



NTT DATA Business Solutions

SAP Service Description Document for G-Cloud for:

SAP Identity Management

8 January 2026 | Document Version V1.00

NTT DATA Business Solutions is a Global Value-Added Reseller of SAP and provides all SAP products in the same form as if they had been purchased

NTT DATA Business Solutions

We Transform. SAP® Solutions into Value

We understand the business of our clients and know what it takes to transform it into the future. At NTT DATA Business Solutions, we drive innovation - from advisory and implementation, to managed services and beyond, we continuously improve SAP solutions and technology to make them work for companies - and for their people.

Aiming to transform, grow and become more successful? We provide you with more than in-depth expertise for SAP solutions: As your passionate partner, we connect your business opportunities with the latest technologies – and offer you a unique approach to get the job done as smoothly as possible. Our close ties to SAP and other partners give you access to innovative solutions and developments. Being part of the global NTT DATA group enables us to master any scope of project.

With operations in more than 30 countries, we have enabled thousands of companies become more efficient and effective during the last three decades. Our more than 14,000 experts around the world will also accompany you on your journey toward a truly intelligent enterprise – wherever you want to start! We have specialised in making SAP solutions work for companies – and for their people: We Transform. SAP® solutions into Value.

We are proud to be consistently recognised within the SAP ecosystem, having won multiple SAP accolades over the years. We are also delighted to announce our recent achievement of four SAP Pinnacle Awards in the categories of GROW with SAP, SAP Business AI Customer Adoption, Business Transformation Management, and Cross-Portfolio Success. These awards celebrate the exceptional performance of the world's foremost SAP partners, underscoring our commitment to excellence and innovation. With four wins and five finalist positions, we stood out as the leading winner in 2025. Additionally, our greatest asset and our most significant differentiator is our people. In 2025, the NTT DATA Group was named a Global Top Employer in 33 countries by the Top Employers Institute. This award highlights our dedication to creating a thriving work environment and confirms our status as a choice destination for IT professionals.

Summary

SAP Identity Management aligns user lifecycle management with key business processes running in the cloud and on-premise. Business managers define role-based, compliant user access rights and identity management across SAP and third party enterprise applications – whilst IT maintains centralised data, alerts, and reporting needed to maintain control and manage risk.

Quick facts

Summary

The SAP Identity Management component helps you align user lifecycle management with your organisation's key business processes running in cloud and on-premise solutions. Now, business managers can define role-based, compliant user access rights and identity management across enterprise applications – both SAP and third party – while giving IT the centralised data, alerts, and reporting needed to maintain control and manage risk.

Objectives

- Reduce operational costs and minimise risk in complex system landscapes
- Manage access to applications
- Extend existing on-premise identity management solutions to the cloud
- Improve compliance with local and global regulations

Solution

- Business-driven, compliant identity management for business processes running in cloud and on-premise solutions
- User access rights assigned and maintained across multiple systems
- Password self-service functionality and synchronisation
- Roles aligned with business processes rather than technical directory structures
- Reports based on current access and past events

Benefits

- Lower costs and increased productivity due to tight integration with your business processes – both in the cloud and on premise
- One central location for identity data storage, eliminating redundancies
- Support for regulatory requirements, which minimises segregation-of-duties (SoD) risks



Learn more

For more information, contact your SAP representative or visit us [online](#).

The challenges of manual identity management

Identity management has become a significant challenge for organisations today. Users need fast, hassle-free access to a multitude of applications both on premise and in the cloud. And IT must ensure that enterprise data and systems are secure and that access to them is compliant with company policies and legal regulations. Meeting these competing demands requires **moving beyond manual, time-consuming, and IT-centred identity management** so you can operate with agility, efficiency, and confidence.

If your organisation is still manually managing the identities of employees, contractors, and customers who need access to heterogeneous systems, you likely face a number of challenges. Let's take a closer look at why – and explore how integrating identity management with business processes within and beyond your enterprise can help you address these challenges.

High operational costs and security risks

Complex system landscapes require that your IT department maintain multiple sources of identity data – for example, by entering data for each user, assigning user permissions for multiple systems, and maintaining user passwords for each system. When IT administrators manually perform these tasks, it can take longer to provision users of multiple systems, slow new employee onboarding, and delay their time to productivity. It also means that users are dependent on IT help desk staff for password resets and changes in access or permissions. This can drive up help desk staffing requirements and costs.

