4 JUNE 2020

Cloud exit strategy – testing of exit plans

TECHNICAL PAPER

CONTENTS

Chapters

ABBREVIATIONS

API	Application programming interface
BCM	Business continuity management
CaaS	Container as a service
CSC	Cloud Service Customer
CSP	Cloud Service Provider
GL	Guidelines
IaaS	Infrastructure as a service
NCA	National Competent Authority
OS	Operating System
PaaS	Platform as a service
Para	Paragraph
SaaS	Software as a service
SLA	Service Level Agreement
VSI	Virtual Server Infrastructure

1 Aim of this paper

The EBA Guidelines (GL)[1] on outsourcing arrangements require institutions to have a documented exit strategy when outsourcing critical or important functions which are in line with their outsourcing policy and business continuity[2]. Institutions have to take into account the possibility of unintentional or unplanned termination of services.

These will include:

- the termination of outsourcing arrangements;
- the failure of the service provider;
- the deterioration of the quality of the function provided and actual or potential business disruptions caused by the inappropriate or failed provision of the function;
- material risks arising for the appropriate and continuous application of the function.

To ensure institutions' availability to exit outsourcing arrangements, the EBA GL present steps to be taken under para. 107, among them a sufficiently tested exit plan.

The wording of EBA's GL allows for a level of proportionate considerations, especially a risk-based approach, in the context of exit strategy. The EBF Cloud Banking Forum supports this risk-based approach to outsourcing, though it believes that the approach to the supervisory requirements can benefit from a detailed understanding of the cloud environment with regard to financial institutions[3].

It should be taken into account that cloud computing offers a set of features that makes a major service failure less likely than in other IT paradigms: cloud services embody redundancy, high availability and resilience thanks to their distributed nature. In most cases, Cloud Service Providers (CSPs) can have stronger security than the level most individual companies can maintain and manage in a given situation, especially due

[1] EBA Guidelines on outsourcing arrangements (25 February 2019), https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements/38c80601-f5d7-4855-8ba3-702423665479.
[2] Ibid., Title IV. section 15, paragraph 106.
[3] EBF Cloud Banking Forum, Technical Paper "The use of Cloud Computing by Financial Institutions" (2019).

to the fact that cloud is (one of) the CSPs' core businesses and they are continuously investing in meeting the strictest and newest security standards. Nevertheless, an exit strategy is the ultimate risk mitigation for extreme service failures of the service provider – including the failure of the CSP itself – and, as already reflected, must be approached in a risk-based way. The withdrawal to consider can be partial or complete. Technical failures can be contributing factors to this extreme failure. However, an exit strategy is not intended as a tool to respond to technical shortcomings in a matter of hours or even days.

An exit strategy comprises different elements. Its centrepiece is the exit plan[4] that, depending upon various risk factors, may require further testing to increase confidence as discussed further on in this document.

Exit plan testing can take different forms, reflecting diverging needs for the cloud service in question. Their testing must be balanced against both positive and negative risk factors in order to avoid harming the benefits coming from the cloud outsourcing arrangement. Testing may carry high costs, disproportionate to the risk of the service failing in the first place. It may also be possible that an institution chooses, specifically, a cloud service specifically to reduce the risk of service failures by deliberately selecting cloud modules that offer a very high resilience or better Service Level Agreement (SLA) compared to on-premises. Similarly, the financial solvency of the CSP, or the product licensing conditions, may result in a lower associated risk when using cloud compared to other IT paradigms. This can reduce the need for exit planning. And finally, exit plan testing may carry inherent risks. Consequently, testing cannot be applied without careful consideration by the financial institution.

