SAP Cloud ALM in Regulated Environments

Contents

Abstract

Life science customers must independently assess the use of SAP Cloud Application Lifecycle Management (ALM). SAP is a technology provider of back-end business processes designed for general availability. SAP provides this document for informational purposes only. Any information outlined in this document may change at any time at SAP's discretion.

This document outlines SAP's efforts to support life science customers implementing SAP Cloud ALM. Life science customers must comply with sector-specific regulatory requirements, including laws and recommended practices per industry, or GxP. Industry-related GxP includes good laboratory practice (GLP) for laboratories, good manufacturing practice (GMP) for manufacturing, and good clinical practice (GCP) for clinics.

Life science customers are required to adequately assess the security and quality management services of SAP Cloud ALM. This white paper provides information that life science customers operating in GxP-regulated security environments may use in their side of audits or inspections.

Cloud computing, including software as a service (SaaS), is a cloud service category. Beyond the standard GxP complexities, it introduces additional considerations as it becomes an increasingly vital technical solution across various industry sectors. Customers seek highly scalable, reliable, and secure solutions. Due to its efficiency and value, cloud computing is steadily receiving a higher priority.

This white paper outlines practices that life science customers use, including internal quality and development practices critical for GxP compliance. The following outlines each party's focus on GxP requirements.

About SAP Cloud ALM

SAP Cloud ALM is an offering for application lifecycle management (ALM). It’s intended for customers who use multi-cloud and hybrid solutions by SAP.

SAP Cloud ALM helps customers to implement and operate intelligent cloud and hybrid business solutions.

Customers benefit from an out-of-the-box, native cloud solution, designed as the central entry point to manage their SAP landscape with content-driven guided implementation and highly automated operations. The key value of SAP Cloud ALM is that it can help to:

Experience optimal support experience.

Minimize effort to adopt and operate the suite of Cloud ERP, complemented by human experience management (HXM), SAP Intelligent Spend and Business Network (ISBN), and customer experience (CX).

Reduce total cost of implementation and end-to-end operation.

Consolidate all the solutions that help customers to implement SAP solutions faster and operate them better.

SAP Cloud ALM is included in customers' cloud subscriptions that contain SAP Enterprise Support, cloud edition, and in SAP Enterprise Support.

More:

- SAP Cloud ALM (SAP Support Portal)
- SAP Cloud ALM (SAP Help Portal)

SAP Cloud ALM in a regulated environment

Life science customers are subject to strict regulatory surveillance. They are required to prepare themselves to demonstrate their compliance efforts with regulators. Although life science customers are solely responsible for assuring compliance with GxP laws and practices, SAP ensures that GxP guidelines are followed to demonstrate minimal viable compliance.

SAP summarizes specific GxP-relevant information for SAP Cloud ALM, as follows:

Technical and procedural measures and controls

SAP's institutional knowledge to develop and operate SAP Cloud ALM in a controlled state

How to ensure the confidentiality, integrity, and availability of customers' data

Such information enables life science customers to assess their compliance with GxP.

To make this information more accessible, this white paper consolidates and further highlights GxP-relevant aspects, like the quality management system (QMS) for SAP Cloud ALM, software development and operations lifecycle (SDOL), and IT operations and services.

More:

- SAP Cloud ALM in Regulated Environments (SAP Support Portal)
- The latest version of this document: SAP Cloud ALM in Regulated Environments (PDF)

Certifications and attestations

SAP Cloud ALM follows the SDOL process given by SAP.

As per corporate requirement for software security, it is mandatory to fulfill the Secure SDOL requirements.

SAP's innovation lifecycle and the SDOL is certified in ISO 9001 and ISO 27001. SAP Cloud ALM follows these processes and controls for its development.

Both certificates are available in the SAP Trust Center (ISO 9001 quality management system and ISO 27001 information security management system). More information about the SDOL is available in the document The Secure Software Development Lifecycle at SAP.

Architectural overview

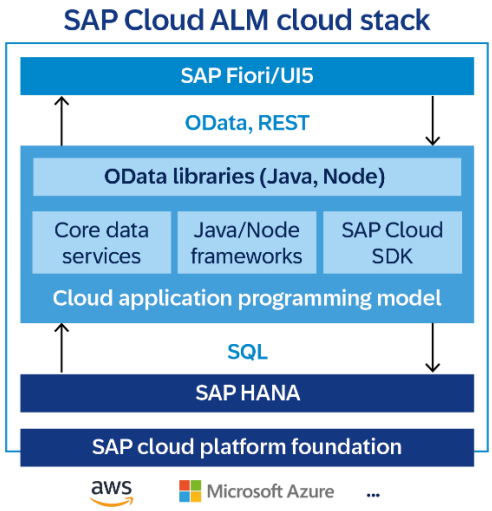
SAP Cloud ALM is SAP's cloud-based application lifecycle management offering.

There is an automated onboarding process for SAP Cloud ALM that customers can trigger from SAP for Me. This creates one global account with a subaccount for the SAP Cloud ALM subscription.

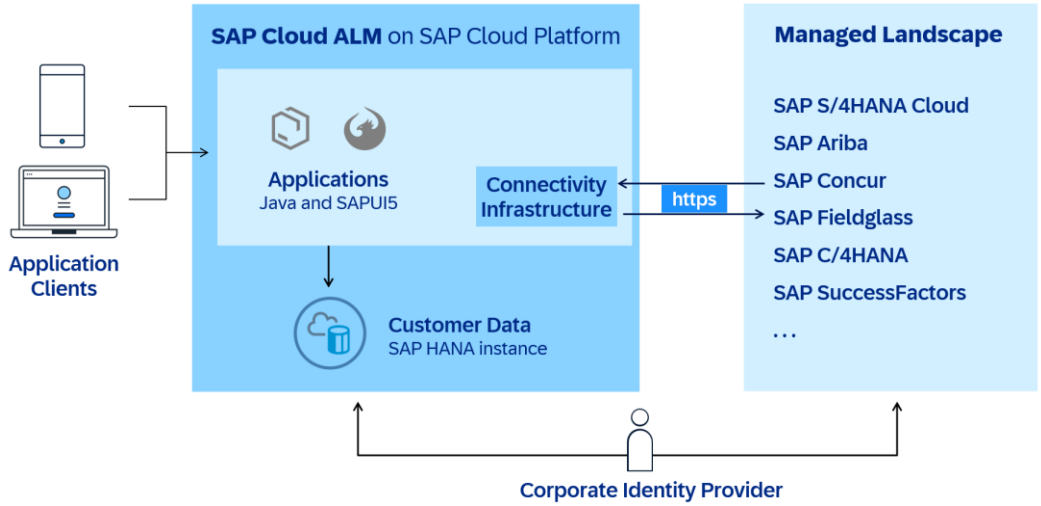
SAP Cloud ALM is built on SAP Business Technology Platform (BTP), in a Cloud Foundry environment. The software stack enables programming services with the Cloud Application Programming (CAP) Model of SAP BTP.