Identity management solutions can help by automating manual tasks for IT staff, pushing certain tasks to line-of-business managers and employees (such as password updates) and tracking and reporting on who has access to what systems and data and when.

Evolving security risks

Manual, paper-based identity management processes also create security risks. For example, it's not uncommon for employees who have changed roles or have left an organisation (either through retirement or termination) to have access to certain systems and data longer than they should. Paper-based approval processes can complicate and slow the process of shutting down or adjusting user access, which can frustrate employees. Identity management solutions can help by introducing standardised workflows and automating many processes related to the identity lifecycle.

Changing business consumption models

In today's complex business environment, organisations are increasingly extending their business processes into the cloud. As new software consumption models emerge, managing user access to these cloud applications within and beyond enterprise boundaries can become a challenge. For example, you may have identity and access management processes that were originally defined for on-premise landscapes and don't necessarily work for cloud applications. Addressing this would mean reassessing requirements based on changing business needs and then determining how to manage users in the cloud.

Identity management solutions can help by protecting existing identity management structures, provisioning relevant data to cloud applications, and helping your organisation build on what it already has, rather than reinventing the wheel.

Increasing compliance requirements

One of the key factors driving the adoption of identity management solutions is compliance requirements. Numerous laws and industry-specific regulations – for example, in healthcare or

banking – require that your organisation be able to report with certainty who had access to what system resources and when. Identity management solutions help you achieve compliance, enforce SoD policies, provide audit trails, and prevent unauthorised access.



Effective identity management:

A lifecycle approach

In addition, there's a broader challenge of managing identities across the hire-to-retire lifecycle of an employee – from the onboarding process to the termination of their employment contract. Without an identity management solution that automates tasks, supports employee self-service, and centrally tracks access and permissions, things can get complicated quickly. The manual work required to provision and manage user access in a compliant and auditable manner can become increasingly labour intensive, repetitious, and error prone.

When employees are hired, your organisation gives them certain permissions in a variety of systems. Later, an employee may receive a promotion or change roles and receive new, additional permissions. Furthermore, you may need to grant other temporary privileges for some year-end activities or while an employee is covering for a colleague on vacation. Thus, an employee typically tends to accrue privileges over time and often continues to have access that's no longer required for their current role. This is, of course, a security risk. But it's also a potential compliance violation. Adding a new role might cause conflicting authorisation for the user.

Consider this example: A purchasing manager is authorised to issue orders to external vendors, for example, to buy office supplies. To step in for a colleague on sick leave, this purchasing manager temporarily needs the authorisation to create vendors in the system. The employee could now misuse this role, create a new fictitious vendor, and issue an order. To minimise the risk that comes from such SoD violations, you must perform a compliance check for all role assignments that apply to critical business processes, such as ERP system roles. Finally, when the employee leaves your company, the access that this user has may still not be revoked, perhaps even years later, which presents obvious and ongoing security risks to your organisation.

At each stage, you need to provide users access to the right set of applications according to their current role – no small task without a deeper understanding of employee roles and responsibilities and an automated way of managing this work across an evolving IT landscape.



SAP Identity Management shifts the responsibility of identity management from the IT department to each line of business – or more specifically, from

IT administrators to business process owners.

SAP Identity Management: Taking a business-centred lifecycle approach

The SAP Identity Management component simplifies and optimises how your organisation grants and manages user access to SAP and third-party applications to help ensure that this work is performed:

- Securely, efficiently, and in a timely manner
- In alignment with your business processes and roles
- In accordance with audit and compliance requirements

The component provides a central mechanism for provisioning users and assigning them appropriate business roles and permissions. It goes beyond

traditional identity management to support related processes such as password management, self-service, and approvals workflows. Equally important, it shifts the responsibility of identity management from the IT department to each line of business – or more specifically, from IT administrators to business process owners who have a deep understanding of employee roles and responsibilities.

The table provides an overview of the core capabilities of SAP Identity Management.

