

In this article series we want to provide an overview of possible options for companies and give a brief assessment of the strengths and weaknesses of each solution. Please note that these assessments should in no way be considered 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, Okta, Omada Identity
- Part 4: On-Premise Solutions – e.g. One Identity, SIVIS

This part takes a deeper look at the various SAP solutions that are central for companies of all sizes and industries. As an introduction, we discuss continuing operation of SAP Identity Management (IDM), which will likely remain a transitional solution for many SAP customers. Key components of the future include SAP Cloud Identity Services in combination with SAP Identity and Access Governance (IAG). Moreover, we shed light on the importance of SAP CAP (Cloud Application Programming) applications, which may help close functional gaps in the cloud infrastructure. Finally, SAP GRC (Governance, Risk, and Compliance) is discussed, which plays a decisive role in ensuring corporate compliance and risk management, yet is often also used in the implementation of identity management.

Option A: Continuing Operation of SAP IDM 8.0

Option B: Running SAP IDM 8.0 in the Cloud?

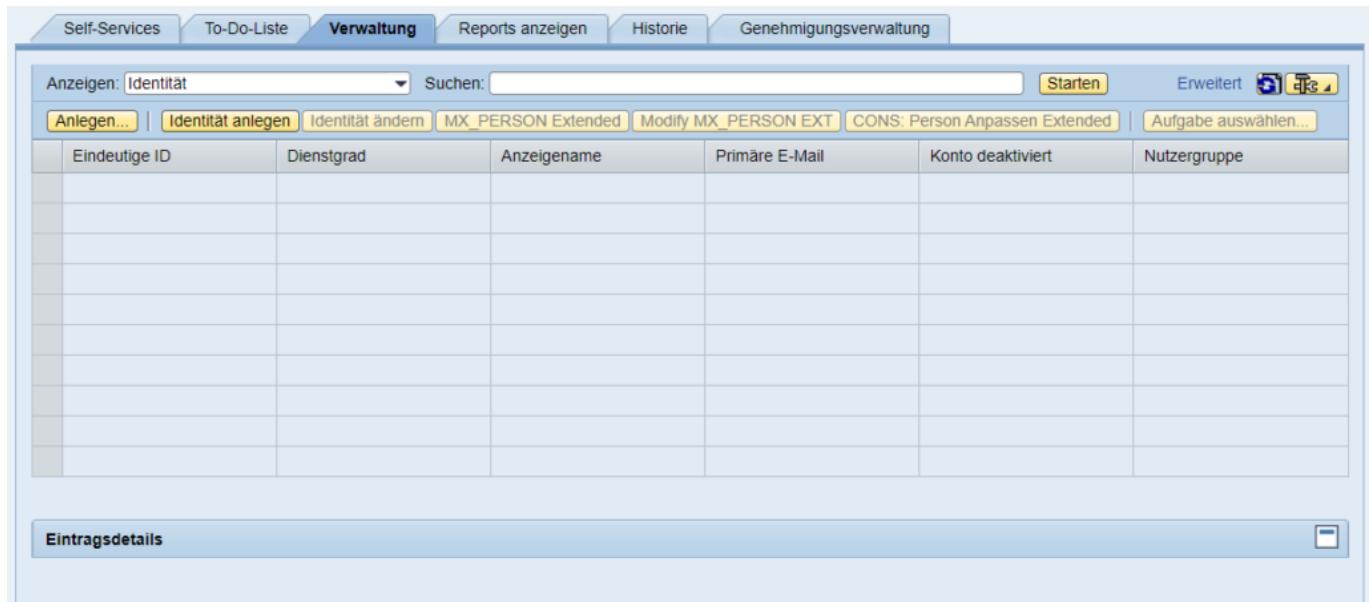
Option C: SAP Cloud Identity Services – IAS/IPS + IAG

Option D: SAP Cloud Identity Services and CAP Extensions

Option E: SAP GRC 12.0 / edition for SAP HANA

Option A: Continuing Operation of SAP IDM 8.0

The last service pack for SAP IDM 8.0 was released more than three years ago. A pointed question arises: what support does SAP really intend to provide? Over time, many customers have built practical solutions or workarounds and may operate without further patches.



We won't be missing it ☐ – The SAP IDM Standard UI

However, the decision is not that simple. The problem lies especially in the IT security of the underlying AS Java components, for which constant security updates are offered. Those who do not keep these components “up to date” risk the long-term integrity of their system landscape.

Thus, continuing with IDM 8.0 is more of a “wait-and-see” strategy before the inevitable transition takes place. It's also not impossible that an extended support option for some (large) customers, or even general extension, may be offered. Whether only support is discontinued or whether an effective prohibition of use for the AS Java environment will be imposed is unclear.