SAP Cloud ALM currently contains more than 90 microservices, which are implemented in Java.

SAP uses a domain-driven design to model the microservices.



The implementation stack of each microservice



Simplified view on integration architecture between SAP Cloud ALM and the Managed Landscape

To implement communication with business systems like SAP S/4HANA, the SAP Cloud software development kit (SDK) is reused. The SAP Cloud SDK is an abstraction and comfort layer on top of the Cloud Foundry stack. For example, it simplifies communication with open data protocol (oData) and reduces boilerplate coding for connectivity handling.

SAP Cloud ALM as a SaaS solution

SAP Cloud ALM is a SaaS offering. A cloud service provider, in this case, SAP, hosts these applications and makes them available to users over the internet. In contrast to software solutions that are traditionally deployed on premises, the software and underlying infrastructure of a SaaS solution is managed by service providers.

This requires specific security controls and compliance. Accordingly, SAP commits to providing information on its technical and operational measures within its control environment to assist the customer in assessing its compliance with GxP.

As part of life science customers' architecture governance, receiving assurances on security measures and quality management systems is an essential first step toward GxP compliance.

Customer-managed SaaS application

SAP Cloud ALM is a SaaS application on a customer-managed subaccount on SAP BTP. Like all customer-managed SaaS applications, customers are responsible for the following:

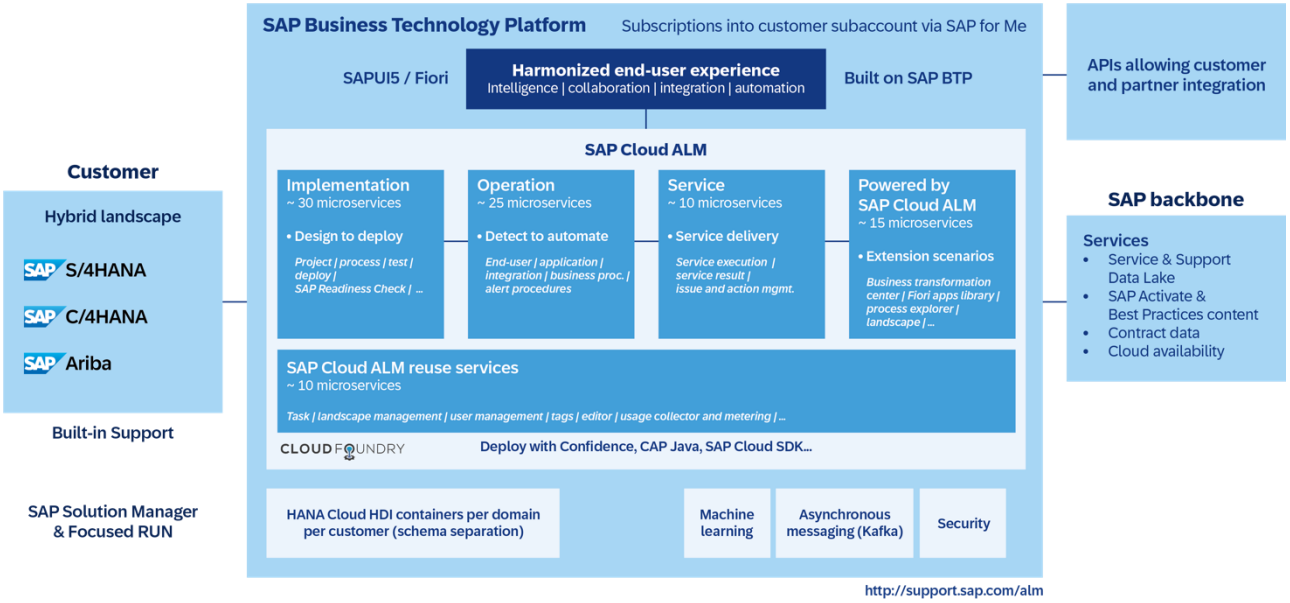
- global account
- subaccounts
- assignment of a tenant in the identity authentication service
- subscription
- configuration of the cloud services

However, where possible, SAP provides setup automation to simplify and streamline our customers’ tasks.

All microservices are

- consumed by customers in customer-managed SAP BTP subaccounts.
- deployed and operated in one provider subaccount per data center where SAP Cloud ALM is available for customer subscription.
- consumed per SaaS subscription.

There is no software deployment/installation per customer. The license materials are assigned to the global accounts of the customer-owned SAP BTP subaccounts so that the software can be subscribed to.



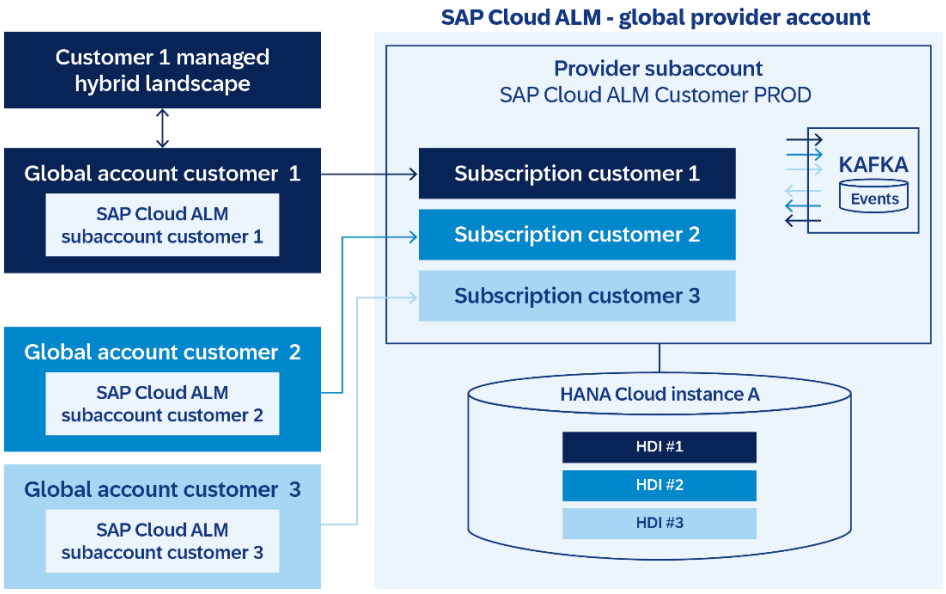
High-level architecture

Data separation

The SAP Cloud ALM architecture is based on multi-tenancy-enabled microservices. Multi-tenancy refers to software architecture in which tenants share the same technical resources but isolate data and users. In SAP BTP Cloud Foundry, several instances of each microservice may operate (depending on scalability and resiliency needs). Each instance may serve multiple customers (tenants). Efficient load distribution is managed via SAP BTP.