The EBF Cloud Banking Forum intends to support banks, CSPs and National Competent Authorities (NCAs) in reaching a common understanding on what a sufficient testing of exit plans could possibly imply. Bringing together the expertise of European banks and CSPs, this paper intends to offer guidance to answer the questions: When is testing appropriate? What may constitute sufficient testing of exit plans? Without providing mandatory features for testing, this paper aims to make financial institutions and NCAs aware of relevant factors for consideration and inform on possible voluntary options for testing methods. We are convinced that this enhanced understanding will support a harmonised approach to the supervisory requirement under the EBA GL for testing of exit plans, ultimately supporting the adoption of public/hybrid cloud solutions through the avoidance of potentially conflicting interpretations of supervisors' requirements or an incoherent view of industry-wide concentration risk.

[4] See below under Chapter 2, figure 2.

CHAPTER TWO

2 Exit strategy for critical or important functions

Banks are required to have a documented exit strategy when outsourcing critical or important functions[5]. For the purpose of this paper, we assume a relevant function according to the applicable definition under the EBA GL[6].

To avoid confusion regarding the terminologies, we propose the following definitions for different terms used in the context of the exit strategy and testing:

TABLE 1

Exit strategy	*A high-level description of an institution's ultimate risk mitigation strategy when dealing with a failing cloud provider or when terminating the outsourcing. This might include exit and transition of outsourced functions and data to an alternative provider (in part or completely), the return of these functions on-premises, or even discontinuation of the process.*
Exit plan	*An underlying element to the exit strategy. A high-level document describing how to implement the exit strategy including a description of all its phases, involved roles and responsibilities and various plan features such as the ones mentioned in the EBA Guidelines para. 108 (see also figure 2). A plan is to be enacted in case of pre-defined events following a long-term strategy approach. It does not include short-term incident management, since the business implications of enacting an exit plan can be considered severe. The exit plan ensures business continuity in case of the pre-defined events, aiming at response times appropriate to the severity of the triggering event.*
Testing of an exit plan	*Activities to be performed to ensure that an exit plan is well documented and actionable when necessary. A table-top exit plan test involves a 'paper evaluation' to ensure that the exit plan is fully documented, understood by stakeholders, realistic and achievable in line with business and regulatory requirements. This includes checking on the availability of resources identified in the plan.*

[5] EBA GL, para. 106.
[6] EBA GL para. 12, 29 to 31.

It is important not to confuse business continuity management and exit strategy. The EBA GL require exit arrangements to work without undue disruption of the business activities[7]. Regardless of the type of the cloud service, the difficulty to exit a given service strongly depends on features such as standardisation of inputs and/or outputs, interoperability of systems (availability of standard application programming interface, common messaging formats) and open source. According to the EBA Guidelines on internal governance[8], business continuity management (BCM) refers to the ability of a bank to operate on an ongoing basis and to limit losses in the event of severe business disruption. Thus, the exit strategy can be a component of a business continuity plan when a third party is involved in a critical activity. However, it is not the main element of a BCM, as the time needed to sever a business relationship with a third party is usually longer than the maximum acceptable time a critical activity can be down.

A prime objective of any exit strategy should be to ensure (long-term) continuity of the business function after the outsourcing arrangement is terminated. For that reason, having in place continuous monitoring of the activities addressed by the strategy is as important as having a complete and actionable exit plan in the first place.

EBA GL para. 107 focuses on minimizing the overall impact when exiting the service and sets requirements to achieve this objective such as (summarised):

a. exit plans must be comprehensive, documented and sufficiently tested where appropriate;

b. alternative solutions must be identified, and transition plans must be described to allow for business continuity throughout and after the transition phase.

