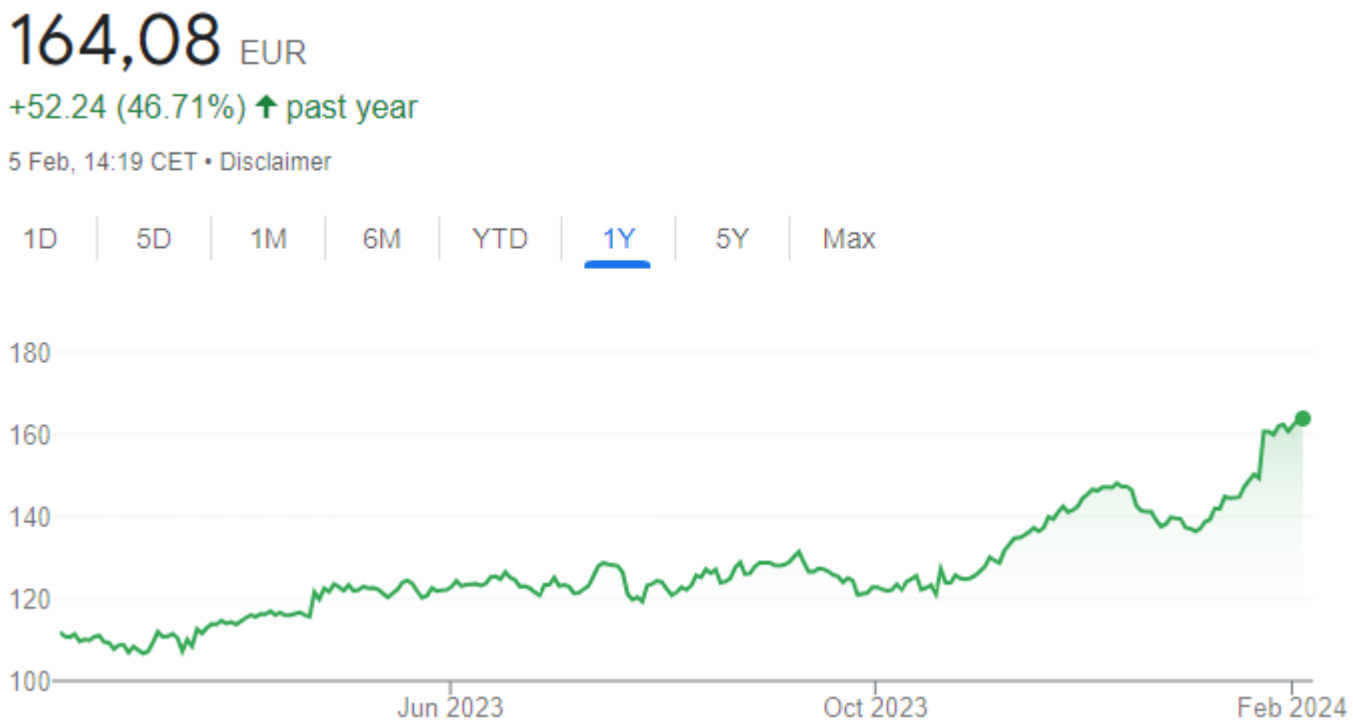
In a groundbreaking strategic realignment, SAP is consistently focusing on the Software-as-a-Service (SaaS) model and corresponding cloud solutions in order to gradually phase out traditional on-premise systems. This underscores SAP's commitment to agility and scalability in the cloud, offering customers a contemporary IT infrastructure. In the course of this transformation, SAP Identity Management (IDM) is expected to go out of maintenance by 2027 or 2030, giving sufficient lead time for migration to alternative solutions. Recently, as part of the IDM working group of the DSAG, SAP confirmed that no additional information will be provided to IDM customers. The end of maintenance in 2027/2030 is thus to be considered authoritative and binding.

The transformation from SAP to cloud solutions raises questions regarding the peripheral operations (for SAP) concerning identity management. Based on the information available to us, it can be assumed that SAP will not provide an adequate replacement solution that offers the familiar functional scope and flexibility of SAP IDM. Since SAP has meanwhile become one of the top 50 rated companies worldwide, a move away from the cloud-centric strategy is becoming increasingly unlikely.



Given their success, a shift away from the cloud strategy seems improbable.

