*{17-AUGUST-2025}*

*Cloud Services,*

*A Framework for Adoption in the Regulated Life Sciences Industry*

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Summary** |
| 0.1 | 17-08-2025 | First version |

This document has been developed by the PHUSE Project on Cloud Adoption and is subject to ongoing consultation and feedback from all relevant stakeholders.

You may submit comments and suggestions regarding this document to [anders.vidstrup@regionh.dk](mailto:anders.vidstrup@regionh.dk)

Contents

[1 Scope 3](#_Toc206345370)

[2 Exit Strategy in relation to working with Cloud Service Providers 3](#_Toc206345371)

[2.1 Authorities and Standardization Organisations Requirements for Exit Strategy’s 5](#_Toc206345372)

[3 Clarification on definitions 7](#_Toc206345373)

[4 Elements in Exit Strategy 7](#_Toc206345374)

[4.1 Data Security and Integrity 7](#_Toc206345375)

[4.1.1 Data Security 7](#_Toc206345376)

[4.1.2 Data Integrity 8](#_Toc206345377)

[4.2 Business Continuity 8](#_Toc206345378)

[4.3 Vendor Lock-In Prevention 8](#_Toc206345379)

[4.3.1 What is Vendor Lock-In? 9](#_Toc206345380)

[4.3.2 Key Strategies for Vendor Lock-In Prevention 9](#_Toc206345381)

[4.3.3 Benefits of Vendor Lock-In Prevention 10](#_Toc206345382)

[4.4 Risk Management 11](#_Toc206345383)

[4.4.1 Identifying Risks in Cloud Exit Strategies 11](#_Toc206345384)

[4.4.2 Risk Mitigation Strategies 12](#_Toc206345385)

[4.4.3 Ongoing Risk Monitoring and Review 12](#_Toc206345386)

[4.5 Performance and Satisfaction 12](#_Toc206345387)

[4.5.1 Key Performance Indicators (KPIs) for Cloud Services 13](#_Toc206345388)

[4.5.2 User Satisfaction Metrics 13](#_Toc206345389)

[4.5.3 Evaluating the Need for a Cloud Exit 13](#_Toc206345390)

[4.6 Scalability and Flexibility 14](#_Toc206345391)

[4.6.1 Importance of Scalability in Cloud Services 14](#_Toc206345392)

[4.6.2 Flexibility Considerations 14](#_Toc206345393)

[4.6.3 Strategies for Ensuring Scalability and Flexibility 14](#_Toc206345394)

[4.6.4 Exit Considerations for Scalability and Flexibility 14](#_Toc206345395)

[5 Cloud Escrow Service 15](#_Toc206345396)

[6 Glossary 15](#_Toc206345397)

[7 References 15](#_Toc206345398)

# Scope

In adopting cloud-based solutions for GxP workloads, understanding the essential characteristics of cloud services and solutions is important 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 in relation to working with Cloud Service Providers..*

*It is one of four supplements to the “Cloud Services – Pre-Amble” ref [5] which all together form the*

*“Framework for Adoption of Cloud Services in the Regulated Life Science Industry” from PHUSE.*

# Exit Strategy in relation to working with Cloud Service Providers

Looking at good engineering practices, the Cloud Service Customer as a part of purchasing process must ensure that an Exit Strategy is in place to make sure that they have the ability to exit the Cloud Service Provider if needed.