In accordance with the EBA GL para. 108, exit strategies should be developed with specific features:

a. define the objectives of the exit strategy;

b. perform a business impact analysis that is commensurate with the risk of the outsourced processes, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;

c. assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;

d. define success criteria for the transition of outsourced functions and data;

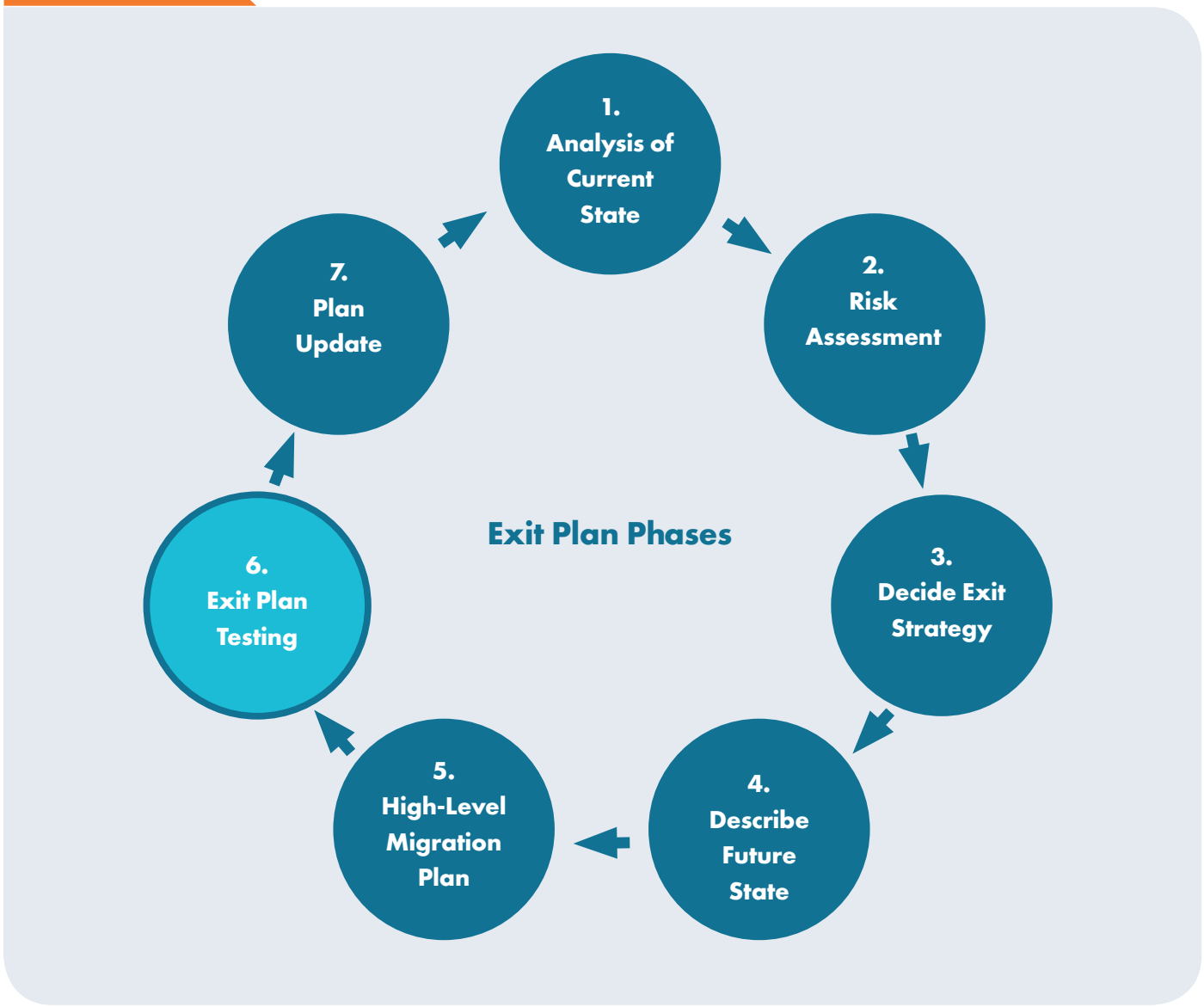
e. define the indicators to be used for the monitoring of the outsourcing arrangement, including indicators based on unacceptable service levels that should trigger the exit.

[7] EBA GL para. 107.

