A New Era of GRC for SAP Customers

The Road Ahead: **Soterion's Insights and Predictions**

soterion

There are challenges on the horizon for organisations using SAP. An increasing number of organisations are making the transition to S/4HANA with the rapidly approaching upgrade deadline. One source estimates that around 22,000 customers have licenced S4, with approximately two-thirds of those having completed an implementation.

While the move to S4 brings many benefits in terms of speed, flexibility, and analytics power, it also creates greater complexity. This leap forward is more than a simple software upgrade; it represents a major shift in how organisations will secure their data in the face of rapidly evolving business processes.

As with many large digital transformation projects, security has traditionally taken a backseat, as organisations focus on configuration and maintaining business-critical processes.

The need for robust security is becoming undeniable with a noticeable uptick in security incidents over the last decade, including cyber-attacks and data fraud. Data from a 2023 World Economic Forum study found that 43% of organisational leaders think it is likely a cyberattack will materially affect their own organisation within the next 2 years.

As well as causing reputational damage, these kinds of attacks can have significant financial consequences. A report by Cybercrime Magazine in 2020 forecast that by 2025, global cybercrime would cost USD $10.5 trillion annually – exponentially larger than the damage inflicted from natural disasters, and more profitable than the global trade of all major illegal drugs combined.

The growing rigour of SAP audits presents an additional challenge. Regulatory bodies are adopting increasingly strict measures to ensure compliance, intensifying the pressure on businesses to properly secure their SAP environments and adopt stringent Governance, Risk and Compliance (GRC) measures.

These mounting pressures have ushered in a new era of GRC. One where managing SAP environments is likely to become more complex than ever before. Understanding the dynamics at play and anticipating future developments is essential for leaders aiming to stay ahead in this increasingly complex environment.

We share **four pivotal insights and predictions** that we believe will shape the future of GRC for companies running SAP in this report.

Soterion's Predictions for the Future of GRC in SAP

Prediction 1:

Shortage of skilled SAP security resources may increase risk exposure

The anticipated increase in SAP security complexities, coupled with a global skills shortage, may expose organisations to increased risk as they struggle to find adequately skilled SAP security resources.

Prediction 2:

The drive towards standard business processes will cause widening of access

Amid the push for adoption of standard business processes and pre-defined roles, organisations may be forced to assign multiple roles to users, consequently broadening access and increasing organisational risk.

Prediction 3:

As cloud adoption increases, clarity on ownership and risk exposure becomes blurred

The increasing adoption of third-party cloud solutions is causing ambiguity in access risk exposure, and the push to SAP's cloud raises questions around ownership and management of security.

Prediction 4:

The rise of the hybrid IAM/GRC model

As organisations weigh up the benefits of IAM vs GRC solutions, more will consider a hybrid model that leverages the strengths of each system.

Prediction 1:

Shortage of skilled SAP security resources may increase risk exposure

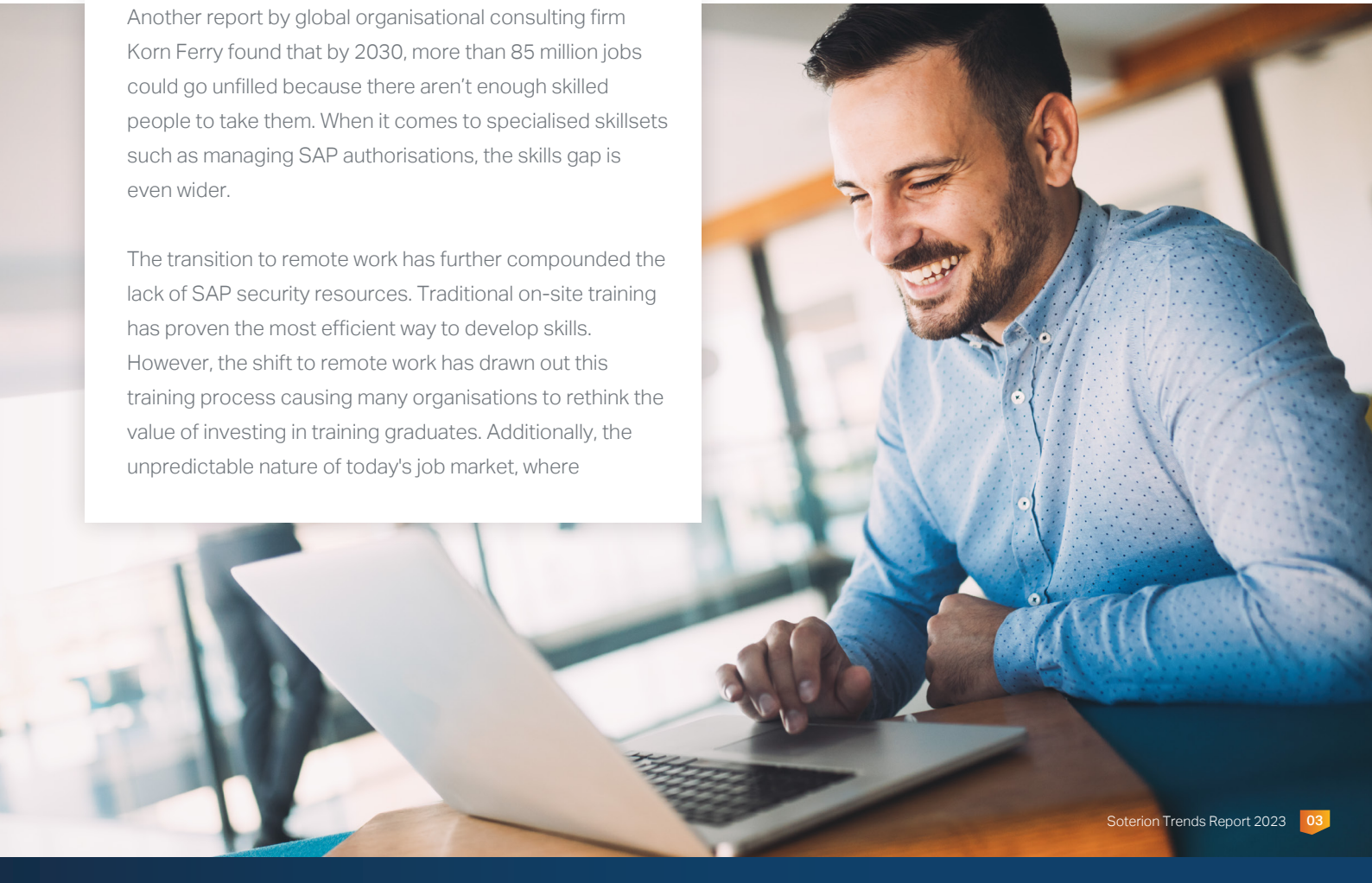
Managing SAP authorisations is a demanding and complex task. It requires both advanced technical skills and a deep understanding of system intricacies. It takes years of training to become a proficient SAP security administrator, and with the expected increase in complexity of managing S/4HANA, organisations may find themselves needing to double their security resources to manage it well.

In light of the significant changes to how security is managed in S4, many veteran SAP security professionals nearing the end of their careers may be reluctant to adapt to these new approaches, potentially leading to a loss of senior talent. This leaves organisations with the prospect of recruiting and training new people - a significant challenge amid the massive global skills shortage we're experiencing.

A 2021 McKinsey report found that 87% of companies worldwide have skill gaps, or expect to within a few years. Another report by global organisational consulting firm Korn Ferry found that by 2030, more than 85 million jobs could go unfilled because there aren't enough skilled people to take them. When it comes to specialised skillsets such as managing SAP authorisations, the skills gap is even wider.