Even though SAP Identity Management is far from perfect software, it has allowed many companies—through years of work and expertise—to build highly customized solutions. This

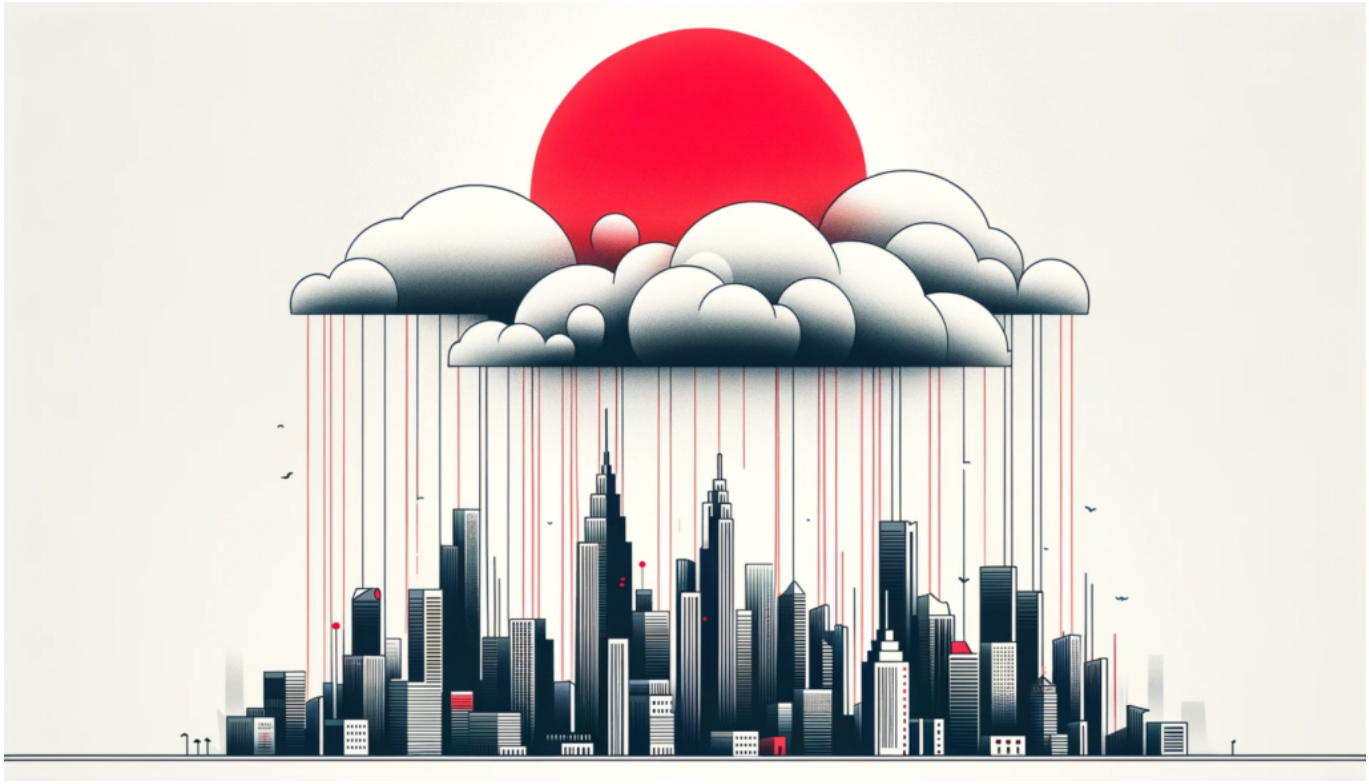
was especially true for companies with a strong focus on integrating dozens to hundreds of SAP applications. In particular, regarding SAP integration and flexibility, most competitor products will likely fall short compared to the in-house solution.

In this article series, we want to provide an overview of possible options for companies and give a brief assessment of strengths and weaknesses of each solution. Please note that these assessments should not be regarded as final and do not replace individual consulting.

- Part 1: The End of an Era: The Future After SAP IDM
- Part 2: SAP: Cloud Identity Services, GRC edition for SAP HANA
- Part 3: Cloud Services: Microsoft Entra ID, Okta, Omada Identity
- Part 4: On-Premise Solutions: e.g. One Identity

The IT "Gretchen Question": Should We Move to the Cloud?

That the direction in recent years has shown a clear trend toward cloud infrastructure is no news. More and more companies are willing to relocate even sensitive data and process IT to the cloud. From our point of view, this trend is inexorable, and using a cloud-based IDM solution is the next logical step. However, the parameters *security*, *data protection*, and *flexibility* must be carefully defined.