[8] EBA/GL/2017/11 (21 March 2018) on internal governance under Directive 2013/36/EU. https://eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance%20+%28EBA-GL-2017-11%29_EN.pdf/531e7d72-d8ff-4a24-a69a-c7884fa3e476

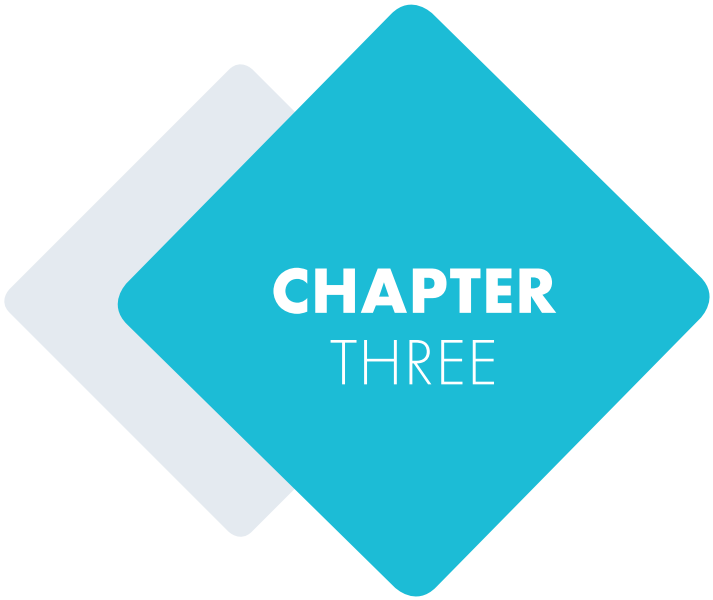
A comprehensive exit plan does not only describe the exit strategy to be applied, but it also embeds the different steps necessary to make the transition from the current state towards a future state where the outsourcing arrangement has ended. This paper does not look to address every step within the exit plan. Instead, it focuses specifically on exit plan testing, providing orientation as to the interpretation of the EBA Guidelines para. 107a. A harmonised approach to the appropriateness and sufficiency of testing by financial institutions and NCAs will reduce the danger of fragmentation in banking supervision in different Member States, thereby helping the financial sector to adopt cloud computing for cross-border business in Europe in general. The necessary risk-based approach to outsourcing arrangements, explicitly acknowledged by EBA, requires cloud-specific considerations in order to appropriately reflect appropriately, the reality of the technology[9].

FIGURE 2



[9] EBF Cloud Banking Forum, Technical Paper "The use of Cloud Computing by Financial Institutions" (2019). Institutions and NCAs are presented with the need for awareness regarding cloud computing's control demand and control landscape.

This paper does not intend to address best practices for banks facilitating the switching of cloud service providers. Following Article 6 of the Free flow of non-personal data Regulation, the SWIPO Working Group already conducted works on the development of self-regulatory codes of conduct at the EU level, addressing processes, timeframes and other aspects of porting and switching. The industry-led Working Group provides codes for IaaS and SaaS, e.g. targeting the supply of detailed and transparent information prior to the conclusion of contracts for data storage and processing. Since SWIPO has already executed the above work in order to reduce 'vendor lock-in' risks, this paper will not replicate the mentioned activities. Instead, the financial industry is encouraged to take careful note of the code of conducts and make use of voluntary best practices appropriate for the individual institution's cloud service model.



3 Guidance on exit plan testing

Concentration risk is stated by EBA to be particularly relevant for cloud outsourcing, creating a need to monitor and manage such risks[10]. A sound and sufficient exit plan testing provides a partial risk mitigation measure at the level of the institution, highlighting the management capabilities in place to counter a disproportionate reliance on cloud services (mitigation of single point of failure).

In agreement with the EBA GL, financial institutions and CSPs consider the testing of exit plans to be important. However, in order to understand how this commitment should translate into practice, the following questions must be answered in a way that allows financial institution to adopt cloud solutions without disproportionate burden:

ONE - When is exit plan testing appropriate?

TWO - What can constitute sufficient testing of exit plans?

