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, Risk und Compliance (GRC) im Mittelpunkt des Interesses. Unternehmen wollen die Bedeutung und den möglichen Mehrwert der jeweiligen Lösungen 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 miteinander, verbunden mit dem Versprechen, 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, ein entscheidendes Element fehlte jedoch. Den meisten IAM-Lösungen fehlt die Möglichkeit den SAP-Zugang auf einer detaillierten oder technischen Ebene zu analysieren, also hinunter bis zur Objektebene und den Berechtigungsfeldern.
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.

Unternehmen, die SAP einsetzen, benötigen unbedingt ein detailliertes Instrumentarium zur Steuerung ihrer Zugangsrisiken. Business User treffen ständig Entscheidungen mit einem erheblichen Risikopotenzial, über die Risiken selbst haben sie jedoch in aller Regel wenig Informationen. Wenn beispielsweise eine jährliche Überprüfung des SAP-Benutzerzugangs mit einer IAM-Lösung durchführt wird, kommt es häufig vor, dass Prüfer lediglich anhand des Rollennamens prüfen, ob eine SAP-Rolle für Benutzer geeignet ist. Es können keine Informationen über die tatsächliche Rollennutzung und des damit verbundenen Zugangsrisikos generiert werden, da IAM diese detaillierten Informationen gar nicht auf die gleiche Weise wie eine GRC-Lösung anzeigen kann.

Da das Problembewusstsein für solche Sachverhalte zunimmt, denken wir, dass immer mehr Unternehmen ein hybrides IAM/GRC-Modell in Betracht ziehen werden, bei dem Business Rollen in der GRC-Lösung definiert werden. Dieser Ansatz macht Zugangsrisiken und Nutzungsinformationen transparent, so dass User von Business Rollen die richtigen Entscheidungen bei dem Einsatz dieser Rollen treffen können.

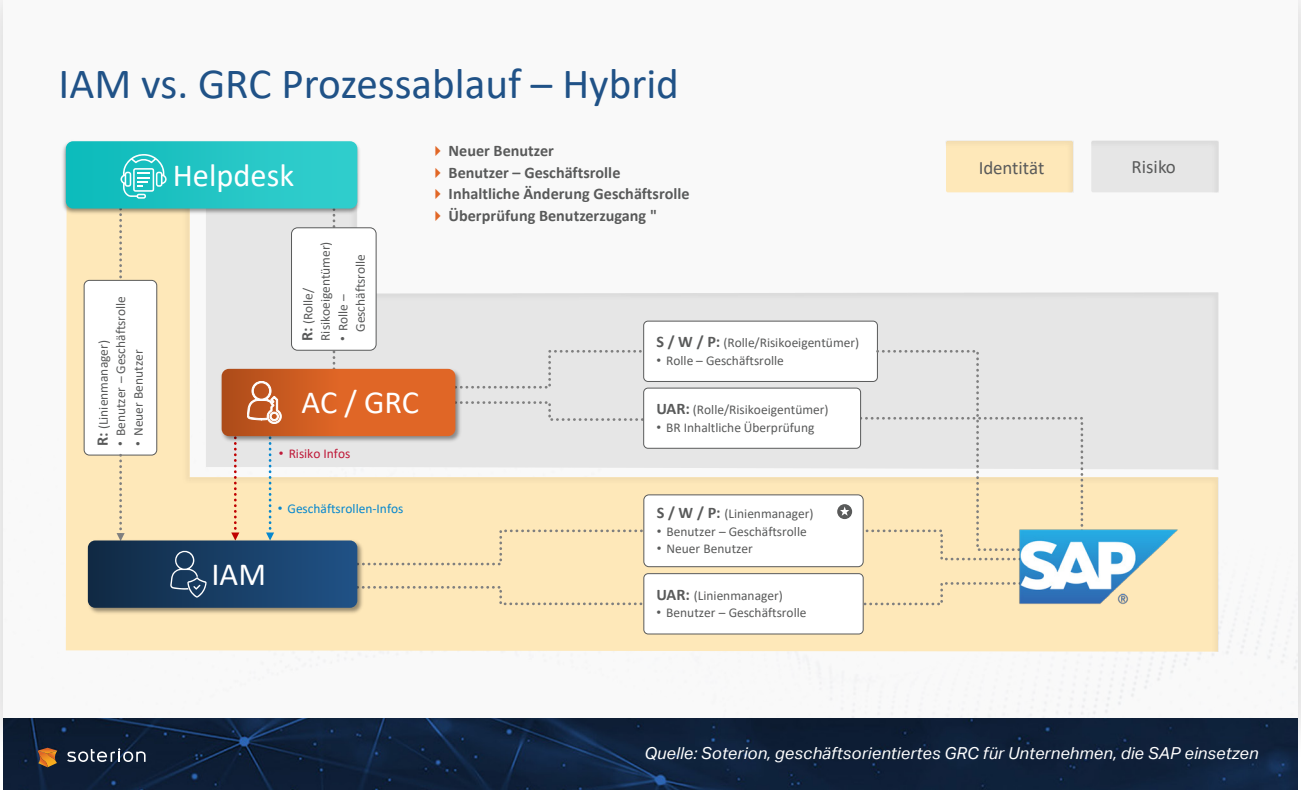
Es ist offensichtlich, dass sowohl GRC- als auch IAM-Lösungen wichtige Funktionen erfüllen.
Die Verknüpfung der beiden Lösungen hat sich in der Praxis jedoch als schwierig erwiesen, da sich ihre Funktionen überschneiden. Wenn beide Lösungen miteinander kombiniert werden, wird es erfolgsentscheidend sein, welche Lösung welche Aufgaben im Einzelnen übernehmen soll wie etwa Steuerung der Workflowprozesse, Bereitstellung des Benutzerzugangs etc.