Advantages

- No additional initial effort
- Wait for market consolidation or new developments from SAP to make a better decision later

Disadvantages

- Ongoing investment in a dying software
- Declining availability of specialists
- From about 2030 onwards, security restrictions likely
- Possibly usage restrictions or prohibition after 2030

Assessment

From our point of view, waiting and continuing operation of SAP IDM 8.0 is a valid strategy—especially for very small or agile implementations that can be replaced in time. Complex landscapes, however, must be migrated over several years. For companies planning a cloud transformation, it may make more sense to invest directly in a new solution. However, we cannot recommend long-term planning based on SAP IDM 8.0.

Option B: Running SAP IDM 8.0 in the Cloud?

A post in DSAG forums by the company ROIABLE announced a BTP port for SAP IDM 8.0. The idea is: since fundamentally only the support for AS Java is to be discontinued, one could migrate the IDM components to SAP BTP and offer them there as a service.

While this sounds promising—especially since ROIABLE is known in the SAP IDM scene—a practical implementation is likely to receive little acceptance from SAP, making it a risky move.

Advantages

- Minimal porting effort
- Eliminate the problematic AS Java component
- Potential performance benefits
- Closer integration in cloud networks

Disadvantages

- Not supported by SAP
- No planning reliability

Assessment

The idea is attractive enough to mention, but due to external constraints should not be seriously declared as a strategy.

Option C: SAP Cloud Identity Services - IAS/IPS + IAG

Welcome to the jungle of SAP cloud services. The two BTP services for Identity Authentication (IAS) and Identity Provisioning (IPS) are grouped under the name **SAP Cloud Identity Services**.

Modern, clean, and essential for the BTP – SAP Cloud Identity Services (IAS/IPS)

IAS and IPS are available as part of the **SAP Cloud Identity Services** and play an important role within the **SAP Business Technology Platform (SAP BTP)** ecosystem—particularly when it comes to the **integration and management of identities and access rights**.

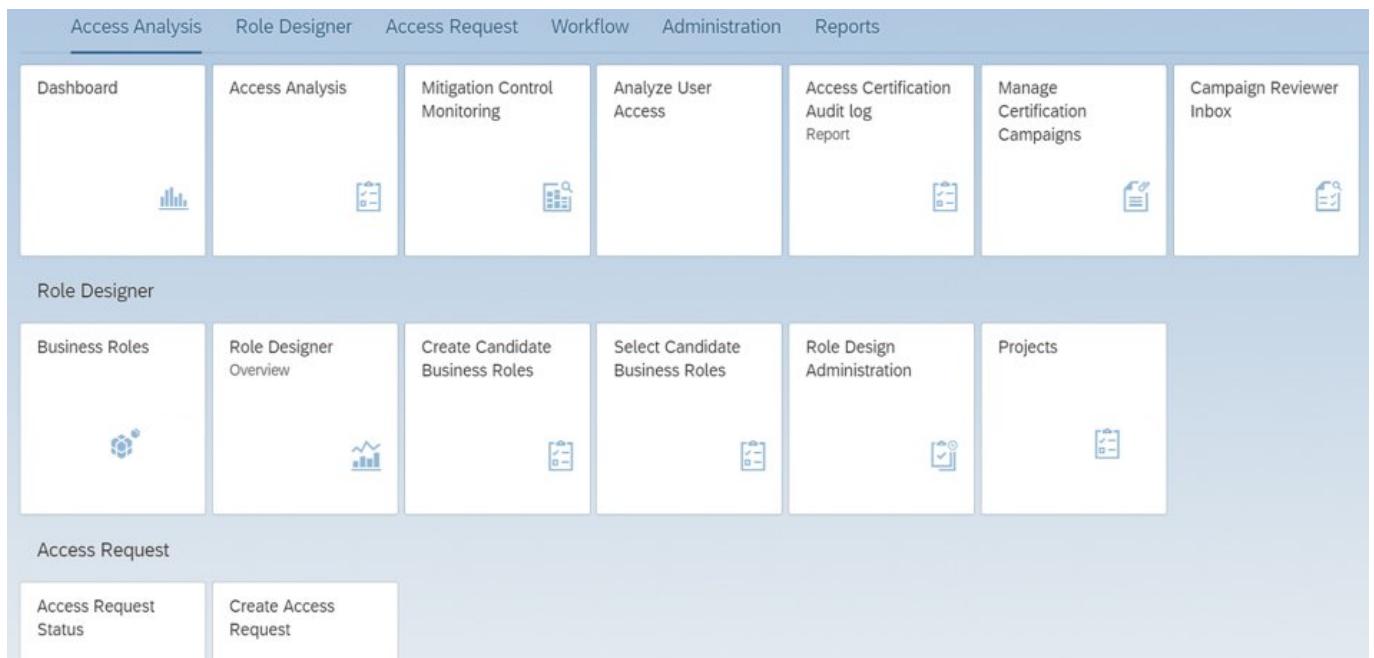
For **SAP BTP customers**, IAS and IPS are **fundamental services**, especially relevant when using other SAP cloud solutions such as **SAP SuccessFactors** or **SAP S/4HANA Cloud**. SAP BTP is designed to deliver its cloud solutions with **integrated identity authentication**, meaning that **IAS/IPS are required** to ensure seamless and secure access to these applications.