3.1 When is exit plan testing appropriate?

Testing according to the EBA GL para. 107a. will depend strongly on the cloud approach taken by the organisation and the type of activity using cloud computing. The IT services should not always have to perform the same level of testing, but rather allow for a proportionate approach. An unplanned complete exit from a cloud outsourcing agreement is a rather rare event to be observed in the markets. This should be reflected when determining the proportionality of risk considerations and, in turn, the appropriateness of testing.

Organisations should take a risk-based approach to determine if exit plan testing is appropriate: meaning a consideration of general necessity and time frame in which a service should be able to exit a provider in case of an unintentional/unexpected termination.

The risk-based approach allows the possibility to reflect upon the central aspect of proportionality, taking into account in particular the financial

[10] EBA GL Background para. 46.

institutions' and CSPs' stability, internal organisation and the nature, scope and complexity of its activities, as well as the overall level of service resilience. A risk-based approach also requires understanding and awareness of the control demand for a specific cloud sourcing. This includes consideration of risk dimensions for the cloud service in question[11] and the effects on the control management of financial institutions and CSPs. Based on the risk assessment and business impact considerations, appropriate testing scenarios can be defined.

Exiting a cloud service requires a look at reversibility, meaning the notion that you can modify or roll back immutable projects, workload deployments or the entire cloud environment to reset to an alternative state.

Its two major dimensions should be considered.

PORTABILITY: defining the effort to use a different technology for the service. The effort is driven mainly by the Layer of abstraction sourced (cloud service model), the availability of supporting functionality and the usage of the market's industry standards.

CRITICALITY: defining the effort to use a different technology for the service in a certain process. This is also driven by the level of integration into a process and its relevance.

For different cloud service models please see table 3.

TABLE 3

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Container as a Service (CaaS)	Software as a Service (SaaS)
Supplies customers with IT infrastructure, provided and managed over the internet on a pay-as-you-use basis, e.g. servers and storage. The two common models of delivery for IaaS are 'bare metal' and Virtual Server Infrastructure (VSI). In the case of bare metal, the financial institution or their designee is responsible for managing the servers, storage, virtualisation, OS, middleware, runtime, data and applications. In the VSI model the financial institution is responsible for managing the OS, middleware, runtime, data and applications.	*Supplies customers with an on-demand environment for developing, testing, delivering and managing software applications over the internet. The financial institution is responsible for managing its data and applications.*	*Offering for container-based virtualisation in which CSPs offer a complete framework to customers for deploying and managing containers, applications and clusters. CaaS offers a completely enabled container deployment service with security and governance control for IT management.*	*Allows customers to connect to and use a cloud-based application over the internet on a subscription basis, e.g. Microsoft Office365. The entire stack is managed by the service provider.*

[11] See visual support tool (spider web) in EBF Cloud Banking Forum's Technical Paper "The use of cloud computing by financial institutions" (2019), Chapter 4.2.

Picking up on cloud services' differences, please find an overview of factors relevant for appropriateness of testing:

Required time for testing

Testing of exit plans can tie up considerable resources in an institution, impairing business operations elsewhere.

Cost of testing

In line with the principle of proportionality, tests can be rendered inappropriate due to disproportionate burden of costs for the institutions. The latter should be able to take a risk-based decision not to enact detailed testing due to its disproportionate cost.

Exit plan considerations as part of the cloud service model's design

The cloud service model may already incorporate testing elements during its design process. Their availability can reduce complexity and costs of later testing.

