Cloud Services: A Framework for Adoption in the Regulated Life Sciences Industry

phuse.global

Contents

This document has been developed by the PHUSE Cloud Adoption in the Life Sciences Working Group Project and is subject to ongoing consultation and feedback from relevant stakeholders.

You may submit comments and suggestions regarding this document to anders.vidstrup@regionh.dk.

Revision History

Version	Date	Summary
1.0	17 August 2025	First version

1 Scope

When adopting cloud-based solutions for GxP workloads, it is important to understand the essential characteristics of cloud services and solutions for determining the applicability of GxP requirements to specific cloud service providers and/or cloud-based solution models.

This document provides guidance in preparing and conducting an exit strategy when working with cloud service providers.

This is one of four supplements to the Cloud Services – Pre-Amble ref [5], which together form the PHUSE Framework for Adoption of Cloud Services in the Regulated Life Sciences Industry.

2 Exit Strategy When Working with Cloud Service Providers

Looking at good engineering practices, cloud service customers, as a part of the purchasing process, must have an exit strategy in place to be able to exit the cloud service provider if needed. There are several reasons why companies should have an exit strategy when working with a cloud service provider:

1. Data Security and Integrity:
   - **Data Retrieval:** Ensuring you have a clear plan for retrieving your data from the cloud provider, in a usable format, prevents data loss and maintains data integrity.
   - **Data Deletion:** Your data must be securely deleted from the provider's servers to prevent unauthorised access post-exit.

2. Business Continuity:
   - **Minimise Downtime:** A well-planned exit strategy minimises service disruption and downtime.
   - **Backup Solutions:** Identifying backup solutions and alternative providers in advance ensures your business continues to function if the current provider experiences outages or other issues.

3. Compliance and Legal Requirements:
   - **Regulatory Compliance:** Depending on your industry, there may be legal and regulatory requirements regarding data storage, handling and retrieval that need to be adhered to during the transition.
   - **Contractual Obligations:** To avoid legal complications, it is essential you understand and comply with the terms and conditions of your contract with the cloud provider.

4. Vendor Lock-In Prevention:
   - **Avoid Dependency:** An exit strategy prevents over-reliance on a single vendor, giving you flexibility and negotiating power.
   - **Multi-Cloud Strategy:** Adopting a multi-cloud or hybrid-cloud strategy diversifies risks and avoids you being locked into a single provider's ecosystem.

5. Risk Management:
   - **Mitigate Risks:** Identifying potential risks associated with vendor dependency and having a plan to mitigate these risks protects your business.
   - **Disaster Recovery:** Incorporating exit strategies into broader disaster recovery and business continuity plans ensures readiness for unforeseen circumstances.

6. Performance and Satisfaction:
   - **Regular Evaluation:** An exit strategy encourages regular performance reviews of the cloud provider against your business needs and expectations.
   - **Alternative Solutions:** Stay informed about providers and solutions with better performance, features or costs, so you don't settle for subpar service.

7. Scalability and Flexibility:
   - **Future Growth:** Ensure your cloud strategy is scalable and can adapt to growth or changes in business direction.
   - **Flexibility in Operations:** Having an exit strategy allows for agile shifts in technology or operational strategies without the constraints of a single cloud provider.

Having a well-defined exit strategy ensures your business remains resilient, compliant and competitive, regardless of changes in the cloud service landscape. It provides a safety net that manages risks and optimises your cloud usage.

Both planned and 'unplanned' exits will benefit from the above.

Planned exit or 'migration' – This is more typical. As part of normal business/IT operations, executing against the annual regular IT planning technology strategy, which includes technology life cycle management (TLM), system and/or application upgrades must happen. This might include adopting more external public cloud IaaS/PaaS from traditional in-house, multi-vendor/cloud strategies, or adopting best-in-class SaaS providers. In most cases, robust, compliant practices associated with computer systems validation, combined with the elements described in this cloud services framework will apply. Fundamentals associated with platforms and data migration should be followed.

Unplanned exit – This is where the challenge lies, because, in most cases, you are given less time to respond. What if your software or SaaS vendor goes out of business, or is acquired, and there is a significant change or a discontinuation of the product offering? What if your own company is divesting a portion of the business, and current shared platforms/services need to be split, with operations maintained?

Estimate the costs associated with existing as a cloud service provider, considering data migration, infrastructure setup and potential downtime.

2.1 Authority and Standardisation Organisation Requirements for Exit Strategies

Authorities and standardisation organisations do have input into exit strategies when working with cloud service providers. In the table below quotes from regulations is listed.

OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, Advisory Document on GLP & Cloud Computing ref [3]	
5.1. Responsibilities of the test facility	The archivist is responsible for the management of archives. If GLP archives are stored in a cloud-based solution, the archivist may need to use the assistance of specialists to look at technical aspects. Nevertheless, the archivist remains responsible and should still ensure that: ... 6. A process is implemented to ensure the readability of data after being migrated from the cloud environment to the test facility (exit strategy).
5.3.1. Risk assessment and selection of the cloud-based services	Risk management should be applied throughout the lifecycle of any computerised system, taking into account data quality, data integrity and data availability. ... A detailed description of the expectations to the use of the cloud solution and the associated impacts should be available before any choice is made. The steps of the risk assessment include (but are not limited to): ... 3. Impact on GLP compliance, especially regarding data migration and storage, resulting from adopting the system provided by the cloud service (non-exhaustive list): ... c. Associated new risk on data integrity and data availability: level of control of remote access to the data, level of protection of the data, secure location for the physical storage of the data (physical infrastructure access, disaster recovery strategy, recovery time objectives and recovery point objectives, location of the data hosting servers, long term integrity of electronically archived data). For SaaS, as the test facility has generally no access to the software itself in case of release event, impacts on data integrity and data availability should be carefully considered by end user when anticipating the business continuity plan, the disaster recovery plan and the exit strategy of the GLP test facility.
5.3.2. Cloud service provider assessment	Following general items may be addressed during the assessment (non-exhaustive list): ... 12. Exit strategy ...
5.3.3. Service Level Agreement (SLA)	Exit strategy The SLA should clearly describe the test facility's right to obtain all data and meta-data (including audit trails) in a readable and convertible format, in case the contract with the cloud service provider is terminated (see also OECD document No. 22 chapter 6).
Eudralex proposal for update of Annex 11 [7]	
7.5 Contracts	viii. Defines an exit strategy by which the regulated user may retain control of system data
ISO27002-2022 ref [2]	
5.23 Information security for use of cloud services	*Control* Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements. *Purpose* To specify and manage information security for the use of cloud services. *Guidance* The organization should establish and communicate topic-specific policy on the use of cloud services to all relevant interested parties. The organization should define: ... j) how to change or stop the use of cloud services including exit strategies for cloud services.

3 Clarification on Definitions

Some sources say that an exit strategy should be in place. A clear definition isn't clearly defined. In this document, a working definition has been established with the following sources as input:

Source	Definition
Cambridge Dictionary (online) [4]	Exit strategy A plan of how someone will end something such as a business deal or a military operation.
KPMG [6]	A cloud exit strategy, commonly referred to as a reverse migration, is the process of developing a plan to ensure a business can effectively switch from one cloud provider to another without a larger disruption. This should be the focus area for all businesses who want to migrate to cloud. Ideally, they need to explore and document the challenges and roadblocks before moving to cloud. This may also be the case even if your companies never return to on-premises infrastructure (cloud repatriation). An exit strategy can help you through talks with service providers and have an impact on your design (current and future state).

4 Elements in Exit Strategy

4.1 Data Security and Integrity

Data security and data integrity are two foundational concepts in information security and data management, each focusing on different aspects of protecting and maintaining data.

4.1.1 Data Security

Data security refers to the protection of data from unauthorised access, misuse, corruption, or theft throughout its life cycle. It encompasses the processes, technologies and practices designed to safeguard data from malicious attacks, loss or compromise.

Key aspects of data security need to be covered in an exit strategy:

- Confidentiality: Ensure sensitive information is accessible only to those with authorised access. This often involves encryption, access control mechanisms, and data masking.
- Integrity: Protect data from being altered or tampered with by unauthorised users. This is achieved through checksums, hash functions, digital signatures and access controls.
- Availability: Ensure data is available to authorised users when needed, which involves backups, failover systems, and reliable access.
- Authentication and Authorisation: Verify the identity of users accessing the system and ensure they have appropriate permissions.
- Data Encryption: Encrypt data both at rest (stored data) and in transit (data being transferred over networks) to prevent unauthorised access.
- Data Loss Prevention (DLP): Implement measures to prevent internal and external data breaches, leaks and loss.

4.1.2 Data Integrity

Data integrity refers to the accuracy, consistency and reliability of data throughout its life cycle. It ensures data remains unchanged from its source and is protected against unauthorised modification.