Data separation ins done by creating separate database schemas via separate SAP HANA Deployment Infrastructure (HDI) containers in SAP HANA Cloud. There is a separate HDI container per customer tenant and per domain. SAP Cloud ALM uses the recommended tenancy model of schema separation.

For resilience and scalability reasons, the HDI containers of the microservices are distributed across many SAP HANA Cloud instances per deployment. The minimum number of SAP HANA instances currently used per deployment is 16 and the maximum can be beyond 100. The HDI containers of the different microservices (domains) and customers are then distributed across the SAP HANA instances.



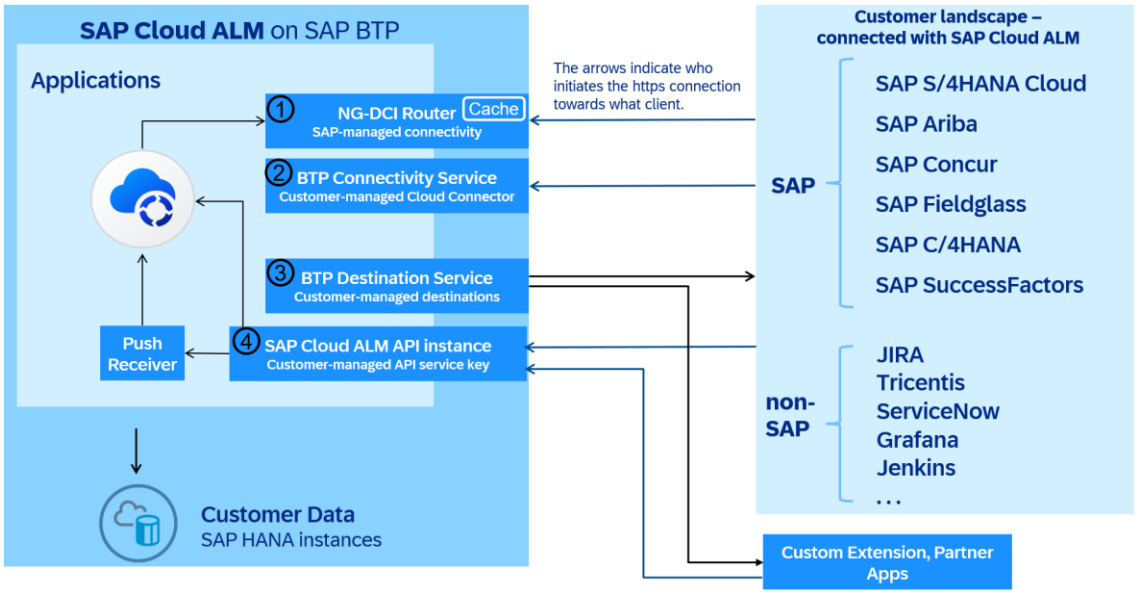
Simplified depiction of separated HDI containers on one SAP HANA Cloud instance.

To better understand the SAP BTP subscription model, some introduction to the SAP BTP domain model is helpful. See Basic Platform Concepts for SAP BTP.

Managing integration between SAP Cloud ALM and the managed systems/services

Managed systems and services vary significantly in their architectural designs and operational models. These differences directly influence the effective integration with SAP Cloud ALM. The overarching goal is to establish a secure, straightforward, and automated integration process.

The optimal integration depends on the specific type of the managed system or service. Hence, SAP Cloud ALM supports various integration methods to accommodate different system landscapes and connectivity requirements. The detailed setup guides per managed product are referenced under Integration and Configuration Options for SAP Cloud ALM.



Methods of integration between SAP Cloud ALM and the Managed Systems/Services

For each system and service type that needs to be integrated, there is an optimal method. How to perform the setup is described under:

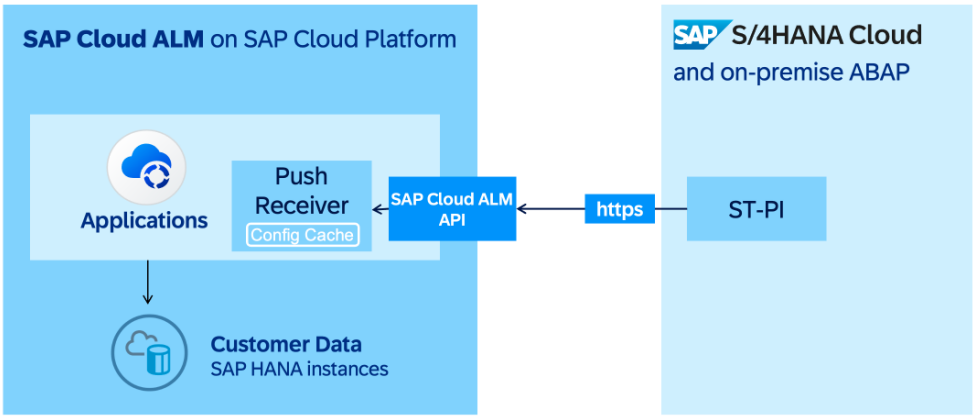
- Integration and Configuration Options for SAP Cloud ALM
- Connecting Systems and Services

The integration options can be grouped into four main categories:

1. **SAP-managed integration using NG-DCI**
   The Next Generation – Data Collection Infrastructure (NG-DCI) provides a secure integration mechanism where SAP manages the technical integration setup. It is available for many standard SAP solutions. More under OpenTelemetry and NG-DCI.
2. **Integrations using the Cloud Connector**
   A limited number of use cases (e.g. SAP Focused Run and SAP Business Transformation Center) require a specialized setup leveraging SAP Cloud Connector. More under Setup information for SAP Focused Run and Setup of Business Transformation Center.
3. **Integrations using the Destination Service in the BTP subaccount of SAP Cloud ALM**
   This method allows calling from an SAP Cloud ALM tenant to an external system or service via the internet. It uses destinations that are managed in the SAP BTP subaccount on which SAP Cloud ALM is subscribed. Destinations define the connection parameters and credentials for third-party or SAP-managed services. This type of integration is utilized for several scenarios:
   - The PULL data collector is mainly used in SAP Cloud ALM for Operations. Example: Integration of SAP Integration Suite (Cloud Integration) on Cloud Foundry.
     PULL data collection can be realized for non-SAP systems, too. See Outbound Metrics API
   - SAP Cloud ALM to call into external systems or services, for example, to notify on events. Example: External system maintains Events in SAP Cloud ALM.