Key features and functions of SAP Identity Management

Business-driven identity management	Tightly integrated into your SAP business applications, the SAP Identity Management component offers a one-step approach to user administration for your SAP and third-party software landscape – on premise and in the cloud.
Cloud connectivity	You can extend your identity management processes into the cloud by connecting SAP Identity Management to the Identity Provisioning service of SAP Cloud Identity Services. This approach combines your tried-and-tested processes with the flexibility and ease of use that comes with a cloud-based identity provisioning solution.
Reporting and auditing	Critical for compliance, extensive auditing functionality enables you to produce reports based on current access and past events. If questions come up, reports can conclusively state whether the person in question had entitlements to particular applications and associated features and functions. You can transparently maintain changes to data, user access rights, and administrative permissions. Tight integration with the SAP Access Control application and the SAP Cloud Identity Access Governance offering allows for the effective mitigation of SoD risks and a compliant user-provisioning process. In addition, privileged access management can be used to meet more critical and sensitive access requirements.
Provisioning, workflow, and approvals	Business rules and policies drive assignment and maintenance of user access rights across multiple systems. You can quickly provision employees and business partners, and changes and approvals are auditable.

Key features and functions of SAP Identity Management

Password management and employee self-service	The component supports self-service password reset and password synchronisation across connected target systems, as well as the ability to perform self-service updates of personal information. These functions help reduce the cost incurred by your help desk in servicing password resets.
Roles and entitlements	Roles align with business processes rather than technical directory structures. Users are assigned roles and given certain privileges, called entitlements, that enable access to various systems.

Integrated user provisioning

Functionally, SAP Identity Management supports user provisioning by offering one centralised place from which to manage users in SAP and third-party applications, regardless of the individual data stores. This means that, for example, when a phone number or e-mail address is changed in one system, it automatically updates across relevant systems.

You gain:

- Tight integration with your company's business processes
- Built-in connectivity with SAP Cloud Identity Services for smooth compatibility and integration of on-premise and cloud identity management processes
- Integration between SAP Identity Management and SAP Cloud Identity Services, which offers comprehensive identity lifecycle management capabilities in hybrid IT landscapes

Supporting heterogeneous IT landscapes

SAP Identity Management enables you to streamline the provisioning of users into applications (both SAP and third party), operating systems, file systems, and databases using an ever-expanding library of built-in connectors that come with the component. You can also buy connectors from SAP partners or develop your own using an SAP-provided connector development kit. The integration is based on open communication standards that enable the integration of most applications, including Microsoft Active Directory, Microsoft Exchange, IBM Lotus Notes, and many others.

Extending the identity lifecycle to the cloud

As shown in Figure 1, you can extend SAP Identity Management to the cloud by connecting to SAP Cloud Identity Services. This option opens up numerous possibilities for designing hybrid scenarios for your business processes.

