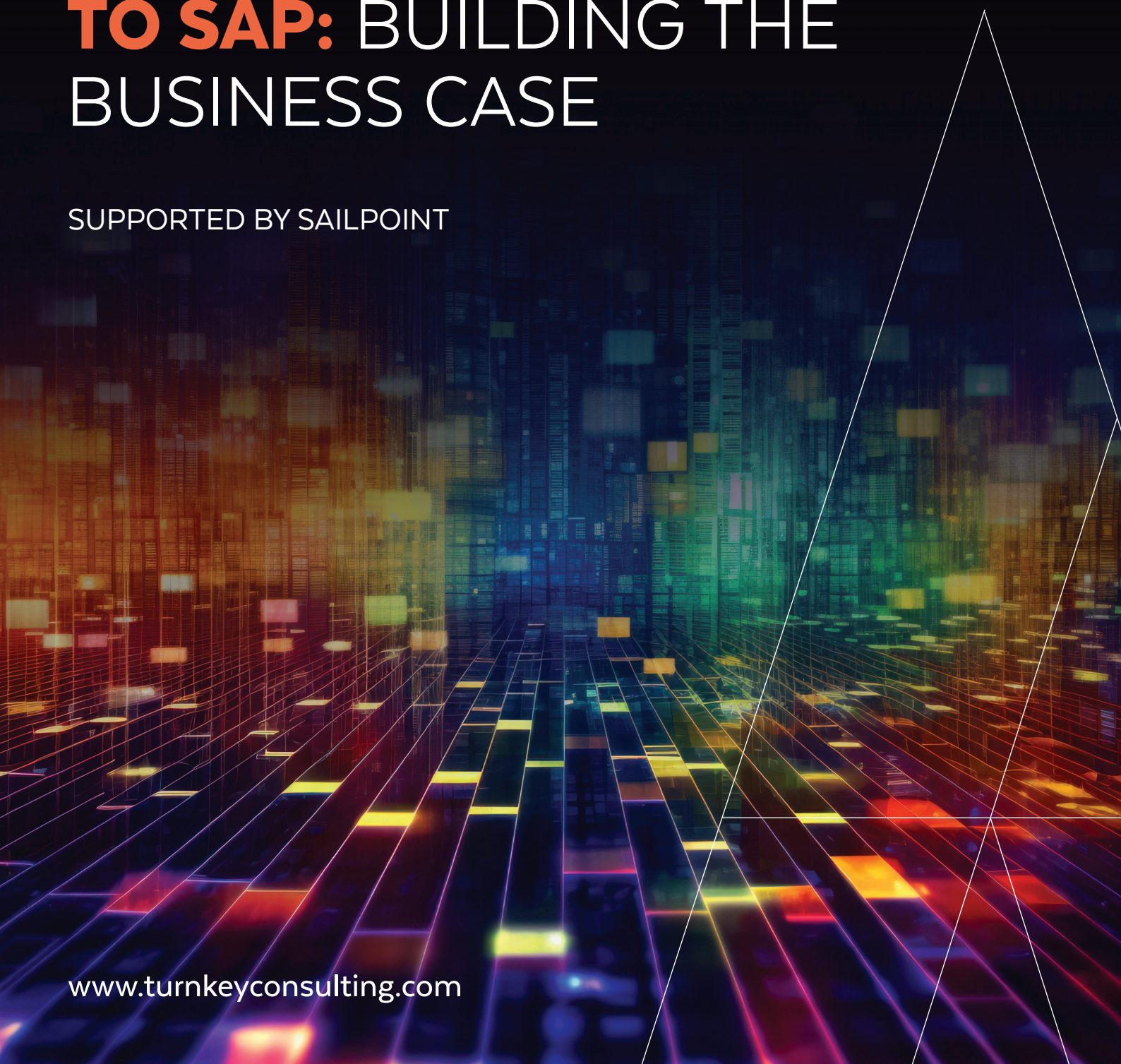
TURNKEY

SailPoint

KEY INSIGHTS GUIDE

EXTENDING IDENTITY GOVERNANCE SOLUTIONS TO SAP: BUILDING THE BUSINESS CASE

SUPPORTED BY SAILPOINT



www.turnkeyconsulting.com

CONTENTS

3 **INTRODUCTION -** WHY NOW IS THE TIME TO INVEST IN IDENTITY GOVERNANCE FOR SAP

4 **SECTION ONE -** THE BENEFITS OF IDENTITY GOVERNANCE AND ADMINISTRATION

7 **SECTION TWO -** THE POWER OF CLOUD-BASED ACCESS GOVERNANCE SOLUTIONS FOR SAP

8 **SECTION THREE -** WHY BUSINESS STAKEHOLDERS SHOULD BE INVOLVED IN ACCESS RISK DISCUSSIONS

9 **SUMMARY -** EXTENDING IDENTITY GOVERNANCE SOLUTIONS TO SAP

INTRODUCTION

WHY NOW IS THE TIME TO INVEST IN IDENTITY GOVERNANCE FOR SAP

It's never been more important to secure SAP. That's for a variety of reasons, including changes in legislation around the world, a shift to cloud solutions, and a business landscape that is increasingly fluid. In addition, more people working remotely and more outsourcing to third parties make it essential to know who is accessing systems and data when and from where.

Legislation is influencing this shift particularly heavily. In May 2023, the National Office of Cyber Security was established in Australia to ensure the cyber resilience of business and critical infrastructure entities. Similar regulations are either in place or are in the works around the world, including the new SEC cybersecurity ruling in the US, NIS2 in Europe, and the National Cybersecurity Policy Framework in South Africa.

These regulations are good news for security practitioners and engineers: they're helping them escalate the importance of investing in security improvements to senior management. But where should this investment go?

With so much variability in the where and what of business, it's logical that the target for security should focus on the biggest constant: the who. And that means identity.

Much of this might sound obvious, but many organisations still struggle with security due to size, complexity, legacy controls, and a host of other reasons. The tide of new legislation makes addressing these challenges even more critical as it increasingly highlights 'supply chain risk.' This means businesses are responsible for all activity on IT systems they own or use, including SaaS and cloud applications.

This guide explores the practical solutions to help your organisation effectively manage your access risk. Beyond helping you avoid compliance issues in the long-term, our guidance will assist you in unlocking scalability and growth, whatever the future business and compliance landscapes might look like.

