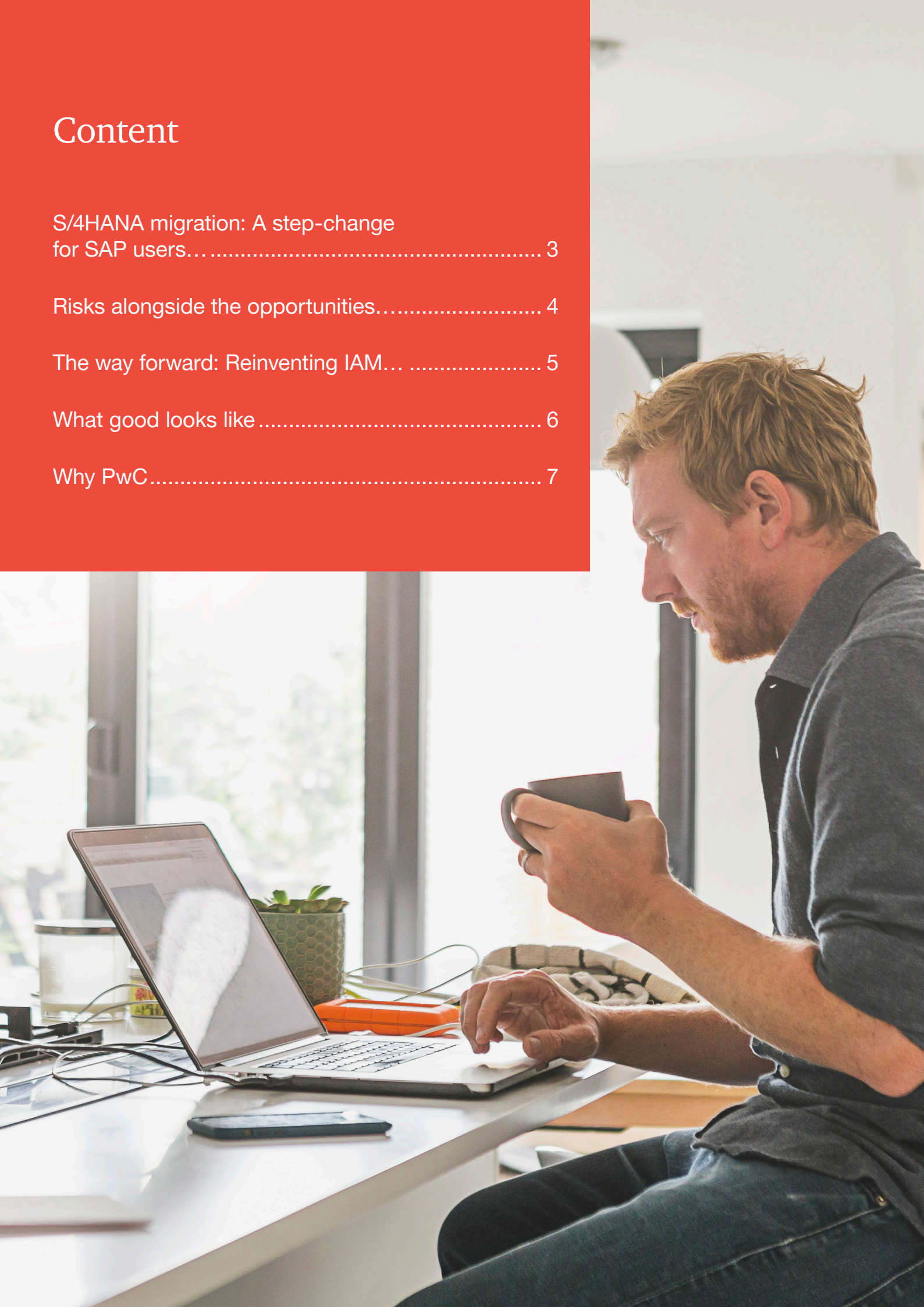
SAP S/4HANA transformation and digital identity

Why you need a new approach to access management

September 2020

pwc

Content



S/4HANA migration: A step-change for SAP users…

SAP has set end of 2027 as the date when support for its Business Suite 7 core Applications[1] will end. For most companies currently using SAP to power their business, the question is not if they will migrate to SAP's next-generation ERP system, S/4HANA – but when. To ensure continuity of their business and systems through the transition, these companies' migration programs should already be underway – or at least at the advanced planning stage.