In terms of **cost**, IAS and IPS are **included by default** within the SAP BTP framework and **do not require additional licensing** when used in connection with an SAP cloud solution, an SAP on-premise application, or an SAP system hosted on **SAP HANA Enterprise Cloud**. Customers typically receive **one productive and one test tenant** without additional license fees. However, if additional tenants

are required, these must be purchased separately.

For customers under the **Cloud Platform Enterprise Agreement (CPEA)** contract, the pricing model is **consumption-based**, meaning that you only pay for the services actually used. There is also the option to **purchase additional cloud credits** to increase your initial commitment and thus avoid overconsumption. Customers can manage their service usage via the **SAP BTP cockpit** and receive **monthly invoices** to maintain transparency regarding incurred costs.

SAP Cloud IAG (Identity Access Governance) is the “**cloud successor to GRC**” and, in our assessment, **still in its early development stages**. Why the quotation marks? As expected, SAP would, according to its overall strategy, like to **completely replace GRC with Cloud IAG**. However, this contradicts SAP’s announcement of **SAP GRC edition for HANA**, scheduled for **2026** (more on that in the section about SAP GRC).



The screenshot shows the SAP Cloud IAG cockpit interface. The top navigation bar includes tabs for Access Analysis, Role Designer, Access Request, Workflow, Administration, and Reports. Below this, the interface is organized into three main sections: Access Analysis, Role Designer, and Access Request. The Access Analysis section contains seven tiles: Dashboard (bar chart icon), Access Analysis (calendar icon), Mitigation Control Monitoring (magnifying glass icon), Analyze User Access (magnifying glass icon), Access Certification Audit log Report (document icon), Manage Certification Campaigns (document icon), and Campaign Reviewer Inbox (document icon). The Role Designer section contains six tiles: Business Roles (gears icon), Role Designer Overview (bar chart icon), Create Candidate Business Roles (magnifying glass icon), Select Candidate Business Roles (document icon), Role Design Administration (document icon), and Projects (document icon). The Access Request section contains two tiles: Access Request Status (document icon) and Create Access Request (document icon).

SAP’s own in-house rival!? – SAP Cloud IAG

SAP IAG offers functions that will strongly remind you of **GRG**: access analysis, business role management, access reviews, and workflows that enable companies to effectively enforce their access policies while maintaining compliance requirements.

Advantages

- Rapid deployment and potentially lower total cost of ownership (to be calculated on a case-by-case basis)
- IAS/IPS are a given for hybrid SAP landscapes
- Central identity provider for both cloud and on-premise applications
- Supports standardized authentication methods, including existing identity providers (e.g. login via Apple ID)
- IAS enables single sign-on functionality
- Dynamic adjustment of account and user authorizations

Disadvantages

- May be less suitable for highly specific, non-standard IAM processes
- Limited customization and development capabilities
- May require process standardization
- More restricted monitoring capabilities compared to SAP IDM
- Troubleshooting cloud interactions can be more complex
- BTP and Cloud Identity Services evolve at a relatively rapid pace – which isn't always beneficial if a minimal and stable solution is desired

Assessment

SAP Cloud Identity Services are a **given** when operating within SAP BTP. However, in our assessment, these solutions **cannot be regarded or used as complete IAM products**.

SAP itself seems to share this view—positioning Cloud Identity Services largely as **middleware solutions** alongside **Microsoft Entra**.

The use of Cloud Identity Services as a **replacement for SAP IDM** can therefore only be recommended in specific cases:

- **Companies with a cloud focus or hybrid landscapes:** Since IAS and IPS

are specifically designed for cloud environments, they are well suited for organizations that already have—or plan to build—a strong cloud presence.

- **Companies with simple, standardized IAM processes:** It should be evaluated case by case whether IAM processes can be simplified enough for IAS/IPS and IAG to suffice.
- **Companies requiring fast and scalable solutions:** As both services are cloud-based, they offer rapid deployment and scalability, which can be particularly advantageous for growing businesses.