THE THREE THINGS YOU ALWAYS HAVE TO KNOW

WHO

is accessing your systems, including remote workers and outsourced activity?

WHAT

can users do within your environment, and what systems and data can they access?

WHERE

is system and data access taking place, across every user and every application, including SaaS and cloud applications owned by third-party providers?

SECTION ONE

THE BENEFITS OF IDENTITY GOVERNANCE AND ADMINISTRATION

Identity Governance and Administration (IGA) is a way of securely and efficiently managing digital identities and access enterprise-wide. By improving visibility into both identity and access privileges, it becomes easier to implement the right controls to enable appropriate access and restrict risky or malicious access. IGA is especially useful in the cloud and for businesses moving away from traditional on-premise solutions and applications. That's because IGA gives you both intelligence and complete visibility over all digital identities and all access through a single-pane-of-glass, which includes what digital identities have which access to which systems.

THE BENEFITS OF CLOUD-BASED IGA

INSIGHTS AND INTELLIGENCE	
	**Address the outliers**: IGA eases the process of understanding different access requirements by role, department, location and so on. Grouping digital identities together on this basis means 'outliers' – people who have access that nobody else in their group has – can quickly be spotted and have their access reviewed. This also provides the basis for anomalous behaviours to be identified.
	**Access recommendations**: Understanding typical group access requirements means a recommended 'template' access profile can be provisioned for everyone in the group instead of access having to be provisioned manually and individually.
	**Gather activity data and insights**: Going beyond knowledge of digital identity access, IGA allows for greater understanding of whether their access is being utilised and if it's really needed. This allows for unnecessary access to be removed. In our experience, this 'cleaning up' process has reduced risk by up to 80% for some SAP customers.
	**Enable proactive risk response**: Out-of-the-box rule sets for SAP in solutions such as SailPoint ISC help prevent people getting certain risky combinations of access at the same time as risk analysis can be conducted before access is provisioned.