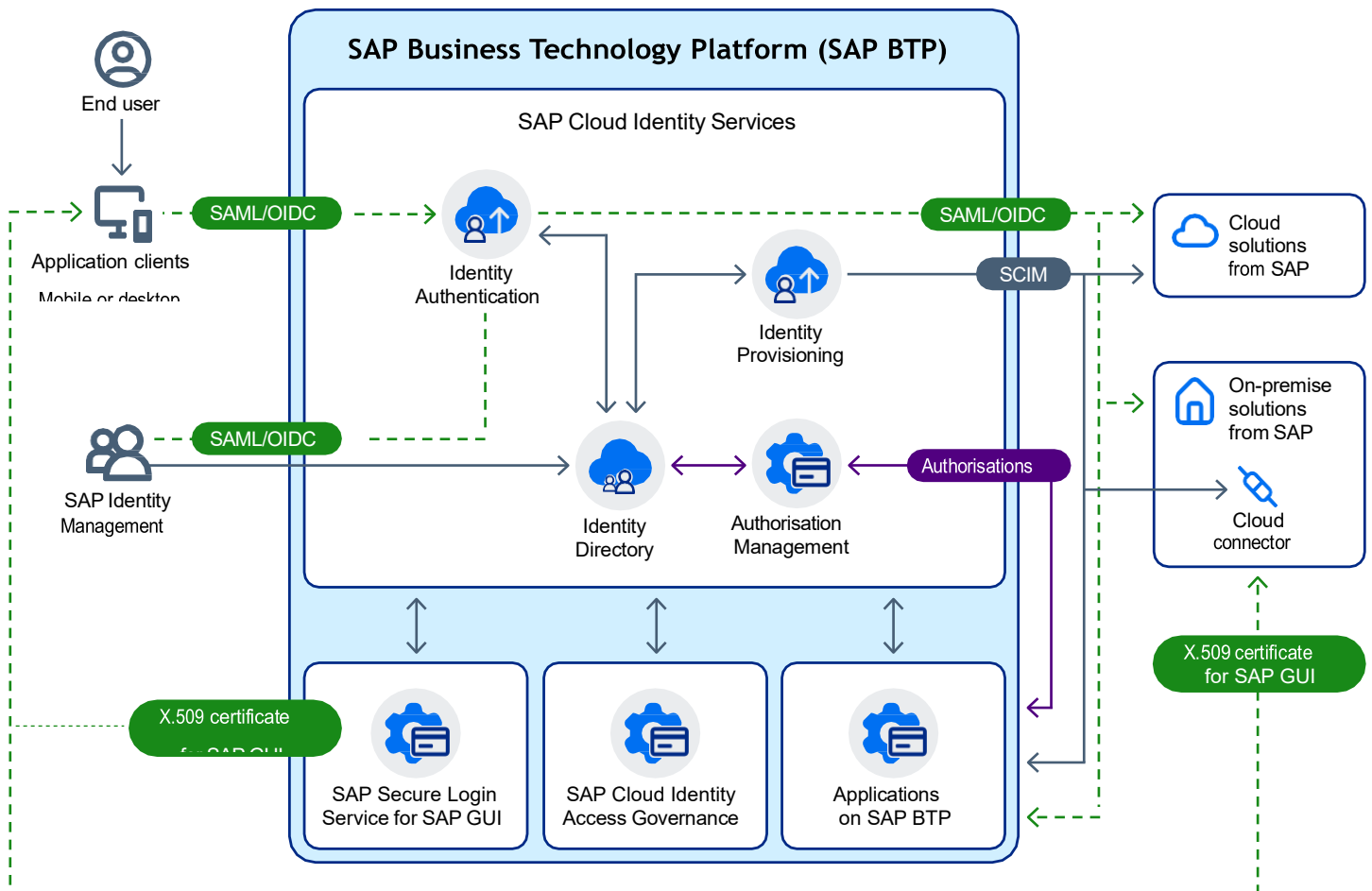


Figure 1: SAP Identity Management extends to the cloud

Enabling business-driven identity management

Identity management solutions were originally developed to help IT organisations better manage users across multiple applications. Essentially IT efficiency tools, they streamlined the process of user management by providing a central mechanism to enable these processes.

Business process integration across your intelligent enterprise

You can realise even greater benefits by aligning user management functions more closely with the core business processes that users access (see Figure 2). SAP Identity Management streamlines this alignment through integration with SAP S/4HANA – the heart of your business where processes run – and plays an important role in the integration aspect of an intelligent enterprise. When you integrate identity management solutions with SAP S/4HANA, you connect identity management processes with business processes, moving them away from the IT world and into the business world. For example, by connecting SAP Identity Management with the SAP ERP Human Capital Management solution, you can automate identity management processes across the hire-to-retire process, one of the key pillars of an intelligent enterprise. This enables identity management across the employee lifecycle, from creating a new user in the system to job changes and promotions and even the retirement of an employee or the termination of a user's contract.