4. **Integrations using the SAP Cloud ALM API instance**
   SAP Cloud ALM provides an API endpoint that can be called from the internet to connect to SAP Cloud ALM. It's a point-to-point connection between the two involved communication partners. The API instance is bound to the SAP BTP subaccount where SAP Cloud ALM is subscribed to. This type of integration is utilized for several scenarios:
   - The PUSH data provider is used mainly in SAP Cloud ALM for Operations. Example: Connect SAP S/4HANA and SAP Business Suite 7 on-premise systems to SAP Cloud ALM.
   - SAP systems and services to call into SAP Cloud ALM via APIs. Example: Integration of LeanIX.
   - Customer-built SAP BTP applications can be instrumented to push monitoring data via the SAP Cloud ALM APIs to the NG-DCI data routing infrastructure.
   - Custom extensions or third-party systems and services can use the SAP Cloud ALM APIs to integrate with SAP Cloud ALM. For example, to read Metrics from SAP Cloud ALM via API or use the Outbound Metrics API.

   Example: One common scenario is the integration between SAP Cloud ALM and SAP S/4HANA Cloud and on-premise ABAP.



Example for Method 4: Integration of SAP Cloud ALM with SAP S/4HANA Cloud

The connectivity is initiated via the ST-PI software component, which is part of the ABAP stack. In the ABAP environment, scheduled background jobs are executed to invoke the APIs of the SAP Cloud ALM API instance hosted on SAP BTP. The SAP BTP infrastructure routes these API calls to the appropriate SAP Cloud ALM applications.

This integration model is referred to as a **push-receiver** scenario in SAP Cloud ALM:

- The managed system regularly pushes data to SAP Cloud ALM.
- Additionally, the managed system can retrieve configuration changes and to-be-executed activities.

Release cycles

SAP Cloud ALM follows a bi-weekly release cycle to make new features visible to customers. This is also known as feature activation.

However, new code and features are deployed into production daily. New features are deactivated by using feature toggles until they are finally released to customers in one of the bi-weekly feature releases. SAP Cloud ALM follows the single-trunk methodology. So, there is only one single code line (and no separate release branches). The benefits to be highlighted are as follows:

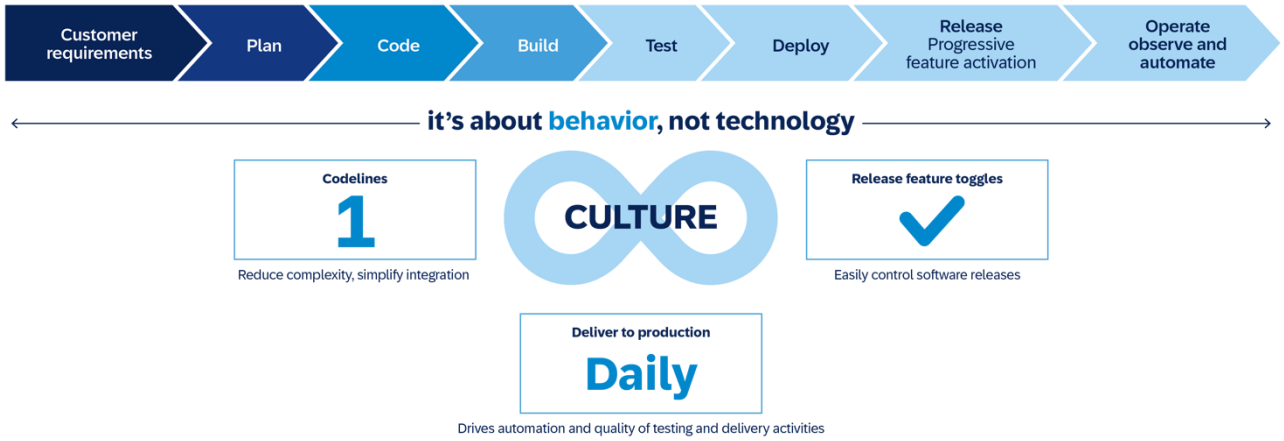
New code and functionality are promoted from development to production daily. There are no “big-bang releases” anymore; end-to-end deployment happens daily.

Continuous delivery into production–SAP doesn’t make new functionality visible to all users immediately. For example, SAP can control to make new functionality visible only internally for testing.

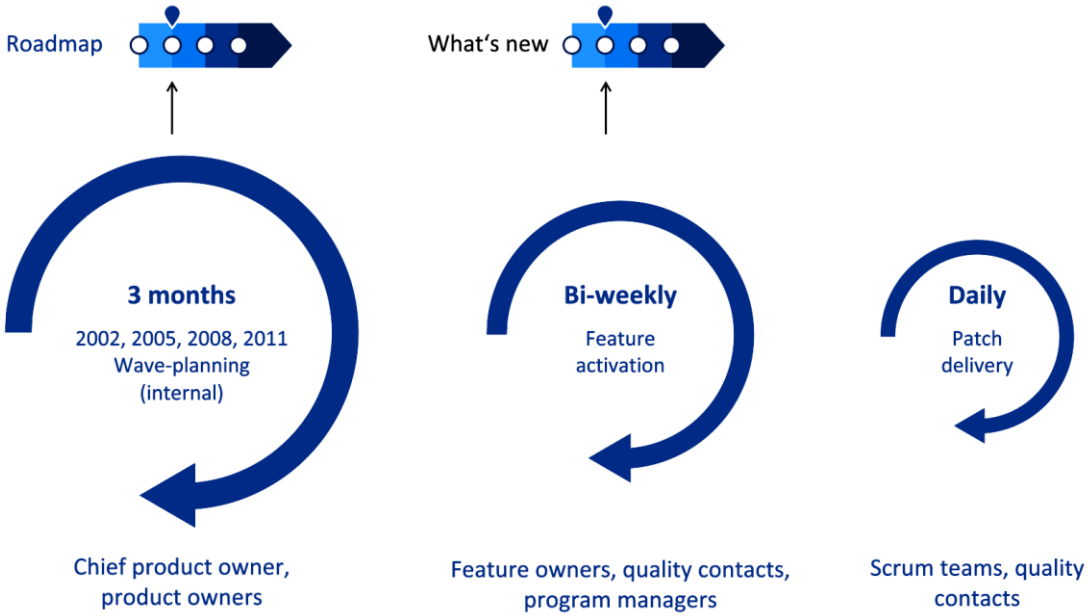
Once product management decides to make functionality generally available (for example, bi-weekly), SAP switches the related feature toggle on. This change is called release and makes the functionality available for all end users.