The transition to remote work has further compounded the lack of SAP security resources. Traditional on-site training has proven the most efficient way to develop skills. However, the shift to remote work has drawn out this training process causing many organisations to rethink the value of investing in training graduates. Additionally, the unpredictable nature of today's job market, where employees can easily take their newly acquired skills elsewhere, deters many from investing in upskilling. This skills shortage is likely to have several knock-on effects. Inefficiently managed access can expose organisations to greater risk, as less experienced administrators may grant broader access than necessary to avoid workflow blockages. This could lead to system downtime, inefficiency, and workplace frustration.

Given these challenges, we predict a significant number of organisations will struggle to find the skilled SAP security resources needed. To maintain appropriate access control, these organisations may have to consider alternative models of support, such as outsourcing or managed services. We anticipate a noticeable shift towards these models in the coming years, as businesses seek to navigate the increasing complexity of SAP security in the S/4HANA era.



Prediction 2:

The drive towards standard business processes will cause widening of access

The recent push by SAP towards the adoption of standard business processes, and in particular, where implementation partners recommend using SAP's pre-defined business roles, represents a significant shift in the SAP landscape. These standard roles aim to streamline implementation and support, but they come with the downside of providing inappropriate, wide user access that places the organisation at unnecessary fraud risk.

The reality is that organisations are not a one-size-fits-all entity. Each organisation has its unique needs and workflows, making it unlikely that a standard role will provide the right level of access. To prevent potential operational bottlenecks, users are often allocated multiple business roles so they have the necessary access to perform all their functions. This approach, however, has its complications.

Assigning multiple roles often results in access privileges being wider than necessary, thus increasing organisational risk. It remains to be seen how many organisations will fully embrace SAP's standard business processes - those that do should be aware of the risks associated with overly broad access permissions.

For organisations opting to create custom roles, or who decide to use the standard business roles and customise them to be more specific to their organisation, it's crucial to ensure a sound role design before transitioning to S/4HANA. Unfortunately, security is often left as a late-stage consideration in many projects, resulting in hasty and potentially flawed setups. Altering user access in a live environment can be challenging and disruptive, so it's advisable to have SAP access and processes well-defined ahead of the move.

This proactive approach will likely require some rework, such as replacing Vendor and Customer Master transaction codes with Business Partners and integrating Fiori access. However, the benefits of a well-planned, secure access control setup in S/4HANA far outweigh the temporary inconvenience of this rework. The key is to plan security measures together with your migration, not as an afterthought.

Prediction 3:

As cloud adoption increases, clarity on ownership and risk exposure becomes blurred

There was a time when businesses running SAP could manage all their operations within a single system. However, as organisations have grown more complex, alongside the rapid proliferation of technology solutions, many have adopted a best-of-breed approach. This strategy involves integrating a variety of solutions into the SAP environment to enhance specific functionalities.

Examples include substituting core SAP functionalities with cloud-based solutions such as replacing HCM with SuccessFactors or Procurement with Ariba. Or you might choose to replace parts of SAP with cloud platforms like Workday or Coupa. These solutions each come with their own unique security concepts, making it a challenge to administer.

Unfortunately, many access control solutions lack the capability to perform a comprehensive access risk analysis on these cloud solutions. As a result, organisations may not have a clear picture of their risk exposure. It's essential for security teams to be familiar with security protocols for all integrated solutions, and to have enough resources to manage them effectively. Look for an access control solution that has the ability to perform access risk analysis for the cloud solutions in scope at your organisation.

This is not the only challenge associated with the cloud. SAP's initiative to incentivise customers to transition to cloud hosting via the SAP Rise programme is further adding to this complexity. Customers can choose to have their SAP systems hosted on a private cloud, for example a hyperscaler like AWS or Azure, or SAP's own public cloud.

While this shift to cloud hosting brings about scalability, performance, and cost benefits, it has led to a lack of clarity regarding responsibility for various activities.

SAP has indicated that they will handle the basic system administration, leaving the rest to the customer. However, the division of responsibilities is not clear-cut. Particularly when it comes to security, there's a degree of overlap and potential gaps in responsibilities which could increase an organisation's risk of access breaches.