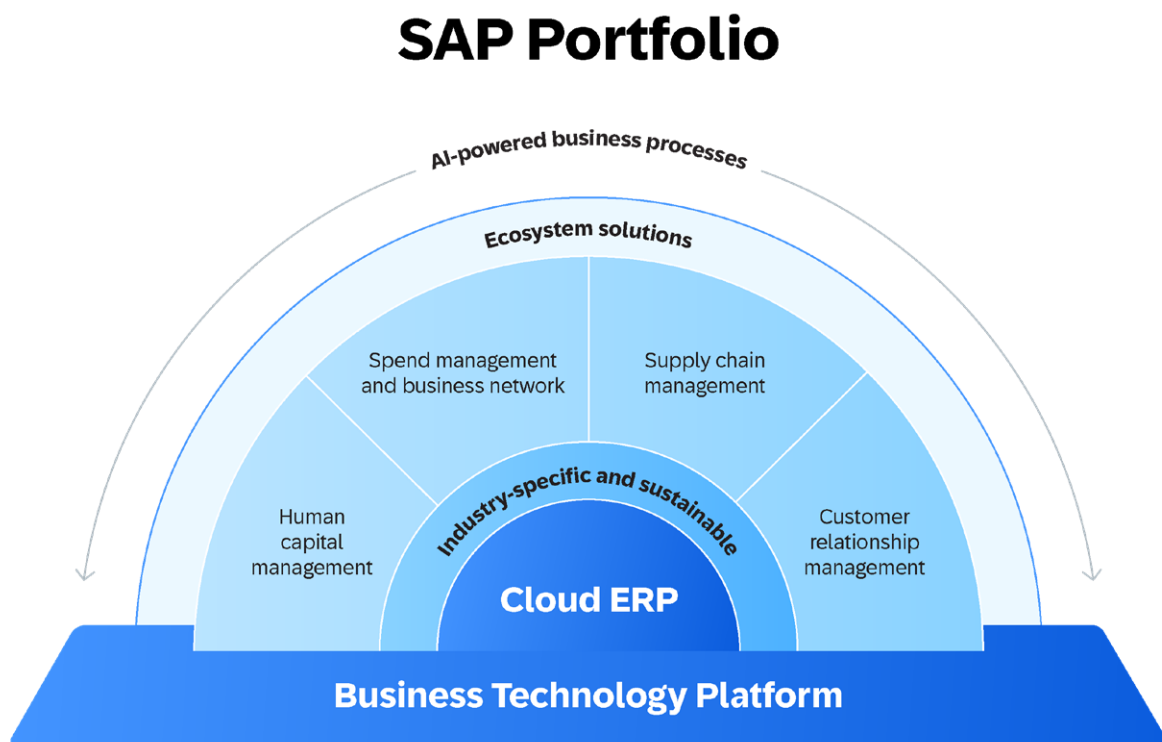


Figure 2: Core business processes that can be aligned with user management functions

Integration across intelligent enterprises is not limited to employee-related processes. For example:

- SAP Identity Management supports processes for business partners and customers, such as the automated creation of users in the SAP Customer Relationship Management application and business partners in the SAP Supplier Relationship Management application.
- Integration with SAP Cloud Identity Services allows for tight integration of user data coming from on-premise applications with the cloud. It protects your existing investments and extends user lifecycle management to the cloud.

Support for business roles

SAP Identity Management supports a powerful role concept that helps improve business role definition and usage so you can reduce the overall number of roles across your organisation. Business roles, which are defined as part of a business process, can be assigned to users within a given application. These business roles consist of one or more technical roles, which are system specific and represent access information or technical authorisations.

These include authorisation roles such as those for SAP software systems that are based on the ABAP programming language or groups for Microsoft Active Directory. By focusing on business processes and business roles, SAP Identity Management simplifies the creation of roles and authorisations by letting managers start with the business requirements they know best, with no need for them to deal with the underlying IT complexity.

When you assign a business role to a user, technical roles for that business role and any role below it in the hierarchy are assigned to the user. In addition, workflow and provisioning are automatically triggered.

By complementing identity management functionality with a governance, risk, and compliance solution for managing access control – such as SAP Cloud Identity Access Governance or SAP Access Control – you can enable compliant identity management. Specifically, you can help ensure that roles and authorisations assigned to a user don't contain conflicting rights. As a result, you're not only securing the identity management process but also making it more compliant and auditable.

SAP Identity Management offers compliant user provisioning and reporting and audit functionalities. By integrating SAP Identity Management with SAP Cloud Identity Access Governance software and the SAP Access Control application, you can prevent SoD violations, such as when roles with conflicting permissions are assigned to a user, and put mitigating controls in place. Your organisation can get and stay clean on the SoD front, as well as retain control of access to applications in your system landscape – from SAP S/4HANA to third-party applications.



Integration between SAP Identity Management and SAP Cloud Identity Services offers **comprehensive identity lifecycle management capabilities** in hybrid IT landscapes.

Taking identity management to the next level

As a business-oriented component, SAP Identity Management shifts the responsibility for identity management your from IT administrators to business process owners – the people who understand employee roles and responsibilities best. For example, line managers can approve role assignments rather than IT staff. At the same time, you can:

- Simplify processes related to identity management
- Centralise identity management across applications
- Extend identity management into the cloud
- Free up IT resources by shifting responsibilities to lines of business
- Improve compliance by giving identity management responsibilities to those with a deeper knowledge of the business and compliance requirements
- Provide richer auditing and reporting functionality
- Integrate with SAP governance, risk, and compliance solutions to prevent SoD violations

Perhaps most important, the component supports identity management across SAP software as well as your heterogeneous and hybrid third-party landscape, including Lightweight Directory Access Protocol, third-party business applications, operating systems, e-mail systems, and databases.