Zero downtime deployment and feature activation are enabled via organizational and technical means. The concepts ensure that no user session or API call is impacted by these changes. Users will not notice the updates at all. If new features were activated by a change, these get visible only after the user logs out and logs in again (or after auto-logout that happens after latest 24-hour usage).

In case of an emergency fix, bug fixes can be pushed to production within 30 minutes.



Principles for continuous delivery at SAP Cloud ALM: single codeline, daily deployment to production, use of feature toggles to control which features become available to customers.



Overall planning cycles for SAP Cloud ALM: quarterly waves, bi-weekly feature activation for customers, and daily delivery of patches.

Release notes are published for the traceability of changes. For more information see What's New for SAP Cloud ALM.

For the planned delivery of key features in the next quarters, see SAP Roadmap Explorer for SAP Cloud ALM.

Quality management system of SAP Cloud ALM

The QMS covers the development of software business solutions. It aligns and orchestrates all development organizations to provide quality products and services to SAP's customers and ensures that SAP corporate requirements are fulfilled.

The QMS is designed to provide a strategic approach to software quality assurance. It aims to ensure consistency, reliability, and the ability to meet the intended requirements.

The system includes processes for planning, development, testing, inspection, and continuous improvement. Its goal is to detect defects as early as possible in the development process and ensure they are corrected. It also aims to prevent defects in future versions of the software.

The QMS includes standards for coding and documentation, as well as the use of specialized testing tools and techniques. It also includes procedures for handling and managing software defects.

SAP's quality management approach is heavily focused on process improvement. The company applies feedback from customers, partners, and internal groups to refine and improve its development processes. It also conducts regular audits and reviews to ensure compliance with its quality standards and procedures. SAP holds an ISO 9001 certificate for its SAP Development QMS as proof of SAP's commitment to quality and to fulfilling the expectations of SAP customers.

In summary, the QMS is a comprehensive, structured set of procedures and practices designed to ensure the highest quality in software development.

Document management

System lifecycle documents, including policies, procedures, designs, and other documents are stored on SAP internal systems.

Access is restricted to the respective authorized SAP personnel.

Versioning, restore, and historical data are provided.

The overall program management of SAP Cloud ALM is documented in SAP's central software development assurance tool for program management and quality assurance, which supports the innovation cycle process at SAP. It tracks corporate requirements and product standards. The integrated security hub supports the secure development lifecycle process. Furthermore, it supports the new compliance service Cumulus to visualize data coming from pipelines. The tool stores data like the evidence of fulfilled compliance to product standards.

Roles and responsibilities are clearly defined and documented in internal platforms, such as program leads, product owners, development owners, architects, quality accountables, and security coordinators.

Specifications and design papers for software development are managed in an SAP internal GitHub instance.

The program and product backlog are derived from the SAP Cloud ALM product roadmap laid out by the chief product owners. The planning of key features happens in quarterly waves.

Requirements and feature definitions for the continuous development of SAP Cloud ALM are managed in SAP's central project and task management tool and broken down into portfolio epics, roadmap epics, user stories, and backlog items.

All development teams involved use predefined user story templates, which ensure that all required SAP product standards and the usage of defined quality tools.

The automated test results from the pipelines, through which every code change runs, are stored on platforms like Cumulus. This applies for legal and security topics, code quality, regression, and performance tests.

Results for additional manual testing are attached to the central quality assurance (QA) platform. This applies for penetration, accessibility, and language tests.

New employees joining SAP Cloud ALM are trained to follow the defined processes and to correctly use the involved tools. SAP Cloud ALM has, for example, a Learning Compass for new colleagues, for which managers can also track the completion of all steps.

SAP Cloud ALM follows the agile and scrum methodology, ensuring aligned development processes.

SAP Cloud ALM follows SAP's "golden path standard for cloud development."

SAP ensures audit trail in development through various methods including:

Version control: SAP uses version control systems to track changes made to the software code, configuration settings, and other development artifacts. This allows developers to review the history of changes and revert to previous versions if necessary.

Change management: SAP employs change management processes to track and manage all changes made to the development environment, including code updates, database changes, and configuration modifications. This helps ensure that all changes are planned, documented, and reviewed before implementation.

Logging and monitoring: SAP includes logging and monitoring capabilities in its development tools to record and track all activities and changes made by developers. This ensures a detailed audit trail of who made which change and when it was made.

Access controls: SAP implements access controls and permissions to restrict access to development environments and ensure that only authorized users can make changes. This helps prevent unauthorized changes and ensures accountability for all development activities.

By utilizing these methods, SAP can ensure a robust audit trail in the development process, allowing for transparency, accountability, and traceability of all changes made to the software. However, it's always good to also note that while these features ensure accountability, they also rely on good practices made by the development team and systems administration to be truly effective.

Risk management

SAP's risk management policy provides a structured approach to identifying, prioritizing, and directing risk management activities for SAP Cloud ALM.

SAP Cloud ALM operates according to the applicable SAP corporate standards for risk management and covers the following steps:

- Risk identification
- Risk validation
- Risk analysis
- Risk management
- Risk monitoring
- Risk planning

Software development operations lifecycle

The product teams of SAP Cloud ALM follow the secure SDOL (SDOL). This secure software development lifecycle (SDL) provides a framework for training, tools and processes. As security is in the vital interest of anyone who is using SAP products and services to run critical business processes and to store and process sensitive data, secure developed software is a prerequisite for

secure operations. More information is available in the document [The Security Software Development Lifecycle at SAP.]

SAP develops SAP Cloud ALM according to the SAP quality management system processes of its respective product standards. In the reference landscape, test strategy and test evaluations confirm adherence to the quality criteria set in the product standards.

Test cases and test plans provide traceability from requirement to release, which SAP maintains in its internal product management and quality assurance tools.

Requirements implemented during continuous delivery cycles, including planning, are brought to requirement clarity between product management and development before the system design breaks down to epics, user stories, and backlog items and implements development tasks (coding and review).