Model of cloud consumption by the customer

Exit planning depends on the Cloud Service Customers' (CSCs) consumption of services and the available IT environment in case of exit. Hybrid cloud[12] usage requires different considerations regarding the appropriateness of exit testing than full public cloud usage[13], since operational and technical conditions in both cases are different. Hybrid infrastructure can need less testing than public cloud due to incorporated back-up functions potentially located within private cloud elements. For instance, if a cloud service were backed up by an easily accessible private cloud – or even on-premises – system, the risk of data loss would be significantly lower. In turn, testing of exit plans would not be as appropriate since back-up solutions would already enhance service availability for the institution. The business solution in question would continue to operate, even if the respective primary CSP were assumed disabled. Such assumption follows a disaster recovery failover test's line of thinking.
In case of data backups outside the CSP structure, a data reconciliation and consistency test would need to be performed. However, this technical possibility can make the exit plan test more appropriate and – due to the enhanced data security for service performance – lighter/simpler.

Impact of cloud service and technological integration

SaaS: Though typically SaaS services are specific to a CSP, SaaS can be closely integrated into a business process. In this case, exit plan testing would require a full migration to another alternative product. While table-top exercise can address this scenario (incl. by simulation), any data operations for exit testing purposes would be very costly and cause significant workload for the exercise. Respective testing would be disproportionate.

IaaS and PaaS: These services require excessive migration activities. Only if services are set up between different providers in a hybrid setup (e.g. internal, CSP1, CSP2), can testing become feasible. This is true, in particular, with 'liquid workloads', enabled by latest cloud technology using industry standards like containers. 'Liquid workloads' are workloads which can be shifted across different environments without any additional configuration or code change, applying configurations such as containers to orchestrate the environment. Creating 'liquid workloads' is fundamental for efficient hybrid cloud usage and will enable, for example, to burst from internal private environments into public cloud environments. In a hybrid environment, "failovers", switching between resilient capacities, are part of the cloud operations from the outset. Data extractability is a key part of this cloud set-up by the

[12] EBF Cloud Banking Forum's Technical Paper "The use of Cloud Computing by Financial Institutions" (2019), Chapter 2.1.
[13] Ibid.

financial institution, happening repeatedly as part of the day-to-day operations.
Consequently, this daily extractability does not need to be addressed by additional testing.

Specificity and standardisation of the cloud service

Factors inherent in the cloud service can make testing more appropriate, once they reduce required workload or cost implications of the test. The use of low-level services and standardisation (multi-provider solutions such as Ex CaaS) can help to facilitate the transition, making testing more appropriate due to simplified testing opportunities. IaaS and PaaS services benefit from the careful mapping of the level of service solutions between CSPs. The better the mapping exercise, the more readily it will allow an overview of the services, and the easier the possible transition will be executed. IaaS requires testing to ensure that a compatible infrastructure is available (either at a different CSP or internally with the CSC).). However, this testing should not be confused with the creation of an idle dual architecture, creating tremendous burden of cost without operational use. Rather, in preparation of such a test, subsets of functions for the separate environment must be created.

Risk of running the test

Executing a test can have its own operational risk for the financial institution (inherent risk of testing). Next to economic proportionality, such inherent risk needs to be considered as a main factor when considering whether testing is appropriate. A good balance is required between the risk introduced by the test itself and the risk which is meant to be addressed by the testing in the first place. For example, failing an IaaS service over to a different cloud service provider will usually introduce different network topologies to the applications. This will result in the different latency in the communication between applications. In an environment driven by high-volume transactions – like payments or trading – this may result in unforeseen behaviour and therefore outages. Additionally, tests can introduce the risk of potential opportunities for malicious intent (such as data theft). While not deemed common, such consideration should nevertheless be part of the appropriateness assessment.

Relationships between CSC, ingoing CSP and outgoing CSP

What constitutes cooperation between CSPs and how it translates into support measures is important. Such support can help to reduce the risk of IP or security breaches involving customer data. Institutions should have formalised reflections on necessary timeframes for testing available as part of their conducted threat analysis. Testing within the complex cloud ecosystem requires a sound understanding and cooperation between CSPs and CSCs. Consequently, a commitment to support testing should be reflected in the contractual documents between CSP and CSC, highlighting its importance for the relationship.