Cloud Computing – A fundamental decision regarding the entire infrastructure

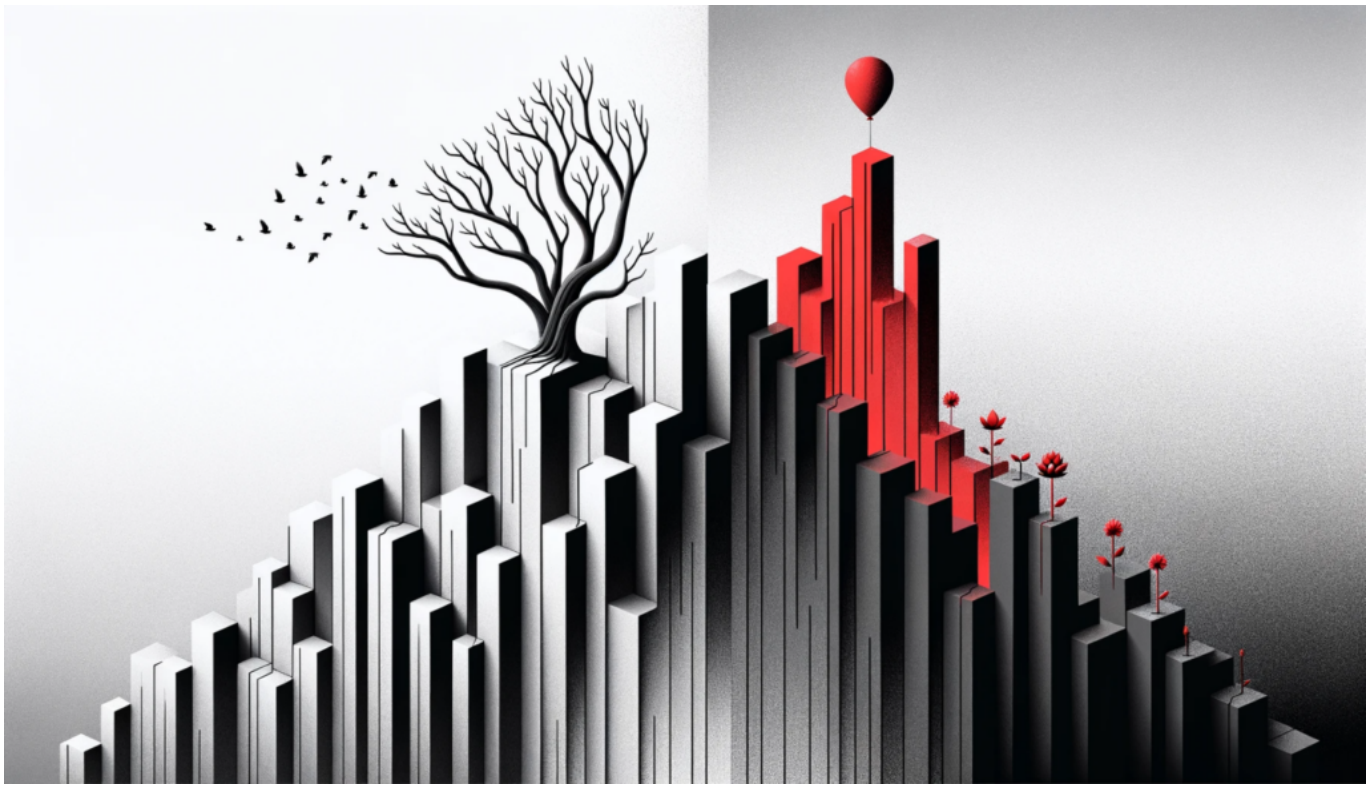
Regardless of this opinion, the decision to use cloud-based services is a strategic one at the highest IT level, and identity management is ultimately only one necessary building block within the chosen IT infrastructure.

For the selection of a suitable IDM solution, answering the cloud question is decisive. Once you decide on one side, the number of candidate solutions effectively halves on its own.

One’s Challenge Is Another’s Opportunity? – The Economics of Change

The low availability of specialists for SAP Identity Management has often been an obstacle in recent years to even introducing the software. The architecture of the software deviates significantly from classic SAP systems, so the introduction was almost exclusively possible by acquiring external consulting firms.

Their availability is likely to further decline in the coming months and years, as many consultants already need to build their knowledge for future-oriented solutions. We forecast a rapid extinction of available SAP IDM consultants.