The fact that SAP users are making the move to S/4HANA reflects the advantages it offers over previous releases. S/4HANA is an intelligent, integrated ERP system that runs on a fast and powerful in-memory database. It can help companies to ramp up new business models quickly and easily, make better decisions faster, and reinvent their IT landscape to make it a better fit for their business.

S/4HANA delivers these opportunities through three main attributes:

Open architecture

New architecture based on modern, open standards and interconnectivity, opening the way to connected value chain models and use-cases.

Automation and intelligence

S/4HANA allows for the revolutionising of business processes with intelligent automation — supported by artificial intelligence (AI) and robotic process automation (RPA).

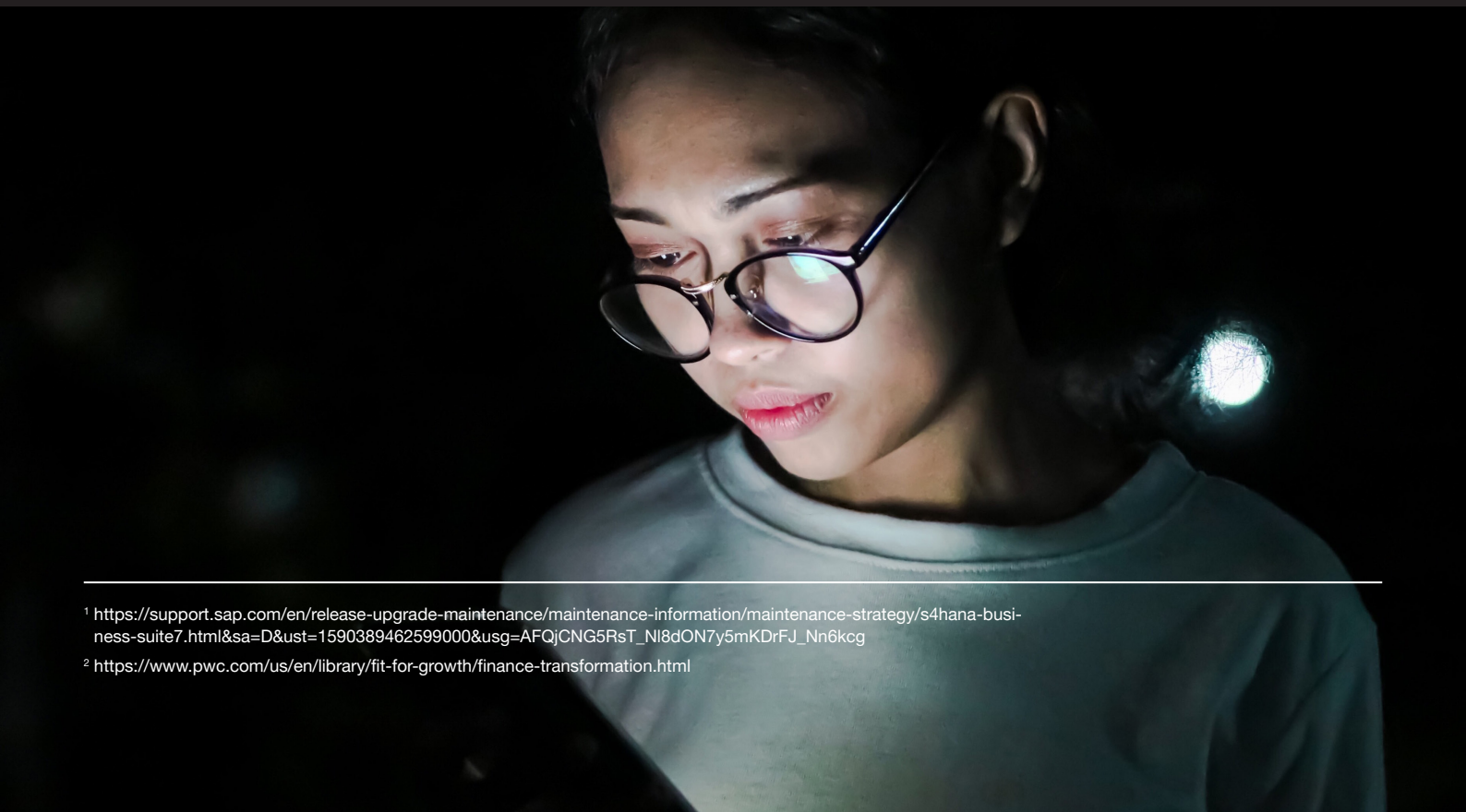
Infrastructure flexibility

Various deployment topologies like on-premise, hybrid cloud/on-premise, or in the cloud, all with a consistent data model, code line, and enhanced, conversational user interface and experience.

"…Involving both business and technology transformation[2]