In light of the above considerations, exit plans should be tested when the following criteria are met:

- the service supported by the cloud service is critical;
- the exit plan does not imply discontinuance of the service;
- an alternative service is not already implemented and running in the real environment;
- input and output data need to be retained and are not stored in a back-up system;
- the cloud service and its migration to an alternative service is not fully standardised;
- the cloud service introduces risks around resiliency or financial stability.

3.2 What can constitute sufficient testing of exit plans?

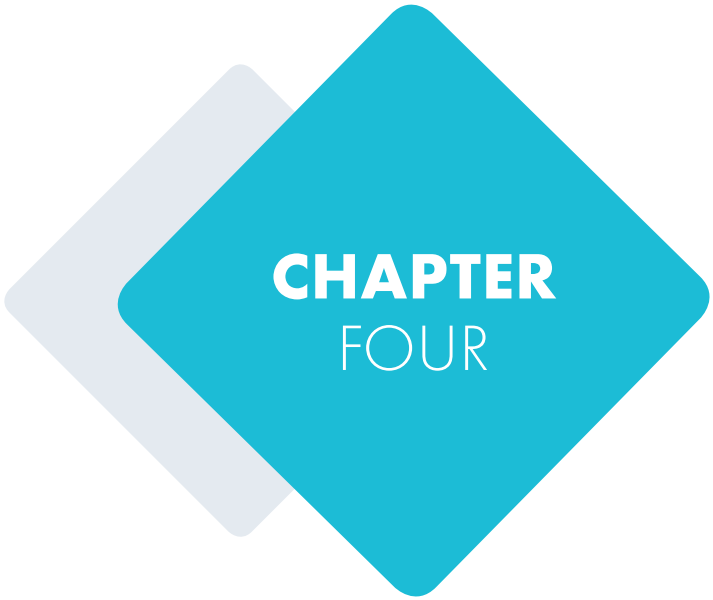
Once testing is deemed appropriate, its elements should ensure compliance with the regulatory requirement established by the EBA: 'sufficiency' of testing[14]. Based on the principle of proportionality[15], institutions must execute discretion as to what this can mean for the cloud service in question. The following overview aims to provide guidance for voluntary consideration by the financial institutions. It shall not be regarded as a catalogue for application to banks regardless of their own considerations on testing.

TABLE 4

Frequency	▸ *Regular testing scheduled by the institution, based on considerations under 3.1* ▸ *In the case of a material breach of a service level defined as an exit trigger*[16]
Objective	*The main objectives of exit plan testing are:* ▸ *to verify that the exit plan continues to fulfil the objectives of the exit strategy;* ▸ *to build and maintain organisational readiness to execute the exit plan;* ▸ *to identify changes and needs for modifications of the exit plan.* *The outcome of the testing is a verified and updated exit plan.*
Test methods	*The following list is provided as an orientation for financial institutions as to what test methods can be applied to achieve the test's objectives. Other test methods can be designed to achieve similar outcomes. The decision on what test methods to apply (in order to test the exit plan in question) should be taken by the subject matter experts working with the particular cloud solution.* ▸ *Review of the technical viability of the exit plan by technical subject matter experts, e.g. via review of solution changes implemented since last testing.* ▸ *Review of the exit plan against existing enterprise capabilities by the IT service owner, e.g. do all roles listed in the exit plan still exist in the organisation and are they familiar with their role in the exit plan?* ▸ *Review of the exit plan against current organisational security standards for protection of data at rest and in transit to verify the adequacy of planned controls, such as applicable encryption and authentication standards.* ▸ *Calculation of current data volumes and identification of impact on data transfer requirements, e.g. is the planned data transfer method still viable?*

[14] EBA GL para. 107a.: sufficiently tested exit plan (e.g. by carrying out analysis of potential costs, impacts, resources and timing implications).
[15] EBA GL para. 18.
[16] EBA GL para 108e.