FRICTIONLESS AUTOMATION

Unlock productivity: The smooth nature of IGA enables more dynamic workforces that get the right access to the right things, wherever and whenever they're working. This boosts efficiency and productivity as end-users move through systems so seamlessly they often don't even notice the IGA system governing their access.

Adapt to change: An agile IGA solution makes it easier to adjust to constantly changing business landscapes, whether it's new applications, new ways of working, or evolving user demands. As a 'set and forget' approach to access is no longer suitable, IGA makes adjusting access to reflect these changes a smooth, simple process.

Make use of AI and ML: The creation and maintenance of provisioning policies can be automated with ease, but artificial intelligence and machine learning are vital for understanding what access to provision and when. Knowing patterns of necessary access can drastically speed up provisioning, removing delays and friction in workflows and processes as well as the manual labour from both provisioning and added help desk support.

Accelerate the identity process: Low-code and no-code workflows mean provisioning can be created by business analysts, irrespective of their level of development experience or programming know-how, allowing any business to get the most out of an IGA solution.

COMPREHENSIVE INTEGRATION

Connect your whole digital ecosystem: Connecting all the applications in an environment to centralised access, controls, and policies makes the approach to identity as easy as possible for every end-user. With solutions like SailPoint ISC, users can request and be granted access within the applications they use every day thanks to full integration with business processes and robust APIs.

Assure adoption: Having a fully integrated solution that is easier to use means users are more likely to adopt and comply with it. If they don't feel slowed down or hindered in accessing the things they need to do their job, they will be less likely to try and find workarounds that can introduce security vulnerabilities.

IGA'S RETURN ON INVESTMENT AT-A-GLANCE

SailPoint ISC is an example of a leading IGA solution that covers all the benefits outlined above. It delivers ROI through several areas:

ACCESS CERTIFICATIONS

1 → 1

year | month

AUTOMATING NEW USER ACCESS

14 → 2.5

hours | minutes

DEPROVISIONING WORKER ACCOUNTS

30+ → 0

days | days

SELF-SERVICE ACCESS REQUESTS

62K | 0 | ~$1M

request filled automatically | help desk calls | annual cost savings

PASSWORD MANAGEMENT

5.5K | 0 | $150k

password resets performed | help desk calls | cost savings

These results ably demonstrate just one area in which security can be much more than a cost centre to a business. Instead, it can unlock efficiency savings and productivity workforce-wide. Alongside risk reduction, this demonstrable ROI means a viable, compelling business case for expanding funding for identity programmes can be constructed.

SECTION TWO

THE POWER OF CLOUD-BASED ACCESS GOVERNANCE SOLUTIONS FOR SAP

SAP is embedded into secure operations in mature organisations, with IGA and other elements established in the IT security landscape. However, there is often a disconnect between IGA specialists and SAP specialists in terms of how the two come together. IGA specialists frequently lack understanding of how complex entitlements work, and SAP experts don't always understand what's required to integrate with enterprise initiatives.

This is where access governance solutions specifically designed for SAP become instrumental, when integrated with your broader, enterprise-level IGA tools and processes. Because of the complexity of the entitlements in SAP, the additional insights provided by this dedicated tooling extends your IGA into this critical estate, providing better security and increased compliance. Over other access governance products, cloud-based solutions like SailPoint ARM can provide additional benefits, including:

INCREASE EFFICIENCY:

Access reviews can be automated and risk mitigation controls documented. Alongside proactive risk assessments that help maintain compliance, these reviews cut the risk of breaches and improve auditing.