Key aspects of data integrity include being covered in an exit strategy:

- Accuracy: Data must be accurate and free from errors. This means that the data reflects real-world scenarios or transactions correctly.
- Consistency: Data should remain consistent across different databases and systems. If a value is updated in one location, it should be updated everywhere.
- Validity: Data must conform to predefined rules and formats, such as data type and range checks.
- Completeness: All required data must be present. Missing or incomplete data can lead to erroneous conclusions or decisions.
- Data Validation and Verification: Regular checks should be performed to ensure data has not been altered or corrupted. Techniques such as checksums, hashes and digital signatures can be used to verify data integrity.
- Audit Trails and Logs: Maintaining logs of all data changes, including who made the change, when it was made, and what the change was, to trace any potential integrity issues. This should include periodic reviews of audit trails and logs for unusual or potentially malicious activity.

Data security is about protecting data from unauthorised access, breaches, and theft, focusing on confidentiality, integrity and availability.

Data integrity is about maintaining the accuracy, consistency and reliability of data over its life cycle, ensuring it remains unaltered and trustworthy.

Together, data security and integrity ensure data is both protected and reliable, making them critical components in any data management and information security strategy, as well as exit strategy.

4.2 Business Continuity

Business continuity is simply defined as a company's plan to restore the most critical functions in the event of a disaster to keep the business functioning. There may be systems that are included in the BCP (Business Continuity Plan) with their own Disaster Recovery (DR) process defined. If your company has such plans in place, it may provide a reference to assist in developing an exit strategy for a platform. Yes, the BCP usually restores operations using the same applications etc., where the exit strategy is moving to a different provider, but there are many common elements to address.

4.3 Vendor Lock-In Prevention

Vendor lock-in prevention refers to strategies and practices that organisations implement to avoid becoming overly dependent on a single cloud service provider (CSP). The goal is to ensure flexibility, portability and ease of migration between cloud platforms or to an on-premises environment without incurring excessive cost, complexity or disruption. This is sometimes referred to as a 'cloud-agnostic' strategy. Although no solution is necessarily 100% agnostic, proper planning and execution may

allow it to be achieved with minimal differences between the two solutions.

4.3.1 What Is Vendor Lock-In?

Vendor lock-in occurs when a customer becomes dependent on a single CSP's technology, services, tools or APIs because switching to another provider would be difficult, costly or impractical. This can result in limited flexibility, increased costs and potential challenges in adapting to changes in business needs or technological advancements.

4.3.2 Key Strategies for Vendor Lock-In Prevention

- Adopt a Multi-Cloud Strategy
  - Use multiple cloud providers to distribute workloads, data storage and applications across environments. This strategy avoids reliance on a single provider and offers the flexibility to switch or move services as needed.
  - Ensure applications are designed to work across cloud platforms by using common standards and technologies.

- Use Open Standards and Interoperable Technologies
  - Use open standards (e.g. Kubernetes, Docker, OpenStack) and interoperable technologies that are supported by multiple cloud providers. This reduces dependency on proprietary services and facilitates portability.
  - Leverage APIs, databases and services that follow widely adopted standards to enable seamless integration and migration.
  - Remember, many of these technologies (particularly the tools) may be open-sourced. If working in a regulated environment, be sure to implement controls on the versions of software used.

- Implement Infrastructure as Code (IaC) with Agnostic Tools
  - Use IaC tools that support multiple cloud environments, such as Terraform, Ansible or Pulumi. These tools allow you to define and manage infrastructure in a provider-agnostic way, making it easier to migrate or replicate environments across clouds.

- Design for Cloud Portability
  - Develop applications with a cloud-agnostic architecture, avoiding deep integration with cloud-specific services and APIs that are difficult to migrate.
  - Consider using containerisation and microservices, which make it easier to move applications between cloud providers or environments.

- Use Data and Application Abstraction Layers
  - Implement abstraction layers that separate applications and data from the underlying cloud infrastructure. This can involve using middleware, APIs or orchestration tools that facilitate interoperability and reduce dependence on specific cloud services.
  - Ensure data is stored in formats that are easily exportable and not tied to a specific cloud provider's proprietary formats or systems.

- Regularly Review Contracts and SLAs
  - Negotiate favourable terms with cloud providers that minimise exit costs and provide clarity on data migration support, data deletion guarantees, and compliance.
  - Review contracts and SLAs to ensure they do not have restrictive clauses that could hinder migration or incur significant penalties for early termination.

- Ensure Data Portability
  - Implement data portability practices by storing data in portable, standardised formats (e.g. CSV, JSON, Parquet) that can be easily transferred between cloud environments.
  - Regularly perform data export tests to verify that data can be extracted and imported without significant loss, corruption or downtime.