We foresee significant challenges and potential disputes between SAP and customers around responsibilities in this area. As we await further clarity from SAP on roles and responsibilities, make sure you understand who is handling which activities to ensure appropriate security measures are covered, if you opt for the SAP Rise program.

Prediction 4:

The rise of the hybrid IAM/GRC model

Within the intricate ecosystem of SAP environments, the conversation around Identity and Access Management (IAM) and Governance, Risk and Compliance (GRC) solutions is taking center stage, with organisations keen to understand the role and potential value of each.

IAM solutions were created to manage an identity across an IT environment and facilitate the Joiner-Mover-Leaver process. The promise of these solutions, which integrate multiple systems, was to solve prior provisioning challenges and accelerate onboarding and user provisioning processes. While they indeed introduced significant efficiencies, they were missing a crucial element. Most IAM solutions lack the ability to analyse SAP access at a detailed or technical level, for example drilling down to SAP authorisation object or field. So, while IAM solutions are excellent at provisioning access, they often fall short when assessing the risk impact of the SAP roles being assigned.

Detailed access risk capabilities is imperative for organisations running SAP. Business users are making decisions with limited information without risk information. For instance, if your organisation performed its annual SAP User Access Review in an IAM solution, the reviewers would make decisions on whether an SAP role was appropriate for users based merely on the role name. It would not highlight usage information or the access risk impact of this role as it does not have the ability to show this detailed information in the same way as a GRC solution.

As awareness of this issue grows, we predict more organisations will consider a hybrid IAM/GRC model where Business Roles are defined in the GRC solution. This approach will make access risk and usage information visible, enabling business role owners to make informed decisions about the role's contents and composition.

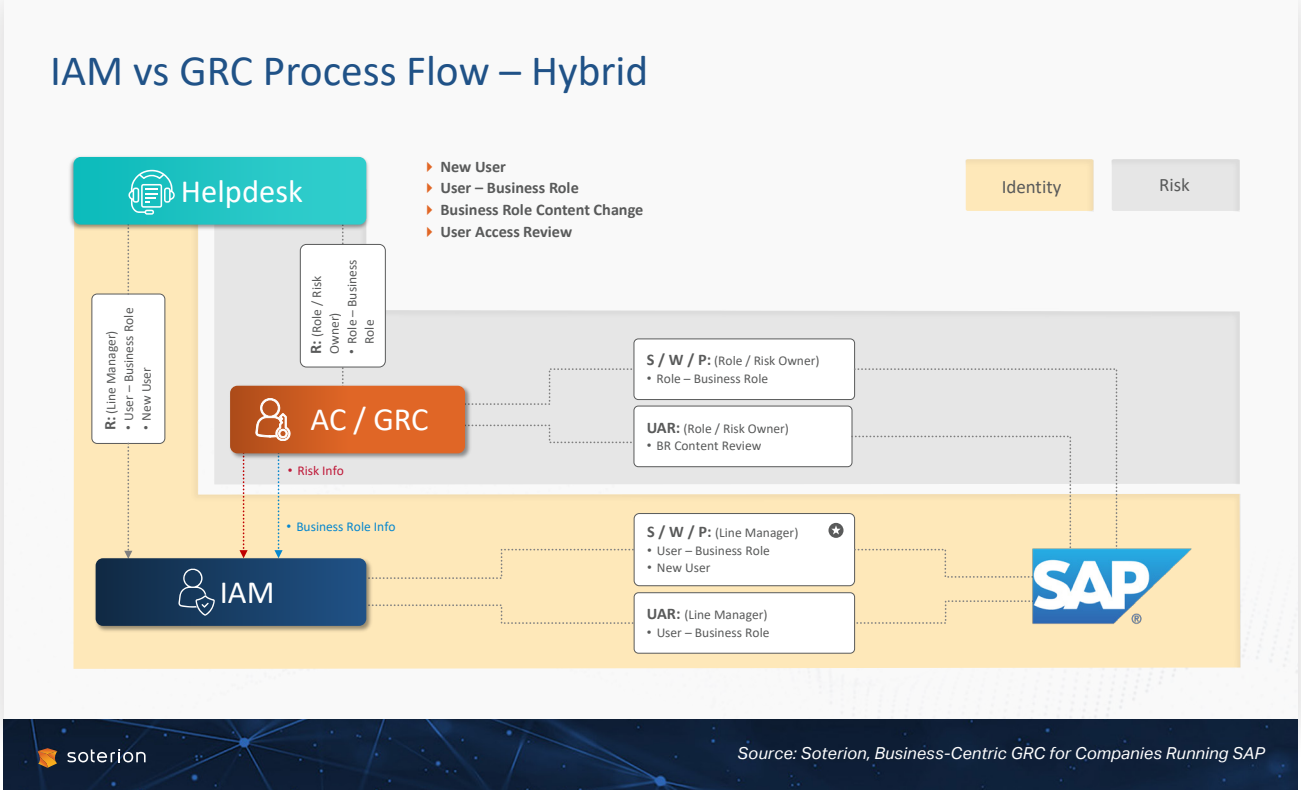
It's evident that both GRC and IAM solutions serve important roles, but integrating the two has proved difficult in practice due to the over-lapping functionality between the two solutions. Choosing which solution performs each function, such as workflow, provisioning and user access, is a critical factor in the success of combining these solutions.