And finally, by lowering total cost of ownership and increasing operational efficiency, SAP Identity Management helps you meet your organisation's objectives of lowering operational costs, increasing productivity, and improving compliance and audit- ability of processes related to user management in your organisation.



Learn more

To learn more about SAP Identity Management and how it can help improve your business, please contact your SAP representative or visit us [online](#).

SAP Cloud Identity Access Governance

The SAP® Cloud Identity Access Governance offering, integration edition helps support access governance capabilities for on-premises and SAP line-of-business cloud applications. This is a pure cloud solution with a pricing metric based on number of resources, which are the unique monitored users in the software. The software will synchronise monitored users among connected applications.

The standard edition supports:

- Self-service access request that enables end users to search for roles and submit access requests for approval
- Complete management and analysis of access risk with a remediation workbench, along with management and monitoring of mitigation controls
- Complete set of role design features, from role mining and discovery to automated candidate role creation and implementation
- Access certification features for automated attestation or access review for user access, management of SoD risks, and role assignments to managers and risk and role owners for periodic reviews
- Complete privileged access management enabling temporary elevated access for urgent situations and including post-session log review for audit compliance

The SAP® Cloud Identity Access Governance offering, integration edition helps support access governance capabilities for on-premises and SAP line-of-business cloud applications. This edition is designed specifically to extend access control for cloud applications and is priced differently from the standard edition, using a metric based on number of system connections. It has a limited set of features to reduce functional overlap with the SAP Access Control application.

SAP Cloud Identity Access Governance:

- - Has a full version of the access risk analysis feature
- - Supports user provisioning fulfilment (but not the full access request feature)
- - Includes role management features for creation, editing, and import of business roles (but not for automated candidate business role design).

NOT included are

- - Privileged access management
- - Access certification
- - Audit log reporting

Key Features

Access Analysis Service	Lets you streamline access with real-time visualisations.
Role Design Service	Allows you to create, optimise, and maintain business roles for cross-business applications.
Access Request Service	Helps you create self-service access requests to business applications and HR-event driven identity lifecycle.
Access Certification Service	Helps you review and certify user access with auditable workflow.

Privileged Access Management Service	Lets you manage workflow-driven auditable privileged access granting and review processes.
---	--

Service Levels and Support

For productive system the service level for availability is 99.7%. For non-productive systems (development, test) the service level for availability is 99.5%.

Additional cost options are available to increase the availability to higher levels for the Private Cloud option for productive systems.

Software Support is provided by SAP Enterprise Support. Additional cost options are available for enhanced support from SAP and details are available on request.

NDBS can also provide additional application and technical managed service support for the application which enhances the SAP Enterprise Support with additional support for the application and the technical elements of the application. This can include 'how do I?' and 'break-fix' type support.

Maintenance Windows

For Public Cloud, there is a weekly maintenance window (Saturday 22:00 UTC) for 4 hours. In addition, there are up to 4 major upgrade windows per year (Saturday 04:00 UTC) for 24 hours. There are 2 upgrade releases that must be taken.

For Private Cloud – there is a major release every 2 years, with interim Feature Packs every 6 months. Upgrades are optional in Private Cloud, but the customer must be on a maintained release (hence must upgrade at least every 7 years). Subscription includes costs for the upgrade every 2 years.

Offboarding, and Access to Data

When offboarding, for the Public Cloud solution SAP provides tools to download the data from the service. It is the customer responsibility to download the data prior to contract termination. Additional cost options can provide enhanced support from NDBS to support the customer in the offboard and data extraction elements up to the contract termination.

For the Private Cloud solution the customer is responsible for extracting relevant data prior to contract termination. Additional cost options can be provided enhanced support from NDBS to support the extraction of the data.

Business Continuity

For Public Cloud, the production system is backed up daily along with multiple archive logs taken daily. Non-productive systems are backed up weekly along with multiple archive logs taken daily. Backups are stored in a secure offsite location. Backup cycles for production data is 28 days; for non-production data the cycle is 14 days.

Enhanced Business Continuity coverage is available as an additional cost service.

After Sales Support

SAP provides Enterprise Support for the duration of the subscription (software support). NDBS can enhance the Enterprise Support, by providing highly flexible Application and Technical Managed Services for the buying organisation. As these can be tailored for individual customer requirements, NDBS can provide specific detail on application.