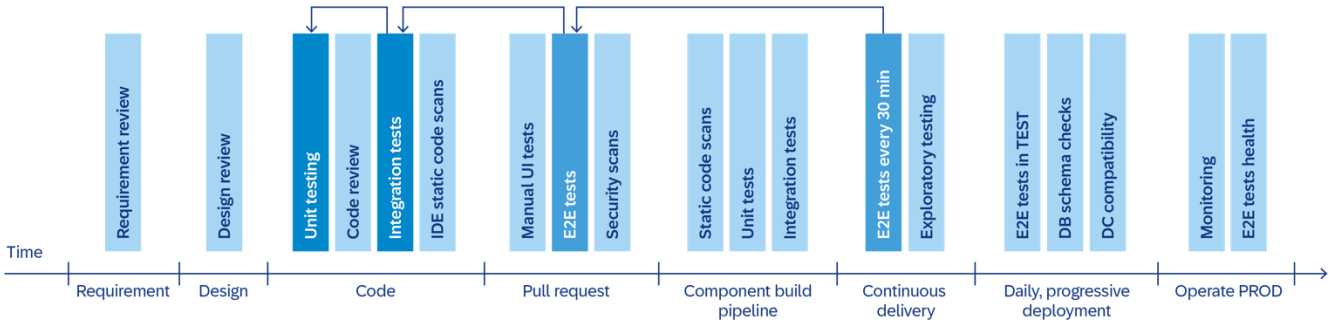
SAP development follows an agile methodology (scrum) and continuously creates test cases without composing a sequential cascade of sprint delivery.

To maintain consistent quality and to meet product standards throughout the agile development process, the test approach relies on full test automation. Before deployment to production, SAP investigates all defects detected according to resolution priority.

With the bi-weekly activation of features for customers, SAP publishes also updates of the documentation.

SAP continuously improves the test strategy as necessary via root cause analysis (RCA) of defect reports.

Following a continuous development concept, with daily deployment to production, the shift left principle is crucial. Shifting left means doing any quality-related activity as early as possible in the development process. As the earlier issues are found, the easier it is to fix them or even automatically avoid that they happen in the first place.



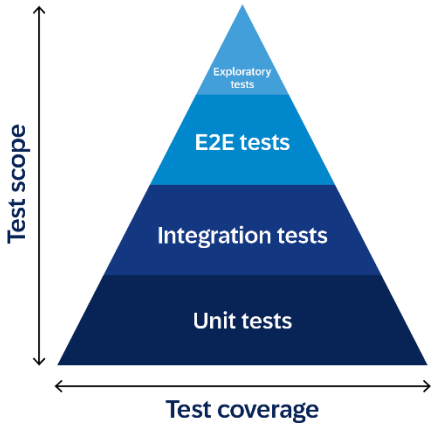
Shift left principle in software testing for SAP Cloud ALM

Exploratory tests are manually executed, case by case.

Automated end-to-end (E2E) acceptance tests focus on whether all components integrate well, for a few straightforward scenarios.

Integration tests focus on integration of your units as well as integration with frameworks, services, and resources, locally for the component.

Unit tests focus on the functional correctness of a feature. The focus is on local units and isolation from classes that are not under local control. We cover >80% of code in unit tests.



Test pyramid illustrating that most tests are done at an early stage (shift left) with a high level of automation.

SAP Cloud ALM is created in compliance with the SAP product standards, which define general software qualities and specific quality criteria for how to achieve them, such as:

- Accessibility
- Functional correctness
- Globalization
- Integration
- Operations support
- Performance
- Security
- Software lifecycle
- User assistance
- User experience

SAP verifies product standards compliance by a test evaluation report outlining the testing results.

Traceability from requirement to release is maintained by linking all process-related information to the requirement via its issue ID in SAP's central project and task management tool.

Before preparing systems designs and during the requirement engineering stage, the program management and development representatives refine each requirement in scope for realizability and clarity. Each system design comprises one or more epics consecutively broken down into user stories and backlog items (containing the definition of done and acceptance criteria) and development tasks.

For feature delivery, SAP converts requirements to code according to user stories and development tasks, scans for code correctness, and verifies it in unit tests.

After pull request and approval, the code enters the continuous integration automation towards the internal deployment infrastructure for integration and regression testing as defined by quality gates (Q-Gates).

For each feature delivery, SAP publishes user-assistance documentation for customers, which provides information about the upcoming release:

- Release Notes (What's New Viewer)
- Feature Scope Description
- Application Help
- In-app help

Approval for release to productive customer tenants, which happens bi-weekly, requires a release recommendation provided during a release decision meeting (RDM).

Compliance and security

The SAP global security policy applies to all businesses within SAP, all SAP employees, all external parties granted access to SAP Information, and all information and assets owned by or administered by SAP. It defines the company-wide requirements for the protection of SAP's personnel, their work, and the information entrusted to SAP by its customers.

SAP Cloud ALM follows SAP's global security requirements and with compliance and security standards.

Compliance and Security Standards: SAP Cloud ALM is compliant with SAP-internal technical policies, procedures, directives, guidelines, and product standards, such as the directive for network device security and the directive for cloud infrastructure.

The major areas covered by SAP Cloud ALM are **Compliance – Data protection and Privacy** and **Product Security.**

Compliance – data protection and privacy

SAP Cloud ALM is compliant with data protection and privacy requirements, ensuring that personal and sensitive data is collected, processed, stored, and shared in alignment with SAP's standard compliance guidelines.

It protects the data from unauthorized access, misuse, loss, or breaches through appropriate security measures.

In addition to compliance with general data protection and privacy acts, it's necessary to consider compliance with industry-specific legislation in different countries. SAP provides specific features and functions to support compliance with relevant legal requirements, including data protection. SAP doesn't give any advice on whether these features and functions are the best method to support company, industry, regional, or country-specific requirements.

More under Data Protection and Privacy (Trust Center) and Data Protection and Privacy for SAP Cloud ALM (SAP Help Portal).

Data classification

SAP Cloud ALM receives customer data through SAP-managed cloud services that are integrating with SAP ALM, from the SAP CRM system (Customer Relationship Management system), and directly from customers who upload documents.

The customer data can contain **personal data**, **business data**, **landscape data**, **technical data**. This data is processed by SAP Cloud ALM. The data is owned by the customer and controlled by the customer, here SAP Cloud ALM follows the SAP Cloud contract as outlined under General Terms and Conditions.

Following SAP's defined compliance guidelines, SAP Cloud ALM processes the following data across all included microservices:

- **Personal data for user logon:** SAP Cloud ALM process, customer user ID, email address, user first name and last name.
  Detailed documentation on user data that's exchanged with managed systems is available in User Data in Managed Systems – SAP Help Portal.
- **Business data and business personal data**: This data comes from the SAP-managed cloud landscape to SAP Cloud ALM. The data is owned by the customer as part of the SAP cloud contract.
  The data can contain business personal data. For example, when SAP Cloud ALM capabilities like Business Process Monitoring are active, business data, such as IDoc payload, PI message payload, or organizational structures are transferred to SAP Cloud ALM.
- **Landscape data:** Mainly related to the customer's landscape information, such as system IDs, URLs, and cloud service types.
- **Technical data: For example, SAP** HANA memory usage, response times, exceptions (check if exceptions may contain personal data), and availability data.