Prediction 4:

The rise of the hybrid IAM/GRC model

The hybrid model might take one of the following forms:

- **Hybrid 1:** Use the GRC solution for all overlapping functions for the SAP systems, and the IAM solution for all non-SAP systems.
- **Hybrid 2:** Use the GRC solution to define the SAP Business Roles, and the IAM solution for the provisioning of these roles and User Access Reviews (performed at the Business Role level).



It is crucial to thoroughly explore alternative approaches for provisioning access, particularly by exploring the potential of Azure AD and SAP Identity Provisioning (IPS). Understanding the roles and capabilities of these solutions to effectively accomplish organisational goals will be of utmost importance.

Conclusion

The ever-increasing complexity of SAP environments highlights the importance of forward-thinking security strategies. With the looming transition to S/4HANA, it is especially vital to move security from the periphery to the core of project planning and execution.

The migration to S/4HANA represents not merely an upgrade but a seismic shift in operations and control. As such, a significant proportion of the groundwork can be done in advance, with roles reassessed prior to the upgrade. It is also crucial to ensure that all policies and procedures are not only up-to-date but also embedded within your organisation's practices.

Equally important is to educate business users about their compliance tasks and obligations, creating a culture of security awareness and responsibility.

Customising your rule set to align with your organisation's specific needs is another vital consideration. Rather than settling for the standard, out-of-the-box rule set from your access control or GRC solution provider, tailoring it will enhance the accuracy and relevance to your organisation.

By taking these steps, you can significantly reduce the rework needed post-migration. Establishing a strong security foundation before the upgrade will also prevent you from scrambling to secure resources and budgets during the project itself.

Navigating the future of SAP environments requires anticipation, preparation, and continuous adaptation. By prioritising security in your strategic planning today, you'll be well-equipped to tackle the complex challenges of tomorrow.

Navigate the future of GRC with confidence

Soterion specialises in helping companies running SAP to maximise their Governance, Risk and Compliance (GRC) processes. We understand the unique opportunities and challenges that exist for most organisations when it comes to their GRC capability.

Many feel overwhelmed and intimidated by SAP GRC and its seeming complexities and expenses, and hence they are hesitant to even begin the process. Others may feel like they're not seeing the full benefit of their SAP GRC software.

We have developed a number of niche GRC tools with the aim of getting our customers to view GRC as a real benefit, not as a burden. Brought to you by our team of expert consultants situated around the world, we specialise in demystifying, uncomplicating and expediting the GRC process.

BOOK A DEMO TODAY