The migration to SAP S/4HANA is a major undertaking, involving transformation in two dimensions. First, it's a **business transformation** – reshaping an organisation's entire financial landscape. And second, it's a **technology transformation**, transferring systems and data to an entirely new platform with enhanced capabilities.

The investment in time and resources required to move to S/4HANA, makes it one of the biggest and most important projects on our client's strategic agenda.



[1] https://support.sap.com/en/release-upgrade-maintenance/maintenance-information/maintenance-strategy/s4hana-business-suite7.html&sa=D&ust=1590389462599000&usg=AFQjCNG5RsT_Nl8dON7y5mKDrFJ_Nn6kcg

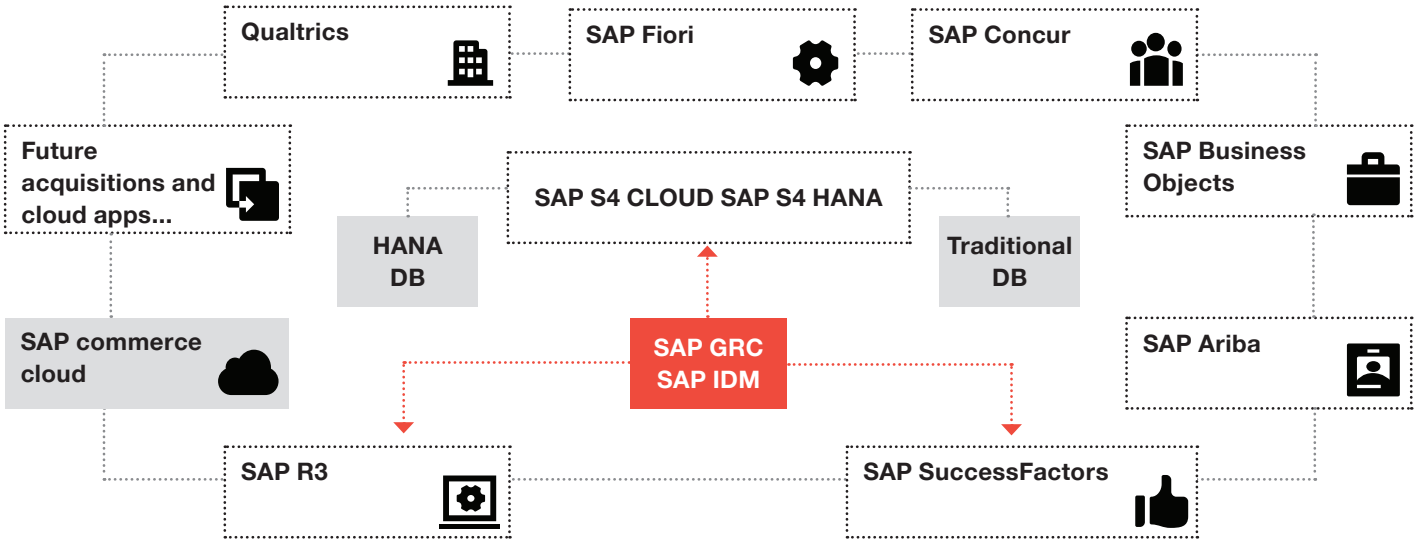
[2] https://www.pwc.com/us/en/library/fit-for-growth/finance-transformation.html

Risks alongside the opportunities…

Like any large project offering major benefits, S/4HANA migration also brings risks. Since it involves transforming the critical systems and processes at the heart of the organisation, and must be completed by a hard deadline, failing to make the transition by the 2027 cut-off point is simply not an option. And even if a company executes the twin-track transformation successfully, there are still risks to address around compliance, as well as real business risks in many areas – not least identity & access management (IAM) and fraud prevention.