- Avoid Proprietary Tools and Services
  - Minimise reliance on cloud-specific tools, services and APIs that are not available or supported by other providers. Instead, use open-source or third-party solutions that work across platforms.
  - Where possible, leverage cloud-native services that offer compatibility with multiple cloud providers or have open-source alternatives.

- Plan for Exit and Migration from the Start
  - Develop a cloud exit strategy as part of the initial cloud adoption plan. This strategy should outline the processes, tools and resources needed to migrate workloads, data and applications to another cloud provider or back to an on-premises environment.
  - Conduct regular testing of the exit strategy to identify potential challenges and refine the process. (It should be noted that this sounds similar to backup/restore procedures.) Regulated companies should verify these procedures periodically to ensure incremental functionality, software upgrades, etc. have not introduced a fault into this process. The exit strategy should be viewed similarly.

- Consider Cloud Management Platforms (CMPs)
  - Use cloud management platforms that provide a single pane of glass to manage multiple cloud environments, offering automation, monitoring, governance and orchestration capabilities across CSPs.

4.3.3 Benefits of Vendor Lock-In Prevention

Flexibility and Agility: Organisations can adapt more easily to changing business needs, technological advances or cost considerations.

Cost Management: Avoiding dependency on a single provider can help organisations negotiate better pricing and avoid excessive costs associated with lock-in.

Reduced Risk: Mitigate risks associated with service outages, changes in vendor policies, security vulnerabilities, or compliance issues with a single cloud provider.

Improved Negotiation Leverage: Being able to switch providers gives organisations leverage to negotiate better terms and SLAs.

By implementing these strategies, organisations can stay flexible, optimise costs, and reduce the risks associated with vendor lock-in in cloud environments.

4.4 Risk Management

Risk management is a crucial component of an exit strategy for cloud solutions for organisations to transition from one provider to another without jeopardising data security, business continuity, compliance or operational efficiency. A well-defined risk management framework helps organisations identify, assess, mitigate and monitor risks associated with cloud service exit strategies.

4.4.1 Identifying Risks in Cloud Exit Strategies

Risk Area	Potential Hazard
Data Loss or Corruption	When transitioning away from a cloud provider, there is a risk of losing critical business data or experiencing data corruption. Incomplete or improperly formatted data migration can lead to discrepancies in business records.
Security Breaches and Data Leakage	Transferring sensitive data between providers increases exposure to cyber threats. Insufficient encryption or inadequate access control can result in unauthorised access to data during migration.
Business Disruption and Downtime	An unplanned or poorly managed exit can lead to significant downtime, affecting business operations and customer experience. Dependency on cloud-native services may complicate migration and cause delays.
Vendor Dependency and Lock-In Risks	Proprietary software, APIs, or data formats may prevent seamless migration. Limited interoperability between cloud providers can hinder smooth transitions.
Regulatory and Compliance Issues	Data sovereignty laws and industry-specific compliance regulations may restrict data transfer to certain locations or providers. Inadequate recordkeeping and lack of audit trails can lead to non-compliance risks.

Historical data and associated reports. Reports used to make quality decisions are expected to be maintained and run against the historical data. If exiting, this must be preserved.

4.4.2 Risk Mitigation Strategies

Mitigation Area	Examples
Develop a Comprehensive Exit Plan	Define a step-by-step exit process that includes risk assessments, data migration strategies, and contingency planning. Establish a clear timeline and resource allocation to ensure a smooth transition.
Perform Data Backups and Integrity Checks	Maintain redundant copies of critical data before initiating migration. Conduct integrity verification tests to ensure data consistency and completeness post-migration.
Implement Security Best Practices	Use encryption protocols for data in transit and at rest. Establish strict access controls to prevent unauthorised access.
Plan for Business Continuity	Maintain alternative service providers or hybrid cloud options to minimise disruptions. Conduct failover and disaster recovery tests regularly.
Ensure Compliance Readiness	Collaborate with legal and compliance teams to adhere to industry regulations. Document all actions taken during the exit process for audit purposes.

4.4.3 Ongoing Risk Monitoring and Review

Continuous monitoring of cloud service providers and periodic risk assessments help organisations adapt their exit strategies in response to evolving risks and technological advancements.

4.5 Performance and Satisfaction

Performance and satisfaction play a critical role in determining when an organisation should consider exiting a cloud service provider. Ensuring cloud services meet business needs, user expectations and regulatory requirements is fundamental to maintaining operational efficiency. Consider key metrics as part of any supplier management programme.