Data encryption

SAP Cloud ALM implemented encryption methods, protocols, and algorithms to help provide a secure path for data in transit through the SAP Cloud ALM infrastructure, and to help protect the confidentiality of data that is stored within SAP Cloud ALM.

Data segregation and minimization

A tenant-specific schema is in place to store each customer data separately.

SAP supports the multi-tenant architecture of SAP Cloud ALM, which supports security, confidentiality, privacy, integrity, and availability of data standards.

SAP Cloud ALM is designed with the assumption that all tenants are potentially hostile to all other tenants. Security measures to prevent the actions of one tenant from affecting the security or service of another tenant or accessing the content of another tenant are in place.

The two primary goals of maintaining tenant isolation are:

- To prevent leakage of, or unauthorized access to, customer data or content across tenants.
- To prevent actions of one tenant adversely affecting the service for another tenant. SAP Cloud ALM implemented multiple forms of protection to prevent customers from compromising SAP Cloud ALM services or applications or gaining unauthorized access to the information of other tenants including logical isolation of customer content within each tenant.

Identity and access management

SAP Cloud ALM ensures the access boundaries around personal and sensitive data and supports compliance with privacy regulations.

Logging

All activities related to data handling are logged in SAP Cloud ALM. More under Change and Audit Log.

EU and NS2 access

EU Access, which restricts the access to and processing of personal data to SAP employees located in EEA/Switzerland, is available for SAP Cloud ALM.

A special entitlement is required for EU Access. To have your SAP Cloud ALM tenant provisioned in an EU Access data center, you need to have a valid EU Access contract.
NS2 access, which restricts the processing of personal data to the U.S., isn't available.

For more information, refer to SAP Business Technology Platform–Regions.

Data transfer

SAP-managed cloud solutions and SAP Cloud ALM operate across geographically distributed data centers. It is essential to ensure compliance with regional data protection regulations while maintaining secure and reliable operations.

SAP Cloud ALM as **data processor** provides the contractual, technical, and operational capabilities that are necessary to support secure and compliant cross-border data transfer. Customers as **data controller** retain the responsibility for configuring their global accounts and

subaccounts and for fulfilling local regulatory obligations. SAP Cloud ALM facilitates this through robust support frameworks, regional hosting, and security measures.

The areas of implementation and operations in SAP Cloud ALM are consumed by each customer exclusively.

Customers have full control of which data from managed services and systems is transferred to SAP Cloud ALM. They need to actively connect their systems and services to SAP Cloud ALM, in the Landscape Management app, and configure the data collection process.
For more information, see Set Up Landscape Management and Connecting Services and Systems.

SAP Cloud ALM enables secure cross-border data transfer across data centers in different regions, with particular emphasis on complex jurisdictions such as China and the European Union (EU), KSA.

Examples:

- China: Local data center hosting for SAP S/4HANA to meet data localization requirements under China's Personal Information Protection Law (PIPL).
- Europe (EU): Regional data center hosting SAP Cloud ALM for monitoring and analytics purposes.

More about the shared responsibility model for security between SAP and customers: https://www.sap.com/about/trust-center/security.html --> *SAP cloud services shared responsibility model for security*.

Cross-border data transfer is the shared responsibility between SAP Cloud ALM, SAP cloud services, customers, and SAP BTP, and the hyperscalers.

SAP's responsibilities and capabilities

- **Data transfer impact:** SAP Cloud ALM performs data transfer impact assessments on a regular basis. The reviewed results are published in My Trust Center: SAP Sub-processors, data transfer factsheets & EU Data Act Online Register.
- **Data Localization and residency (China):** SAP-managed cloud services, such as SAP S4/HANA and SAP SuccessFactors, ensures in China that data remains within the geographic boundaries as required by Chinese regulations to meet China's Cross-Border Data Transfer (CBDT) obligations.
- **Secure cross-border communication:** encrypted data transmission: All metadata or operational data transferred from SAP S/4HANA in China to SAP Cloud ALM in Europe is encrypted in transit using TLS 1.2+, using HTTPS calls and BTP security process to transfer the data.
- **Legal and contractual framework:** SAP Cloud ALM includes Standard Contractual Clauses (SCCs) and regional processing terms in its agreements, providing a legal basis for the cross-border transfer.

- **Role-based access and monitoring:** SAP Cloud ALM ensures secure, role-based access to both systems, with attribute-based access control (ABAC), multi-factor authentication (MFA), and detailed audit logs.

Customer's responsibilities (with SAP support)

- **Data categorization**: Classify which data types, such as logs, KPIs, and alerts, can be shared outside of China.
- **Policy configuration**: Set up SAP Cloud ALM to ensure only allowed data types are integrated from SAP S/4HANA.
- **Cross-border data transfer compliance**: If required, complete China's filings for cross-border data transfer and ensure a lawful basis for sharing metadata.
- **Security governance**: Review access logs and enforce internal data protection policies.

Hyperscaler's and SAP BTP's responsibility:

The hyperscaler security plays an important role in meeting security requirements to store and process customer data in a hyperscaler environment.

As SAP Cloud ALM is deployed on SAP BTP, it follows the SAP BTP security as the basis, by using standard SAP BTP services and the deployment environment.

More under:

- Hyperscalers: Securing SAP Environments
- My Trust Center – SAP subprocessors: Choose *Title* end enter "SAP Cloud ALM" to find the data transfer factsheet and the 3rd-party subprocessors.
- SAP Trust Center: Protecting your cloud solutions and data

Product security

SAP Cloud ALM follows the principles of security measures in the cloud, as laid out in SAP Trust Center: Protecting your cloud solutions and data.

Security is embedded in every phase of the product lifecycle following the secure development and operation lifecycle practices.

Secure by design

- SAP Cloud ALM is compliant with SAP-internal technical policies, procedures, directives, guidelines, and product standards.
- SAP Cloud ALM applies a proactive approach to design and implement security aspects. The Least privilege, défense in depth, fail securely, minimize attack surface, secure UI, secure API calls, transparency with logs authorization concept, usage on open-source component with no licensing risk etc.
- Network security: SAP Cloud ALM uses Network and Communication Security from SAP BTP as foundation and hence SAP BTP Security can be followed.

More information about SAP's security processes is available in the document The Security Software Development Lifecycle at SAP.

IT operations and service

Regulated companies are required to maintain and operate SaaS systems, such as SAP Cloud ALM, in a demonstrable state of control. SAP Cloud ALM has comprehensive procedures for maintaining control of its system throughout its operational life.

The standard operating procedures (SOP) are:

- Operational change management
- Monitoring management
- Backup and restore
- Provisioning and de-provisioning
- Hotfix release process
- Incident management (SAP Global)

Incident management

An operation incident is any unplanned occurrence that prevents (or may prevent) or delays users, the system, an operation, or service from proceeding with an assigned task.