ACCELERATE TIME TO VALUE:

Cloud solutions can be deployed and start delivering business value within days, as they have a minimal footprint on a business's SAP estate. A simple connector is deployed, and all analytics are taken care of by the cloud application.

IMPROVE REPORTING ACCESSIBILITY:

A good cloud solution will feature interactive dashboards, expanding the insights of risk exposure information beyond experienced SAP experts to a wider range of business users. This enables quicker production and adoption of risk reports on who has what access and whether that access is being used.

SECTION THREE

WHY BUSINESS STAKEHOLDERS SHOULD BE INVOLVED IN ACCESS RISK DISCUSSIONS

Identity touches nearly every element of an organisation. Yet, at the same time, recent economic turbulence means the challenge of securing new funding for controls, including those tied to identity governance, has gotten tougher. This means that proving both efficiencies and return on investment is critical to building a business case.

One key perception to break down is that SAP – and other ERPs, for that matter – only comprise a small part of a business's IT landscape. For some organisations, SAP applications may only represent a small subsection of overall server capacity, endpoints, and user base, but a major chunk of an organisation's revenue will flow through that ecosystem – including up to 90% of revenue-generating activity. Think of procurement, supply chain, payroll, finance operations, sales functions. All of these impact many different areas of a business, and all need strong SAP identity governance and controls.

Notably, CIOs and CISOs might not see it that way. Whilst they perceive SAP as only 10% of endpoints and servers, that doesn't mean it's only 10% of the risk profile of the business as a whole. Additionally, CISOs, IT service desk managers, and SAP application managers all have a shared responsibility to secure SAP and other critical applications but can often operate in silos, resulting in a lack of shared funding to achieve strategic objectives.

This means that SAP controls and identity governance – funded and managed properly – is a higher priority for everyone than it has been previously. All stakeholders must be brought into access risk conversations, as the wider business needs IT systems to do their job, and IT needs to gain an understanding of processes and how data, systems, and applications are used in practice. IT are the facilitators of access provisioning on request from the business, so helping the business understand the risks of different levels of access is vital for promoting shared risk ownership.

THE IMPORTANCE OF SHARED OWNERSHIP

of total revenue flows through the SAP ERP, making security and compliance critical

of global transactions each day touch an SAP system, meaning security must be considered by teams worldwide

of the IT estate is related to SAP technology, and so the level of risk may be misjudged by CIOs and CISOs

The responsibility should be shared 50/50 between IT and the wider business to promote effective controls and unlock additional funding.

SUMMARY

EXTENDING IDENTITY GOVERNANCE SOLUTIONS TO SAP

Security and compliance go hand-in-hand, especially with the growth of regulation around the world. This means that now more than ever there should be opportunities to get funding for changes and solutions. To do so requires a well-constructed business case for your SAP identity governance project.

The complexity and abstract nature of SAP means putting any new solution in the context of risk, compliance and ROI should make a new project easier for decision-makers to support and understand.

Solutions such as IGA enable this as they reduce risk, support better compliance, improve productivity, reduce costs, and drive efficiencies business-wide - even as the business landscape changes in the future.

Turnkey is here to help ensure your IGA programmes include your business-critical systems and data, allowing you to both communicate and deliver identity security ROI to your business. Together, we can reframe IGA for SAP as a business enabler, and a driver of agile, resilient enterprises. Contact us today to get started.

info@turnkeyconsulting.com

TURNKEY

ABOUT TURNKEY

Turnkey Consulting is helping to secure enterprises and drive performance through its specialised expertise across Integrated Risk Management, Identity and Access Management, and Cyber and Application Security. We elevate risk and security professionals by creating digital enterprise resilience through business strategy and consulting, technology implementation and managed services.

CONTACT

If you have any questions about extending identity governance solutions to your business-critical systems, or any of Turnkey's services, we'd love to hear from you.

Contact us

info@turnkeyconsulting.com

www.turnkeyconsulting.com
www.sailpoint.com