The SAP environment shown in Figure 1 underlines the nature and scale of these risks. With the new S/4HANA model and SAP's various function-specific acquisitions integrated around it, the SAP landscape can become like a regular enterprise in itself – with a wide array of distributed and siloed applications, different security models, no centralised management, and a mix of SAP/non-SAP and cloud/on-premise components.

Figure 1: The diverse and connected SAP S/4HANA environment



"…not least around IAM

What's more, the move from the relatively closed SAP Business Suite – with a VPN as the external access method – to the open architecture S/4HANA means there are now many different ways for users-and systems – to access the various functions in the systems environment. Yet SAP's Privileged Access Management (PAM) and Identity Governance Administration (IGA) solutions cover the main SAP components. However, looking at the features of this transformation, the deployment options require a broader look towards the infrastructure security, including an integration strategy with enterprise wide PAM and IGA solutions. The features with the most significant impacts on security are listed in Table 1.

All of this means that, in the S/4HANA's world, an integrated IGA and PAM approach is needed between SAP and non-SAP applications, in order to control and monitor access to the diverse blend of SAP/non-SAP components, manage risks effectively, and minimise the need for manual controls. Companies need to move to an IAM approach based on business roles, and implement a consistent structure around this for both cloud and non-cloud solutions. It's a major challenge – and one that companies cannot afford to get wrong, as they put S/4HANA at the heart of their business and technology transformation.

Table 1: Features of S/4HANA with significant impacts on security

1 Rebuilt S/4 business logic

SAP Business suite
Implementation of enhanced/adjusted transactions, programs and objects (and database structure) providing new business functionalities

2 Introduced components and technologies

SAP HANA Platform
Moving to a new database technology as well as developing and provisioning applications and web services directly out of the database platform

SAP Fiori
Moving to web technology and providing access to business data to all end devices

3 Introduced cloud and third-party products

SAP Cloud application
Moving from on-premise to selected cloud applications (e.g. Fiori for cloud, SuccessFactors) due to SAP's or based on your IT strategy

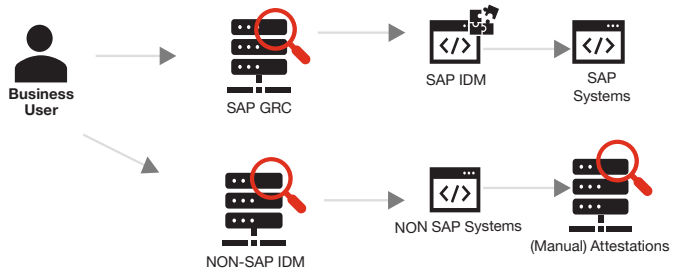
Third-party products
Using selected third-party products (and their interfaces) to enhance business functionalities

The way forward: Reinventing IAM…

The solution involves moving from a traditional user access architecture to a modern, holistic and integrated IGA architecture. An example of a typical architecture pattern is shown in Figure 2, where the approach is to not integrate across SAP Governance Risk Compliance (GRC) and non-SAP identity management (IDM), and often involves manual attestations, impacting speed and efficiency and increasing the risks of errors or fraud.

Figure 2: Traditional user access architecture

From this....



This siloed approach is no longer fit for purpose in an S/4HANA environment, for several reasons. With S/4HANA's increased access surface, IAM risk considerations reach further than the traditional SAP landscape – meaning a standalone IAM strategy and process for SAP user access and identity governance increases risk and compliance issues. Similarly, SAP S/4HANA is heavily integrated with other (non-SAP) systems, meaning the enterprise processes, architecture and supporting systems need to be revisited.