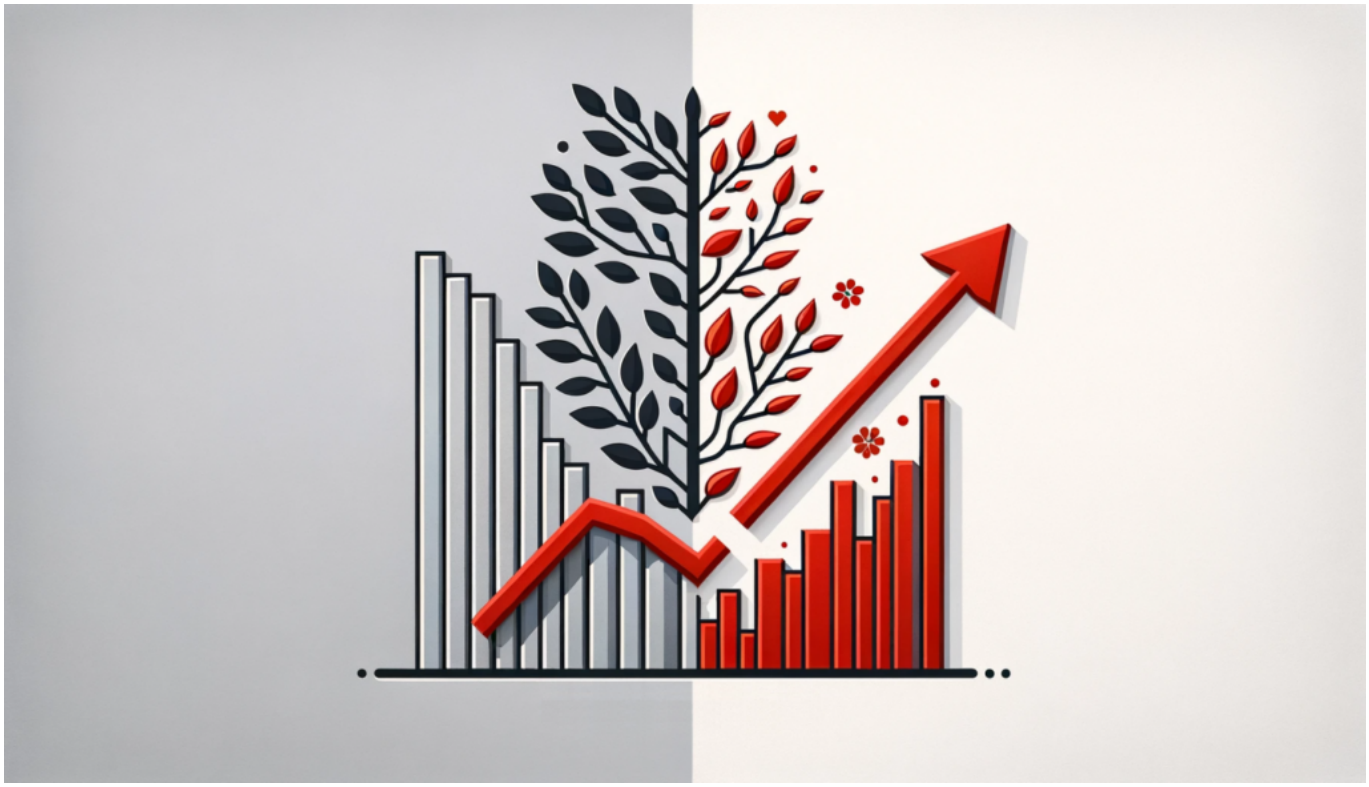


New prospects for consultants

From the perspective of IT service providers, however, there is no reason for concern: In the next few years, an unprecedented demand for IAM specialists is likely to emerge. While companies will be forced to invest again in expensive IT infrastructure and know-how, appropriately positioned firms and specialists may be able to enjoy a real flood of contracts.

Spring Cleaning for IAM Processes? – Opportunities and Risks

In many companies, the IAM (Identity and Access Management) processes have grown historically and are correspondingly complex. But precisely this complexity offers an opportunity: through a well-considered redesign, these processes can be significantly simplified, which not only improves efficiency but also enhances security.



The forced transition opens up opportunities for improvement.

It is a widespread misunderstanding that, outside certain regulated industries (such as banking and insurance), there are strict mandates on the design of IAM processes. In reality, the absence of such rigid requirements gives companies a remarkable degree of freedom.

This fact allows organizations to subject their existing, often oversized role models and approval workflows to critical review. The present moment appears as an extremely

opportune opportunity to evaluate these elements of IAM critically in order to assess their suitability and efficiency in the context of the modern business world and adjust them accordingly.

Implementing a new IAM solution is not a project to be rushed. For a successful introduction, companies should plan at least **12**, preferably **24 months or more**. The required timeframe strongly depends on the complexity of the IAM software requirements as well as the structure of the organization and its processes.

Thorough planning and implementation are essential to ensure that the new solution effectively meets the needs of the company and creates long-term added value.