4.5.1 Key Performance Indicators (KPIs) for Cloud Services

KPI Area	Examples
System Availability and Uptime	Measured through service-level agreements (SLAs). Frequent outages may indicate the need for an exit strategy.
Data Processing Speed and Latency	Evaluate the provider's ability to handle workloads efficiently. Performance bottlenecks can impact on business-critical applications.
Scalability and Resource Allocation	Assess whether the cloud infrastructure can scale as needed. Delays in provisioning resources may hinder business growth.
Cost–Performance Ratio	Compare costs against the quality of services received. Unexpected cost surges due to inefficient resource management signal the need for reassessment.

4.5.2 User Satisfaction Metrics

Satisfaction Area	Examples
Customer Support Responsiveness/SLA	Measure the provider's ability to resolve issues promptly. Slow response times can affect business operations.
Ease of Use and Management	Evaluate the complexity of managing cloud resources. Complicated interfaces and lack of automation can impact on productivity.
Feedback from Internal Stakeholders	Conduct periodic satisfaction surveys among employees using cloud services. Gather insights into usability, integration challenges and overall experience.

4.5.3 Evaluating the Need for a Cloud Exit

If performance consistently falls below expectations and corrective measures fail, organisations should consider migrating to a more suitable cloud provider that meets their operational and business objectives.

4.6 Scalability and Flexibility

Scalability and flexibility are essential in cloud computing to ensure organisations efficiently adapt to changing business demands, growth, and technological advancements.

4.6.1 Importance of Scalability in Cloud Services

- Handling Increasing Workloads
  - Organisations must assess whether the cloud provider supports seamless scalability.
  - Performance degradation during peak usage periods signals potential constraints.
- Elastic Resource Allocation
  - The ability to scale up or down based on demand optimises cost-efficiency.
  - Providers with rigid resource allocation policies may hinder business agility.
- Global Expansion Support
  - Businesses expanding internationally need providers with a global data centre presence.
  - Regional restrictions may impact on performance and compliance.

4.6.2 Flexibility Considerations

- Interoperability Across Multiple Platforms
  - The ability to integrate with existing on-premises infrastructure or hybrid cloud environments.
  - Compatibility with different cloud vendors prevents vendor lock-in.
- Customisation and Adaptability
  - Flexible cloud solutions allow businesses to tailor services to their needs.
  - Providers with rigid configurations may not accommodate future requirements.
- Support for Emerging Technologies
  - Evaluate the provider's ability to support AI, IoT, and blockchain applications.
  - Lack of innovation may hinder long-term growth.

4.6.3 Strategies for Ensuring Scalability and Flexibility

- Implement a Multi-Cloud or Hybrid Strategy
  - Distribute workloads across multiple providers to ensure redundancy and adaptability.
  - Avoid reliance on a single provider's infrastructure.
- Leverage Containerisation and Microservices
  - Using Kubernetes and Docker ensures application portability.
  - Reduces dependency on proprietary cloud services.
- Monitor Usage Patterns and Scale Proactively
  - Analyse resource use trends to anticipate scaling needs.
  - Automate scaling policies to optimise performance and cost.

4.6.4 Exit Considerations for Scalability and Flexibility

If a provider cannot accommodate growing business needs or lacks the flexibility to support evolving technologies, organisations should evaluate alternative cloud solutions that better align with their long-term strategies.

Scalability and flexibility in cloud services are vital for long-term business success. Organisations must continuously assess whether their cloud provider can meet current and future needs and have a well-defined exit strategy in place to pivot when necessary.

5 Cloud Escrow Service

Prior to the cloud, an escrow service would keep a copy of vendor-released software in the event of the vendor no longer being available to support their software. With the advent of the cloud and then DevOps, this became challenging due to cloud providers updating services daily. Today, there are many cloud escrow providers showing solutions to incorporate into an exit strategy.

6 Glossary

See Glossary in PHUSE, Cloud Services: A Framework for Adoption in the Regulated Life Sciences Industry, Pre Amble, Edition 5, November 2023.

7 References

[1] Cloud Security Alliance, Cloud Controls Matrix.
[2] ISO 27002:2022. Information security, cybersecurity and privacy protection – Information security controls.
[3] OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING. Advisory Document on GLP & Cloud Computing, June 2023.
[4] https://dictionary.cambridge.org/dictionary/english/exit-strategy
[5] PHUSE. Cloud Services – A Framework for Adoption in the Regulated Life Sciences Industry, Pre Amble, Edition 5, November 2023.
[6] Article on kpmg.com "Why a cloud exit strategy is essential to enable the future", 2024
[7] Eudralex. Proposal for updated Annex 11, 7 July 2025.