The need for an integrated approach is reinforced by S/4HANA's wider implications for security. The integrated business processes and proliferation of connectivity in an S/4HANA environment increase digital risk exposure, while AI, Robotic Automation Process (RPA) and connected ecosystem use cases drive complexity in the IT landscape, requiring different ways to deal with security.

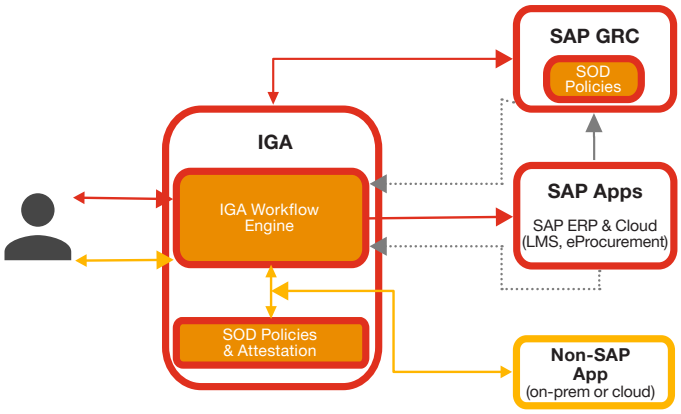
Furthermore, the automation of a large proportion of these processes will increase the severity of potential incidents. Also, existing IAM processes and solutions may not be competent, covering off either SAP or Non-SAP domains. And taking an integrated approach is made even more important by the SAP landscape becoming a heterogeneous set of cloud/non-cloud platforms with their own access controls and security models, connected to the non-SAP world as well.

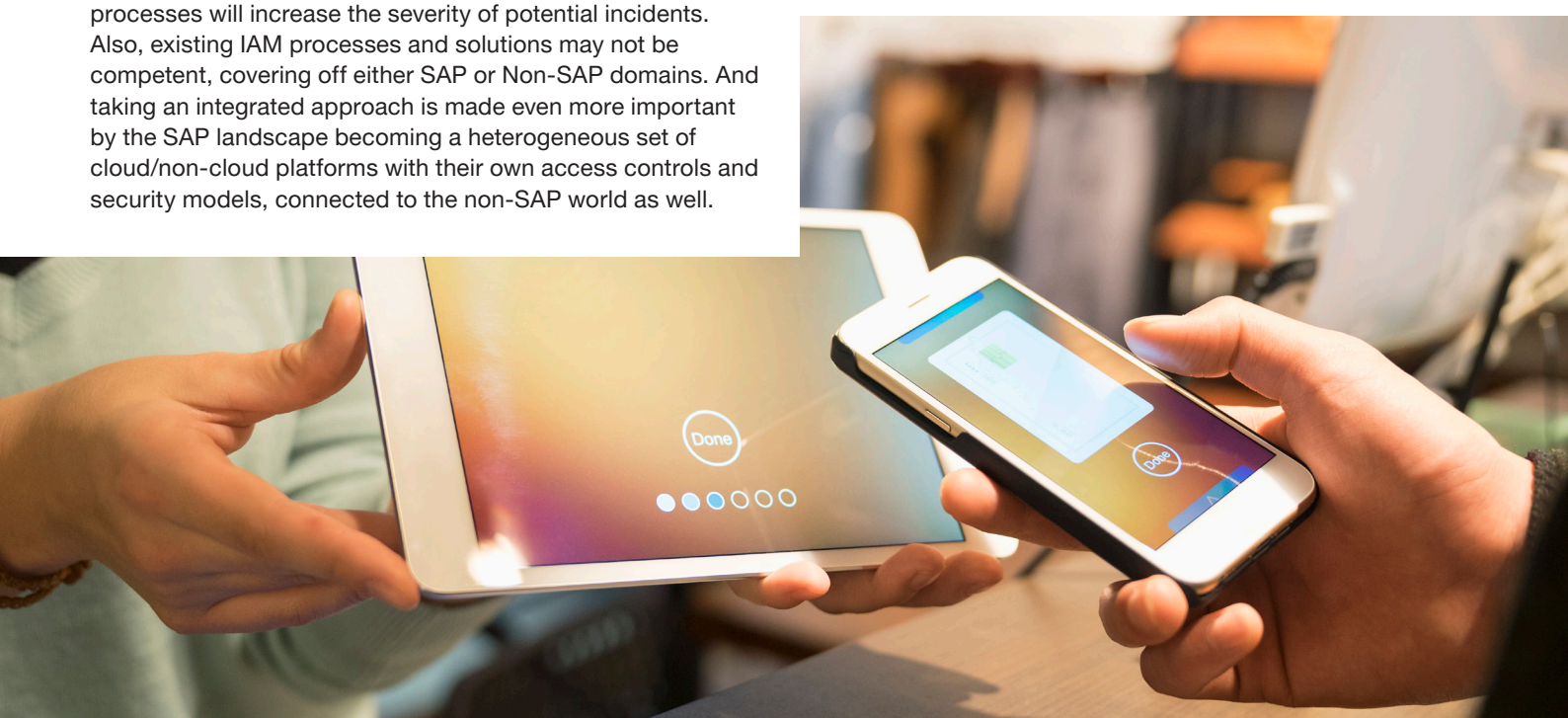
> **"…through an integrated IGA architecture**
>
> All of these factors point to the need to move to the integrated IGA architecture shown in Figure 3. Potential measures to further improve security include defining and implementing new controls – or perhaps adopting them from other functional domains into SAP – to support AI, robotics and connected ecosystem use cases.