The Future of consiness – Our Offering

Consiness is characterized by vendor-independent consulting, which allows customers to receive tailor-made solutions precisely aligned with their specific needs. Despite a continuing focus on SAP-centered implementations, Consiness has expanded its expertise and now can draw on valuable experience with deploying third-party solutions, whether implemented in cloud or on-premise environments.

Continuing to lead in the field of IAG & IAM – consiness

The process of replacing and introducing a new IDM (Identity Management) solution at Consiness always begins with a careful analysis phase. In this essential phase, possible options are not only selected and analyzed, but also planned in detail. This methodical approach ensures that the implementation is built on a solid foundation.

A key aspect to consider when introducing new IAM solutions is the inherent risk of failure that generally accompanies IT projects. This risk underscores the importance of sound planning and strategic orientation.

In the past, Consiness has offered, in addition to its consulting services in the area of Identity and Access Governance, the standard solution *Consiness IDM-Suite*. This solution

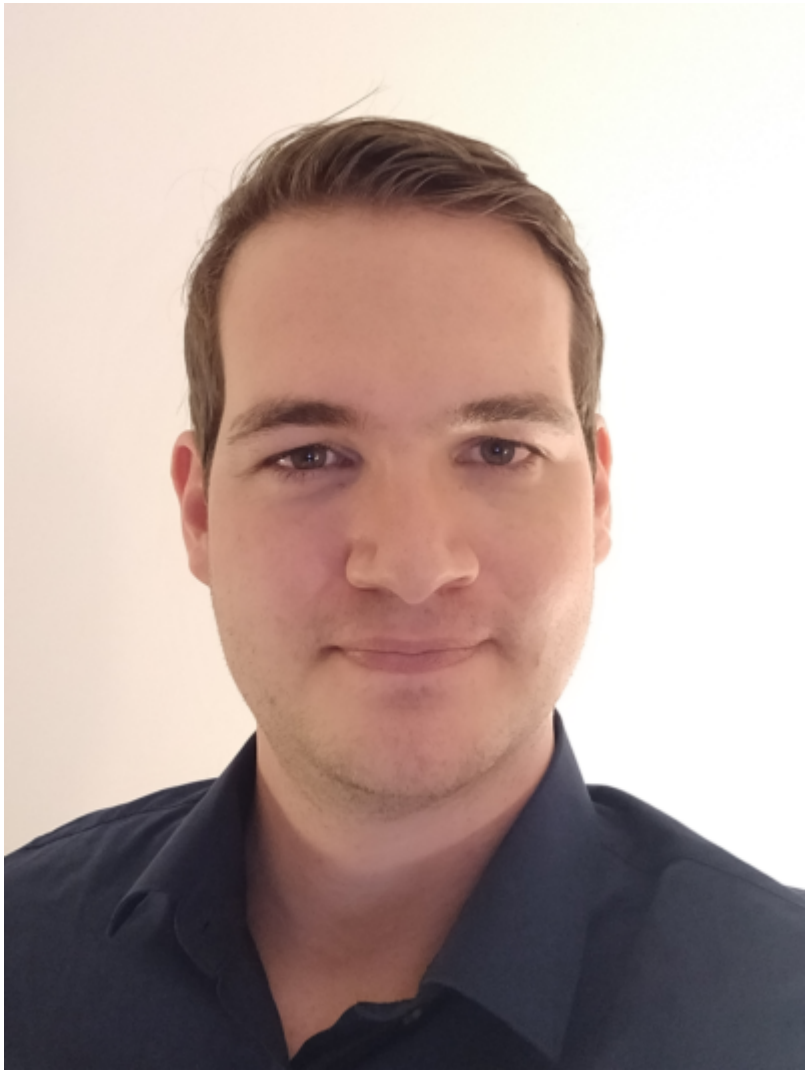
was designed to achieve quick wins in the deployment of complex software. However, under the current circumstances, this specific solution can no longer be continued. In the future, Consiness plans to continue offering a standardized concept based on three central pillars:

- a well-thought-out identity and access governance strategy
- a lean, standardized process model that ensures efficiency and clarity
- a technical solution that is not only easy to implement but also highly adaptable

These components together form the foundation for a successful, future-proof IAM solution that meets each customer’s particular requirements and constraints.

Next: Part 2: SAP: Cloud Identity Services, GRC edition for SAP HANA

about the author



Hendrik Winkler is a partner at **consiness** and the lead architect for Identity and Access Management solutions. He draws on extensive expertise in **SAP ABAP**, **GRC**, **cloud technologies**, and **SAP Identity Management**. With more than ten years of experience in the IT industry, he has specialized in the development and implementation of complex **IAM systems**, always keeping a close eye on **security**, **usability**, and **compliance**.