	Calculation of cost and timing implications of identified changes, such as higher cost and longer transfer time due to an increase in data volumes; faster and cheaper exit due to CSP´s standardisation of the solution; longer exit and additional costs owing to the need to contract third parties (for example a consultancy) due to change of key employees in the institution. *Review of the agreements and collaboration procedures between the institution and the CSP, related to removing outsourced functions and data from the service provider to ensure continued adequacy if deviations are identified in other tests, for example new market standards for data deletion, need for additional technical support, or longer exit period.* *Walkthrough of the plan with exit plan participants, in order to familiarise participants with the current plans and to ensure that the participants understand their roles and responsibilities. This method is useful in identifying gaps in organisational capabilities.* *Desktop exercise, having the participants of the exit plan discuss the plan in theory, checking that it is useable in a passive exercise room environment. The desktop exercise includes testing of organisational roles and escalation. It typically involves a single team discussing the response to a specific scenario under limited pressure.* *Simulation, verifying the robustness of procedures and operating assumptions in a fully monitored and controlled environment by testing the effectiveness of a plan in support of a theoretical response to a scenario. A simulation requires resources for planning and execution and provides deep insight into how to handle the exit. It is a realistic exercise designed to practise roles in an active environment. This test type can contain elements of data extraction, transformation or data import to a target solution.*
Outcomes of exit plan testing	*Reasonable level of confidence that the exit plan is feasible.* *Transparency on time required to execute the exit plan.* *Update of obsolete exit plan areas, agreements and procedures based on identified changes and issues.* *Assurance that the key people involved in a potential exit are familiar with the exit plan.*
Impact	*Effort required to plan and perform the test.* *Effort required to handle deviations and ensure appropriate remediation.* *In simulations, the effort may include additional costs for facility, hardware and software.*



4 Conclusion

Continuity and quality are core features of financial institutions' cloud-based services to clients. Both European banks and CSPs commit themselves to protecting this continuity and quality against detriment, including potential manifestations in case of an exit from a cloud arrangement.

The exit plan of institutions is an important step in the ultimate risk mitigation for extreme failures of the service provider. It must be approached in a risk-based way. This includes respective testing to ensure a sound, continuous safeguard against potential damages.

Financial institutions are invited to consider the voluntary guidance put forward in this paper on the appropriateness of the testing and the orientation for test methods for a table-top testing exercise. While the presented methods do not establish an exhaustive list of any kind, they provide for an understanding of possible actions in order to achieve the presented objectives. This can support financial institutions' preparation for the eventuality of exiting cloud arrangements, thereby avoiding undue disruption to business activities. The assurance won by the suggested preparation for the eventuality of exit contributes to a more aware – and thereby more reliable – cloud application by European banks, ultimately fostering the cloud adoption for the benefit of bank's clients and their business processes in Europe.

THE EBF CLOUD BANKING FORUM

European banks want to adopt innovative cloud technology, to allow them to operate in a fast-developing digital environment, to serve customers and to adapt their business in order to strive for the EU's digital leadership role. In December 2017, the European Banking Federation launched the EBF Cloud Banking Forum,
a policy hub on cloud computing for European banks and Cloud Service Providers to support a harmonised supervisory approach towards cloud computing. This will facilitate the adoption of public/hybrid cloud computing by European banks on a larger scale.

The EBF Cloud Banking Forum focuses on specific regulatory developments related to cloud technology. The forum fosters the important exchange of IT architects, legal experts and cloud specialists from among EBF members (national banking associations and over 15 banks), Cloud Service Providers, and observers.

The latter consist of Cloud Service Providers' trade associations and EU authorities (ECB, EBA, European Commission).

EBF Cloud Banking Forum

FOR MORE INFORMATION CONTACT

European Banking Federation AISBL

Brussels
Avenue des Arts 56, 1000 Brussels,
Belgium,
Julian Schmücker
Policy Adviser - Digital
+32 2 508 3744
j.schmucker@ebf.eu

Frankfurt
Weißfrauenstraße 12-16,
60311 Frankfurt,
Germany

EU Transparency Register ID number:
4722660838-23