For the following types of organizations, IAS/IPS may be **less suitable**:

- **Companies that do not (yet) want or are unable to use the cloud**
- **Companies with highly specific, non-standard IAM requirements:** If an organization has very specialized authentication and identity management needs that go beyond the standard features of IAS and IPS, a custom-built solution may be necessary.

Ultimately, the decision **for or against IAS/IPS** depends on the **specific requirements and goals** of each organization.

Option D: SAP Cloud Identity Services and CAP Extensions

The weaknesses of **SAP IAS and IPS**—such as their limited flexibility for individual customization and restricted monitoring capabilities—can be mitigated by developing **custom CAP (Cloud Application Programming Model)** applications. CAP provides a comprehensive programming environment that allows the creation of **tailored extensions and adaptations** specifically aligned with a company's individual needs.

The End of an Era – Part 2/4: SAP Solutions

File Edit Selection View Go Run Terminal Help ← → CAPDemo

EXPLORER OPEN EDITORS CAP Release Notes cat-service.cds consinessDemo\src data-model.cds consinessDemo\src GROUP 2 Response(4ms) CAPDEMO consinessDemo vscode app db node_modules srv cat-service.cds cat-service.js .cdsrc.json .eslintrc .gitignore package-lock.json package.json README.md sqldiff.exe sqlite3_analyzer.exe sqlite3.exe test.http

cat-service.js

```
consinessDemo > srv > cat-service.js > <unknown> > exports
1 module.exports = (srv) => {
2
3   const {Books} = cds.entities('my.bookshop')
4
5   // Reduce stock of ordered books
6   srv.before('CREATE', 'Orders', async (req) => {
7     const order = req.data
8     if (!order.amount || order.amount <= 0) return req.error(400, 'Order at least')
9     const tx = cds.transaction(req)
10    const affectedRows = await tx.run(
11      UPDATE(Books)
12        .set({stock: ('-=': order.amount)})
13        .where({stock: ('>=': order.amount), /*and*/ ID: order.book_ID})
14    )
15    if (affectedRows === 0) req.error(400, 'Sold out, sorry')
16  })
17
18  // Add some discount for overstocked books
19  srv.after('READ', 'Books', each => {
20    if (each.stock > 111) each.title += ' -- 11% discount!'
21  })
22
23}
```

PROBLEMS OUTPUT TERMINAL PORTS COMMENTS DEBUG CONSOLE

```
at: async ApplicationService.handle (C:\DEV\IDM_Apps\CloudApps\CAPDemo\consinessDemo\node_modules\@sap\cds\lib\srvc\srv\dispatch.js:69:5)
at: async C:\DEV\IDM_Apps\CloudApps\CAPDemo\consinessDemo\node_modules\@sap\cds\lib\srvc\srv\dispatch.js:69:5
code: 400,
numericSeverity: 4,
id: '1768797',
level: 'ERROR',
timestamp: 1707738238913
} [odata] - GET /odata/v4/catalog/Books?
```

Response(4ms)