The incident management procedure categorizes incidents to direct them to the most appropriate resource or complementary process to achieve a timely resolution. Depending on the necessity, such fixes can lead to a hotfix.

SAP Cloud ALM follows SAP's global standards on incident management. The support team is responsible for customer support. It includes customer and internal ticket processing, service request completion, troubleshooting of service availability, and service degradation.

For incident management, SAP Cloud ALM follows the following process steps:

1. Log an incident
2. Categorize an incident
3. Investigate and diagnose
4. Resolve and recover
5. Validate and close

The support policy for SAP Cloud Services outlines how to report and log an incident and defines the customer response levels, including priority, definitions, initial response times, ongoing communication objectives, and resolution target.

An emergency plan for sudden security incidents is in place. SAP Cloud ALM has set up support components and integration with first level support, engineering teams, and operations teams.

Security incidents are handled according to the security incident management process. This process foresees classification, containment, and resolution of the issue. Internal groups and decision-makers are pulled in as needed.

Operational change management

SAP Cloud ALM follows an operational change management process with the following process steps:

1. SAP maintains an inventory of application lifecycle management tools and services, listing the relevant software components with all necessary attributes.
2. SAP monitors upcoming feature releases for each component.
3. SAP implements new features for components according to release cycles, following the SDOL.

The following are in the scope of operational change management:

- Feature releases (regular product increments)
- Corrections to the infrastructure and platform components, systems, and services, including upgrades of the platform, infrastructure components, database, runtime environment, and operating system

Changes to the SAP Cloud ALM solution are not in the scope of this process. The development of SAP Cloud ALM features follows the release process in the scope of SDOL.

SAP Cloud ALM also has procedures in place for:

- Operational changes of SAP HANA Cloud
- New data center setup

Monitoring and alerting management

The monitoring and alerting management process deals with the monitoring, alerting, and reporting of the availability of SAP Cloud ALM, as well as handling of availability incidents. The objective of monitoring and alerting management is to enable the delivery of consistent and timely service to customers.

The Service Level Agreement (SLA) for SAP Cloud Services outlines the system availability SLA and the calculation and definition of the system availability percentage. SAP conducts monitoring and alerting for SAP Cloud ALM using the SAP BTP availability service and SAP Focused Run to monitor, analyze, alert, and report on the availability of services.

Customers can find the monitoring availability reporting on the SAP Trust Center, Cloud Availability Center section. This reporting is data-center specific and is open to everyone. The Cloud Availability Center shows the availability of products and services. It provides details on the time of the incident, the status of availability, and root-cause analysis.

- 24hx7 operations

- Monitoring of all SAP Cloud ALM components in all data centers
- Alerting procedures
- Integration into SAP Cloud Availability Center and SAP Trust Center

No SLAs are published. Refer to the following documents:

Service Level Agreements for Cloud Services

Support Policy for SAP Cloud Services

General Terms and Conditions for SAP Cloud Services

Data backup and restore

The purpose of backup and restore is to ensure the accurate and reproducible copying of digital assets (data and software), protection against loss of original data, and the restoration of assets when required.

Backup and restore are in place for SAP Cloud ALM persistence platform services: SAP HANA Cloud (SAP HANA DBservices), a database-as-a-service offering (DBaaS) managed by SAP BTP, is the data storage for tenant-specific relational business data. SAP BTP also manages backups.

SAP HANA databases are regularly backed up. Read more under Backup and Recovery (SAP HANA Cloud) and Resilience, High Availability, and Disaster Recovery (SAP BTP).
Backups take place in the same region where the customer's SAP Cloud ALM tenant is provided.

Tenant-specific recovery:

Tenant-specific data recovery, also known as tenant restore, is a process that allows for the restoration of data on a per-tenant basis. It enables customers to request the restoration of their individual tenant to a previous point in time.

For the time being, tenant-specific data recovery is not available for SAP Cloud ALM.

Provisioning and deprovisioning

The objective of the customer provisioning process is to ensure the proper and secure setup of the customer tenant.

SAP Cloud ALM can be quickly implemented via nearly fully-automated provisioning, as described in Requesting SAP Cloud ALM.

When a customer's SAP contracts expires, their SAP Cloud ALM tenant and all related data will be terminated after a grace period has passed. Read more under Account Termination.

Hotfixes

Hotfixes deliver a solution via code change for an urgent problem of a customer or a fix for a high-priority vulnerability. The hotfix release process aims to ensure the proper development, testing, and release of a hotfix or a hotfix collection.

SAP conducts an RCA and impact analysis to implement a hotfix. It is QA-tested, and SAP internal approver must review the hotfix, analyze RCA and impact, and test results to approve the deployment.

SAP Cloud ALM releases hotfixes in the daily deployment to production.

Personnel and contractor training

Security education and awareness: SAP employees that are involved in SAP Cloud ALM are regularly trained on the importance of security. Software developers are trained for secure programming.

SAP uses an internal learning management system (LMS) to manage critical course content and training traceability. This LMS includes a dashboard and reporting capabilities for managers to see overall training completion.

Glossary

Abbreviation	Definition
ALM	Application lifecycle management
BTP	Business technology platform
CAP	Cloud application Programming
CBDT	Cross-Border Data Transfer
CX	Customer experience
DPP	Data protection and privacy
EEA	European Economic Area
EU	European Union
FOSS	Free and open-source software
GCP	Good clinical practice
GDPR	General data protection regulation
GLP	Good laboratory practice
GMP	Good Manufacturing Practice
GxP	Good practices for x, such as C (clinical), D (distribution), Doc (documentation), L (laboratory), M (manufacturing), etc.
HDI	HANA deployment infrastructure
HXM	Human experience management
ISBN	SAP Intelligent Spend and Business Network
ISMS	Information security management System
ISO	International Organization for Standardization
LMS	Learning management System
PIPL	Personal Information protection Law (China)
QA	Quality assurance
QMS	Quality management system
RCA	Root cause analysis
RDM	Release decision meeting
SaaS	Software as a service
SAP HANA DB	SAP HANA Database
SAST	Static application security testing
SDOL	Secure software development and operations lifecycle
SLA	Service level agreement
SOP	Standard operating procedure

Version History

Ensure you have the latest version of this document downloaded from SAP Help Portal product page for SAP Cloud ALM.

Time of update	Changes
Dec 2024	First version published.
Jan 2026	Updated illustrations.
Mar 2026	Update of the section *Managing integration between SAP Cloud ALM and the managed systems/services* and of the section *Compliance and security*, incl. subsections.