Having an exit strategy when engaging with a cloud service provider is crucial for a company for several reasons:

1. Data Security and Integrity:
   * **Data Retrieval**: Ensuring you have a clear plan for retrieving all your data from the cloud provider, in a usable format, helps prevent data loss and maintains data integrity.
   * **Data Deletion**: You need to ensure that your data is securely and completely deleted from the provider's servers to prevent unauthorized access post-exit.
2. Business Continuity:
   * **Minimize Downtime**: A well-planned exit strategy helps minimize service disruption and downtime, ensuring business operations continue smoothly.
   * **Backup Solutions**: Having backup solutions and alternate providers identified in advance ensures that your business can continue 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**: Understanding and complying with the terms and conditions of your contract with the cloud provider is essential to avoid legal complications.
4. Vendor Lock-In Prevention:
   * **Avoid Dependency**: An exit strategy helps prevent over-reliance on a single vendor, giving you flexibility and negotiating power.
   * **Multi-Cloud Strategy**: Encourages the adoption of a multi-cloud or hybrid-cloud strategy to diversify risks and avoid being locked into one 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**: Keeps you informed about other providers and solutions that may offer better performance, features, or costs, ensuring you are not settling for subpar service.
7. Scalability and Flexibility:
   * **Future Growth**: Ensures that your cloud strategy is scalable and can adapt to future growth or changes in business direction.
   * **Flexibility in Operations**: Allows for agile shifts in technology or operational strategies without being constrained by the limitations of a single cloud provider.

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

Both planned and “unplanned” exits will benefit from above.

Planned Exit or “Migration” - This is more typical. As part of normal business/IT operations, executing against a strategy, Technology Lifecycle Management (TLM), upgrades of systems and/or applications must happen. This may include adopting more external public cloud IaaS/PaaS from traditional in-house, multi-vendor/cloud strategy, or potentially adopting best-in-class SaaS providers are some examples. In most cases, robust, compliant practices associated with Computer Systems Validation combined with the elements described previously 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 as in most cases, one is given a much shorter amount of time to respond. What if your software or SaaS vendor is going out of business, or perhaps being acquired, with a significant change or discontinuance 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 a cloud service provider considering data migration, infrastructure set up and potential downtime.

## Authorities and Standardization Organisations Requirements for Exit Strategy’s

Different authorities and standardization Organisation do have input for an exit strategy in relation to working with cloud service providers

|  |  |
| --- | --- |
| 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. |

# 

# Clarification on definitions

Some sources describes 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 following sources as input:

| Source | Definition |
| --- | --- |
| Cambridge online dictionary [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 that a business can effectively switch from one cloud provider to another without a larger disruption. This should be the focus area for all the businesses who want to migrate to cloud.  Ideally, they need to explore, document the challenges and roadblocks beforehand (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). |

# Elements in Exit Strategy

## 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.

### Data Security

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

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

* Confidentiality: Ensuring that sensitive information is accessible only to those authorized to have access. This often involves encryption, access control mechanisms, and data masking.
* Integrity: Protecting data from being altered or tampered with by unauthorized users. This is achieved through checksums, hash functions, digital signatures, and access controls.
* Availability: Ensuring that data is available to authorized users when needed, which involves backups, failover systems, and ensuring reliable access.
* Authentication and Authorization: Verifying the identity of users accessing the system and ensuring they have appropriate permissions.
* Data Encryption: Encrypting data both at rest (stored data) and in transit (data being transferred over networks) to prevent unauthorized access.
* Data Loss Prevention (DLP): Implementing measures to prevent data breaches, leaks, and loss, both internally and externally.

### Data Integrity

Data Integrity refers to the accuracy, consistency, and reliability of data throughout its lifecycle. It ensures that data remains unchanged from its source and is protected against unauthorized modification.

Key aspects of data integrity include to be 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 unauthorized access, breaches, and theft, focusing on confidentiality, integrity, and availability.

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

Together, data security and integrity ensure that data is both protected and reliable, making them critical components in any data management and information security strategy also during an exit strategy.

## Business Continuity

Business Continuity is simply defined as a company’s plan to restore the most critical functions as part of a disaster to keep the business functioning. There may be a number of systems that are included in the BCP (Business Continuity Plan), each system having 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 is usually restoring operations using the same applications, etc. where the exit strategy is moving to a different provider, but many elements to address are common.