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 X-Correlation-ID: b6e3e3c8d-ab3e-48c4-808
5-9b02f5b9eaa
4 OData-Version: 4.0
5 content-type: application/json;odata.metadata=minimal
6 Date: Mon, 12 Feb 2024 11:44:01 GMT
7 Connection: close
8 Content-Length: 378
9
10 ~ {
11   "@odata.context": "$metadata#Books",
12   "value": [
13     {
14       "ID": 201,
15       "title": "Wuthering Heights",
16       "author_ID": 101,
17       "stock": 2
18     },
19     {
20       "ID": 207,
21       "title": "Jane Eyre"
22     }
23   ]
24 }
```

Jira: hendrik.winkler: No active issue Bitbucket: hendrik.winkler: 4ms 588b In 21. Col 7 Spaces: 4 UTF-8 CRLF JavaScript

Getting started with SAP development has never been easier – thanks to CAP tutorials from the SAP Developer Center.

For example, **custom CAP-based applications** can be developed to integrate **advanced functionalities** into your **BTP** environment that go beyond the standard capabilities of **IAS/IPS** and even **IAG**—such as **complex approval workflows** or **customized user management processes**.

In addition, **CAP** offers a **flexible platform** to optimize the integration of **IAS/IPS** with other systems and services. This can be particularly useful for enabling **seamless connectivity between cloud and on-premise systems** in hybrid IT landscapes. By leveraging CAP, companies can therefore **compensate for the limitations of IAS/IPS** and create a **more comprehensive identity and access management system** tailored to their specific requirements.

Advantages

- Enables third parties to implement services that are tailored to specific customer needs
- Greatly simplified entry point for newcomers to SAP development through CAP

- Allows the use of SAP Cloud Platform Workflow
- Facilitates the development of migration paths from **SAP IDM → SAP Cloud** for a seamless transition and reuse of existing processes

Disadvantages

- Deviates from SAP's standard solution
- Custom developments must mature over time before full adoption

Assessment

The **extendability of the standard** has always been one of the main arguments in favor of using SAP.

Through the **standardization of Cloud Identity Services**, many customers could face hurdles that might otherwise lead them to adopt third-party solutions.

However, with **CAP**, SAP has created a platform that enables **open development of additional modules by third parties**, which can be **natively integrated** into the **SAP BTP ecosystem**.

The first developers are already working on implementing **IAM modules** that extend or even partially replace **IAS/IPS**.

For companies planning an IT architecture with **SAP Cloud** as the central element, this approach is likely the **most elegant**.

However, it remains to be seen **what capabilities and limitations** will emerge from the development of **CAP applications for IAM**.

As soon as there are updates on this option, we will report on them promptly.

Option E: SAP GRC 12.0 / edition for SAP HANA

The **tremendous success** of **GRC AC 12.0** and its predecessors could not be ignored by SAP, and with the official announcement of **SAP GRC edition for SAP HANA**, the strategic direction is clear: **SAP GRC lives on!**

GRC 12.0 is delivered with a comprehensive suite of Fiori-like applications

GRC is a **compliance tool**, but it encompasses far more than the modules commonly known in IAM circles, creating **positive synergies** for the further development of the **GRC platform**.

The modules relevant to IAM are grouped under the product **GRC Access Control**:

- **ARA - Access Risk Analysis**
- **EAM - Emergency Access Management**
- **BRM - Business Role Management**
- **ARM - Access Request Management**
- **UAR - User Access Review**

The biggest arguments against GRC have been (and still are) that, first, the solution was **not originally designed or built as an identity lifecycle management system**, and second, it **lacked integration with non-SAP products**.

To close these gaps, SAP's prescribed architecture was to use **both IDM and GRC** together. These were connected through one of the many (albeit cumbersome in practice) **integration scenarios between IDM and GRC**.

Nevertheless, the **sum of the available components**, combined with the **proven ABAP stack**, led many companies to adopt **GRC Access Control as an “IDM-**

light” solution.

Any functional gaps were often closed through **custom extensions** developed over the years, thanks to GRC's excellent extensibility.

These companies may now find themselves the **fortunate winners**, benefiting from a **modern, future-proof technology stack, enhanced Fiori interfaces, and improved reporting capabilities**.

Advantages

- Proven technology stack based on **ABAP/HANA DB**
- Established and mature solution for the **lifecycle of permissions and business roles (Access Governance)**
- Flexible workflow design using **MSMP (Multi Step Multi Process)**
- Good availability of **GRC experts**, as well as **ABAP** and **Fiori developers**
- **Future-proof**
- Easy integration with **ABAP-based landscapes**

Disadvantages

- Strategically designed primarily as a **compliance tool**, not as a full **IAM solution**
- Integration with **non-SAP systems** may require development of **custom connectors**
- **Customization** is more complex and time-consuming compared to SAP IDM
- **Highly complex solution** (challenging for new customers or those seeking lean implementations)
- **In-house competition** from **SAP Cloud IAG**

Assessment

Even if SAP might not officially acknowledge this view, **GRC is definitely a serious option** for companies currently using the **SAP + IDM tandem**.

It's no coincidence that, over the past few years, a “**GRC fan community**” has

emerged within the SAP ecosystem—far larger than IDM could ever achieve.

Each company should carefully consider **how to transfer missing IDM functionalities into GRC**, particularly in **SAP-centric infrastructures** that value **complex special cases** and **risk analysis** capabilities.

If **SAP software** is already established and **cloud integration** is (for now) not a priority, **choosing GRC is almost an automatic decision**.

However, it's important to keep in mind that **SAP GRC is complex, costly, and resource-intensive**—a factor that must not be underestimated.

Summary

We hope this overview helps you plan your **future IAM architecture**.

Even within the **SAP ecosystem**, there are numerous options for managing identities and access rights, depending on the infrastructure in place.

As mentioned in the **introductory article**, the **fundamental question of cloud orientation** is indispensable for making the right decision.

In this context, we also recommend reading **Part 3 of this article series**, which discusses **Microsoft Entra**, the **officially announced successor solution** by SAP.wird.

[Next Part 3: Cloud Services – Microsoft Entra, Okta, Omada Identity](#)

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**.