Prognose 4:

Der Aufstieg des hybriden IAM/GRC-Modells

Das hybride Modell kann eine der folgenden Formen annehmen:

- **Hybrid 1:** Während die GRC-Lösung alle sich überschneidenden Funktionen der SAP-Systeme übernimmt, ist die IAM-Lösung für alle Nicht-SAP-Systeme verantwortlich.
- **Hybrid 2:** Die GRC-Lösung übernimmt die Definition der SAP-Business-Rollen und die IAM-Lösung ist für die Bereitstellung dieser Rollen und die Überprüfung des Benutzerzugangs (auf Geschäftsrollenebene) zuständig.



soterion

Quelle: Soterion, geschäftsorientiertes GRC für Unternehmen, die SAP einsetzen

Entscheidend ist, alternative Ansätze für die Bereitstellung von Zugangsrechten gründlich zu prüfen, insbesondere was eine Potenzialanalyse von Azure AD und SAP Identity Provisioning Service (IPS) betrifft.

Schlussfolgerungen

Die ständig wachsende Komplexität von SAP-Umgebungen zeigt deutlich, wie wichtig zukunftsorientierte Sicherheitsstrategien sind. Mit der anstehenden S/4HANA Migration wird es besonders wichtig, die Sicherheit nicht mehr als Randthema zu betrachten, sondern vielmehr in den Mittelpunkt der (Ihrer) Projektplanung und -ausführung zu stellen.

Die S/4HANA Migration ist nicht nur ein Upgrade, sondern verändert Abläufe im Unternehmen in dramatischem Ausmaß. Wenn vor dem Upgrade die Rollen überprüft werden, wird ein erheblicher Teil der Vorarbeit bereits im Voraus geleistet. Zudem muss unbedingt gewährleistet sein, dass alle Richtlinien und Verfahren nicht nur laufend aktualisiert, sondern auch in der betrieblichen Praxis eingehalten werden.

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 Ihrer internen Richtlinien an die spezifischen Anforderungen Ihres Unternehmens ist ein weiterer unabdingbarer Aspekt. Anstatt sich mit dem Out of the Box Standard-Regelsatz Ihres Anbieters von Zugangskontroll- oder GRC-Lösungen zu begnügen, können Sie die Genauigkeit und Relevanz für Ihr Unternehmen erhöhen, indem Sie den Regelsatz für sich 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 während des Projekts zusätzliche Budgets oder weitere fachliche Unterstützung anfordern 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.

Gehen Sie mit Zuversicht in eine (die) GRC Zukunft

Soterion ist darauf spezialisiert, Unternehmen bei der Optimierung ihrer SAP-Prozesse zu unterstützen, und zwar in Bezug auf Governance, Risk und Compliance (GRC). Wir sind darauf spezialisiert, für Unternehmen die besonderen Chancen zu erkennen und Antworten auf die Herausforderungen zu finden, die es bei der Implementierung von GRC gibt.

Viele Menschen fühlen sich von SAP GRC Lösungen aufgrund Ihrer scheinbaren Komplexität und Kosten überfordert, was sie zögern lässt, den GRC Implementierungsprozess überhaupt zu beginnen. Andere haben möglicherweise das Gefühl, dass sie die Vorteile ihrer SAP GRC-Software nicht vollständig ausschöpfen können.

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 entwirren, zu vereinfachen und zu beschleunigen.

BUCHEN SIE NOCH HEUTE EINE DEMO