## Vendor Lock-In Prevention

Vendor lock-in prevention refers to strategies and practices that organizations 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 different cloud platforms or back to an on-premises environment without incurring excessive costs, complexity, or disruptions. This may sometimes be referred to as a “Cloud Agnostic” strategy. Although no solution would necessarily be 100% agnostic, the proper planning and execution may allow it be achieved with minimal differences between the two solutions.

### What is Vendor Lock-In?

Vendor Lock-In occurs when a customer becomes dependent on a single CSP's technology, services, tools, or APIs to the extent that switching to another provider becomes 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.

### Key Strategies for Vendor Lock-In Prevention

* Adopt a Multi-Cloud Strategy
  + Use multiple cloud providers to distribute workloads, data storage, and applications across different environments. This strategy helps avoid reliance on a single provider and provides flexibility to switch or move services as needed.
  + Ensure applications are designed to work across different cloud platforms by using common standards and technologies.
* Utilize 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 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 different 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 containerization and microservices, which make it easier to move applications between different 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 favorable terms with cloud providers that minimize 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, standardized formats (e.g., CSV, JSON, Parquet) that can be easily transferred between different 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
  + Minimize 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 different 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 process, 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 be periodically verifying these procedures over time to ensure that 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 different CSPs.

### Benefits of Vendor Lock-In Prevention

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

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

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

Improved Negotiation Leverage: Having the ability to switch providers gives organizations leverage to negotiate better terms and SLAs.

By implementing these strategies, organizations can maintain flexibility, optimize costs, and reduce the risks associated with vendor lock-in in cloud environments.

## Risk Management

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

### 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 unauthorized 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.  Dependencies 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 record-keeping 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, have the ability to be run against the historical data. If exiting, this must also be preserved.**

### 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 unauthorized access. |
| Plan for Business Continuity | Maintain alternative service providers or hybrid cloud options to minimize 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. |

### Ongoing Risk Monitoring and Review

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

## Performance and Satisfaction

Performance and satisfaction play a critical role in determining when an organization should consider exiting a cloud service provider. Ensuring that 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 program.

### 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 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. |

### User Satisfaction Metrics

|  |  |
| --- | --- |
| Satisfaction areas | 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 productivity. |
| Feedback from Internal Stakeholders | Conduct periodic satisfaction surveys among employees using cloud services.  Gather insights on usability, integration challenges, and overall experience. |

### Evaluating the Need for a Cloud Exit

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

## Scalability and Flexibility

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

### Importance of Scalability in Cloud Services

* Handling Increasing Workloads
  + Organizations 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 optimizes cost efficiency.
  + Providers with rigid resource allocation policies may hinder business agility.
* Global Expansion Support
  + Businesses expanding internationally need providers with a global data center presence.
  + Regional restrictions may impact performance and compliance.

### 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.
* Customization 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.

### 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 Containerization and Microservices
  + Using Kubernetes and Docker ensures application portability.
  + Reduces dependency on proprietary cloud services.
* Monitor Usage Patterns and Scale Proactively
  + Analyze resource utilization trends to anticipate scaling needs.
  + Automate scaling policies to optimize performance and cost.

### Exit Considerations for Scalability and Flexibility

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

Ensuring scalability and flexibility in cloud services is vital for long-term business success. Organiza-tions 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.

# Cloud Escrow Service

Prior to cloud, software escrow was fairly simple. An escrow service would keep a copy of vendor released software in the event the vendor became no longer available to support their software. With the advent of Cloud, and then DevOps, this traditional method became challenging due to the reality of cloud providers updating services on a daily basis. Today, there are many Cloud Escrow providers that may provide solutions to incorporate into an Exit Strategy.

# Glossary

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

# References

1. Cloud Security Alliance, Cloud Controls Matrix
2. ISO27002-2022; 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. <https://kpmg.com/uk/en/blogs/home/posts/2023/04/why-a--cloud-exit-strategy--is-essential-to-enable-the-future.html>
7. Eudralex, proposal for updated Annex 11, July 7th 2025