Also, the access controls framework will need to be updated and implemented by introducing one single IAM governance and process landscape which has a cross-domain effectiveness, including preventive and detective Segregation of Duties (SoD) validation checks. Another recommended measure is to use cross-domain Identity Governance and PAM capabilities that are able to support both platforms, helping to reduce risks and maintain compliance.

Figure 3: Modern, integrated IGA architecture

....to this





What good looks like

A company that takes the optimal approach to IAM for the S/4HANA world will end up with an integrated IAM security architecture of the type shown in Figure 4. This is the holistic systems landscape that companies need to get under control. To function effectively, the controls should be created with a keen awareness of the need to minimise fraud risks. For example, if the same employee is authorised both to issue and approve invoices, there's clear potential for abuse. External risks also need to be addressed rigorously, given the multiplicity of entry points created by S/4HANA's open architecture.

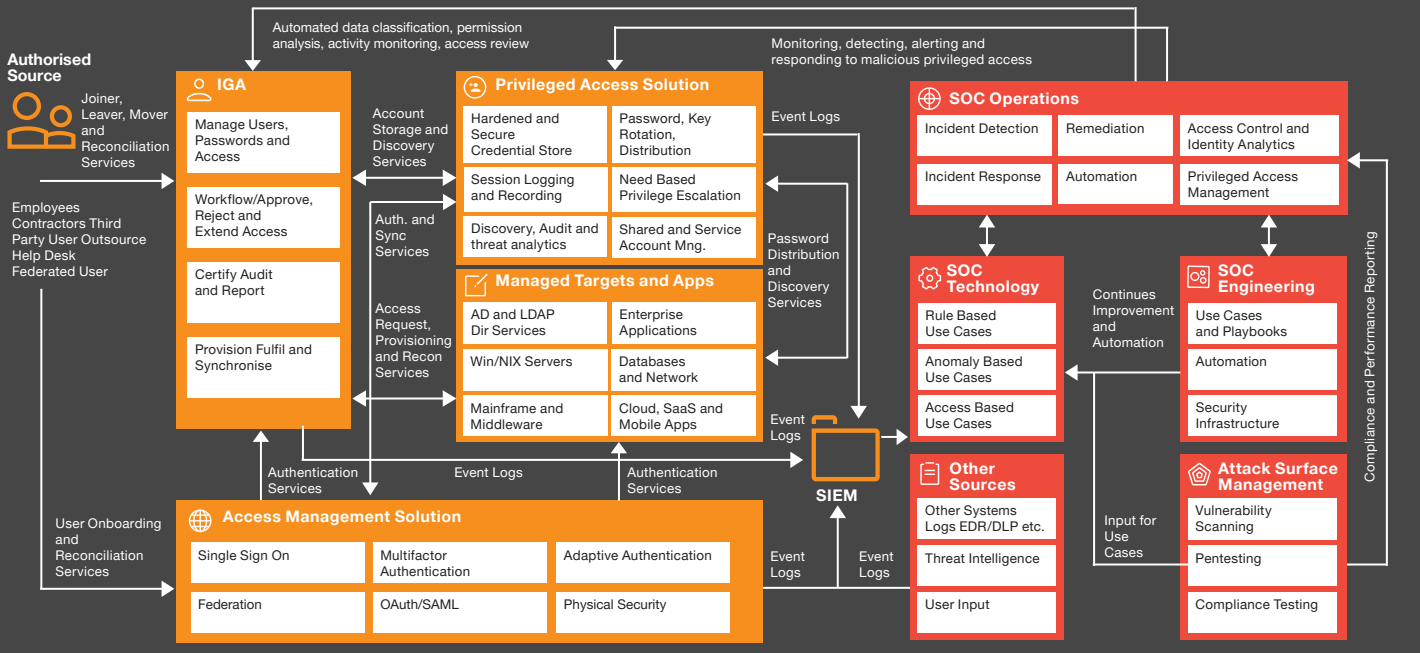
The overall outcome? An IAM environment that's smarter, more automated, more efficient and more secure, and reduces the costs and risks of compliance. For a company migrating to S/4HANA, we believe this isn't an optional nice-to-have. It's a must-have imperative.

In many customer cases, we do see a historically grown SAP authorisation concept which is partly disjunct from the standard office IT aka Windows/Active Directory world. This needs to change. Due to the complexity that comes with the different SAP products, it is no longer a standard SAP User&Role concept, it becomes much broader. The access control concept within SAP Ariba for instance, is way different. Thus, the identity management systems need to easily integrated with those applications to govern access rights.

As an example, within a German, global acting DAX-30 company, we supported a client to onboard approximatively 80 SAP Systems around classic SAP R/3, SAP SuccessFactors, SAP Ariba and others to their Identity Governance platform. This integration allowed quick benchmarks about the effectiveness of the access control compliance, and could be leveraged to reduce license cost and increase the level of cyber security for cloud based SAP applications.

For a large Dutch manufacturer, we helped the client calculate a business case to revamp their IAM strategy leading to significant cost savings over a period of five years, while also significantly reducing their risk exposure related to fraud, data breaches, and business disruption.

Figure 4: Reference integrated IAM security architecture



Why PwC?

PwC is uniquely set up to support your migration to SAP S/4HANA – including both the business and technology transformation pieces, and also making your IAM controls and processes fit for the S/4HANA world.

As a top-tier global service partner of SAP, we combine a large footprint of successful transformation projects with a strong and long-standing relationship with SAP itself. Our recent accolades include being named an SAP Pinnacle Award Winner in 2019 and 2018, and SAP EMEA North Award Service Partner of the Year 2019.

Please, visit our SAP/PwC alliance page: https://www.pwc.com/gx/en/services/alliances/sap.html and our Identity and Access Management page: https://www.pwc.nl/en/services/consulting/identity-and-access-management.html

Our Digital Identity practice is set apart from our competitors by three main advantages:

Large and deep pool of experience

Bringing together and integrating global experience in SAP and IAM business integration and system integration effectively.

Local presence, uniform global approach

Our teams in each market combine local and industry knowledge with a proven and consistent global methodology and approach.

Our strength in accounting services

Unlike 'pure' technology providers, our grounding in accounting means we understand the risks and best practices around financial reporting and controls, which is valuable in these transformations.

To find out more about how we can support your Cyber Security & Digital Identity journey please contact:

PwC Netherlands

Gerald Horst
Partner
Digital Identity EMEA

M: +31 (0)655175151
E: gerald.horst@pwc.com

Ivo van Bennekom
Director
EMEA Impact Center Leader, Digital Identity

M: +31 (0)639115402
E: ivo.van.bennekom@pwc.com

PwC Germany

Moritz Anders
Director
Digital Identity

M: +49 1515 5455621
E: moritz.anders@pwc.com

Xuan Chen
Senior Manager
Digital Identity

M: +49 1511 6472330
E: xuan.chen@pwc.com

2020-06-30_RITM3247231