EUROPEAN CENTRAL BANK

BANKING SUPERVISION

ECB Guide on outsourcing cloud services to cloud service providers

1 Introduction

The European Central Bank (ECB) acknowledges that the use of cloud services offers various benefits to supervised entities. Compared to internal information and communication technology (ICT) infrastructure, cloud services are cost efficient, scalable, secure due to providers using cutting-edge security technologies, resilient due to data backup solutions and disaster recovery options and provide supervised entities with access to innovative technologies.

At the same time, as the cloud services market is highly concentrated, with many cloud service providers (CSPs) relying on proprietary technologies, especially for SaaS and PaaS procurement models, cloud services expose supervised entities to several risks resulting from the dependency on an ICT third-party service provider. Moreover, the nature of cloud services poses challenges regarding the management of cloud-specific risks as well as the monitoring and auditing of cloud services provided by CSPs.

1.1 Purpose

There are three key issues underpinning the ECB Guide on outsourcing cloud services to cloud service providers ("the ECB Guide"):

First, supervised entities are increasingly moving from using internal information and communications technology (ICT) infrastructure and resources to using cloud services offered by cloud service providers (CSPs).[1] The supervised entities in question need to understand, assess, and monitor these technologies.

Second, the ECB has identified deficiencies in the outsourcing of ICT services that supervised entities need to remedy to improve their operational resilience. This is set out in ECB Banking Supervision's supervisory priorities for 2024-26.

And third, the European Union has recently adopted the Digital Operational Resilience Act (DORA)[2] with a view to consolidating and upgrading ICT risk requirements as part of operational risk requirements, which include key principles for the sound management of ICT third-party risk. The requirements set out in Article

1 When discussing the relationship between supervised entities and CSPs, the ECB Guide refers exclusively to the portfolio of procured cloud solutions rather than any non-cloud-related products that might be offered by CSPs.

2 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

5 of DORA and Article 74 of the Capital Requirements Directive (CRD)[3] are driven by the need to establish effective governance of ICT risk − including in particular the management of ICT third-party risk − and ICT security and cyber resilience frameworks. These are required to proactively tackle any unmitigated risks which could lead to material disruption of critical or important functions or services. When applying the relevant requirements, supervised entities should take into account the nature, scale and complexity of the risks inherent in the business model and the supervised entity's activities.

Similar to other ECB Guides, this Guide does not lay down legally binding requirements, practices, or rules. Also, it should not be construed as introducing new rules or requirements over and above those currently imposed by DORA and its implementing acts, nor does it replace relevant legal requirements stemming from other relevant Union or national law.

The aim of the ECB Guide is to provide clarity on the ECB's expectations with regard to the related requirements set out in DORA, thereby fostering supervisory consistency and helping to ensure a level playing field by increasing transparency.

The ECB also provides a collection of observed good practices in the Guide based on experiences from its ongoing and onsite supervision as well as feedback from its ongoing dialogue with the industry. These good practices aim to illustrate concrete examples of actions assessed as adequate by the ECB. The ECB acknowledges that not all observed good practices may be replicated in all supervised entities, given the specificities of individual supervised entity, and that there may be other examples of good practices that also contribute to an effective outsourcing risk management.

[3] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

Definitions of terms used in this guide	
Cloud service provider (CSP)	A service provider that is responsible for delivering cloud services under an outsourcing arrangement.
Cloud services	As defined in Chapter 2, paragraph 12, of EBA/GL/2019/02, services provided using cloud computing – that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Community cloud	As defined in Chapter 2, paragraph 12, of EBA/GL/2019/02, cloud infrastructure available for exclusive use by a specific community of institutions or payment institutions, including several institutions of a single group.
Critical or important function	As defined in Article 3(22) of DORA, a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.
Good practice	Good practice refers to examples of practices observed in the industry by the Joint Supervisory Teams or on-site inspection teams, assessed as adequate by the ECB, provided for illustrative purposes and which the ECB recommends to follow.
Hybrid cloud	As defined in Chapter 2, paragraph 12, of EBA/GL/2019/02, cloud infrastructure that is composed of two or more distinct cloud infrastructures.
Identity and access management (IAM) policy	A set of rules and protocols that determines and controls how individuals or entities are granted access to systems, applications, data and resources within an organisation's ICT environment.
Infrastructure as a service (IaaS)	A cloud computing model where a vendor provides the customer with processing, storage, networks and other fundamental computing resources and the customer is able to deploy and run its own choice of software, including operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and applications – and possibly limited control of selected network components (e.g. host firewalls).[4]
ICT asset	As defined in Article 3(7) of DORA, a software or hardware asset in the network and information systems used by the supervised entity.
ICT concentration risk	As defined in Article 3(29) of DORA, an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of such provider may potentially endanger the ability of a financial entity to deliver critical or important functions, or cause it to suffer other types of adverse effects, including large losses, or endanger the financial stability of the Union as a whole.
ICT vendor lock-in	An exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers that endangers the ability of the institution to effectively exit from some or all the services provided.
Outsourcing	As defined in Chapter 2, paragraph 12, of EBA/GL/2019/02, an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself.
Platform as a service (PaaS)	A cloud computing model where a customer is able to deploy on the cloud infrastructure customer-created or acquired applications that have been developed using programming languages, libraries, services and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure (including the network, servers, operating systems and storage), but has control over the applications deployed – and possibly configuration settings for the application hosting environment.
Private cloud	As defined in Chapter 2, paragraph 12, of EBA/GL/2019/02, cloud infrastructure available for the exclusive use by a single supervised entity.
Public cloud	As defined in Chapter 2, paragraph 12, of EBA/GL/2019/02, cloud infrastructure available for open use by the general public.
Service provider	As defined in Chapter 2, paragraph 12, of EBA/GL/2019/02, a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.
Software as a service (SaaS)	A business model where a customer is able to use a provider's applications running on cloud infrastructure. The applications are accessible from various client devices through either a thin client interface (such as a web browser – e.g. web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure (including the network, servers, operating systems and storage – and even individual application capabilities), with the possible exception of limited user-specific application configuration settings.
Sub-outsourcing	As defined in Chapter 2, paragraph 12, of EBA/GL/2019/02, a situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider.
Supervisory expectation	An expression of the ECB understanding of how supervised entities should apply the existing provisions of Union or national law for the effective governance of risk related to outsourcing.

4 Based on a definition used by the US National Institute of Standards and Technology.

1.2 Scope and effect

The scope of the ECB Guide encompasses the outsourcing of cloud services to CSPs.

The supervisory expectations set out in the ECB Guide are addressed to institutions that are directly supervised by ECB Banking Supervision. They are an expression of the ECB understanding of how supervised entities should apply the existing provisions of Union or national law for the effective governance of risks related to outsourcing cloud services. In addition, they are drafted in a way to be consistent with DORA for issues specific to cloud outsourcing. These expectations are to be understood in accordance with the principle of proportionality set out in Article 4 of DORA. References to Union directives within the ECB Guide should be regarded as covering all legislation that transposes those directives into national law.

When discussing the relationship between supervised entities and CSPs, the ECB Guide refers exclusively to the portfolio of cloud solutions rather than any non-cloud-related products that might be offered by CSPs. Where a non-CSP third-party provider (TPP) is reliant on cloud services that effectively underpin critical or important functions of a supervised entity, the same supervisory expectations apply.

2 Supervisory expectations

2.1 Governance of cloud services

The ECB recommends that a supervised entity, as part of its ICT risk management framework, pays a particular attention to the roles and responsibilities related to the use of cloud services, conduct a comprehensive risk assessment before entering into a contractual arrangement with a CSP and ensure consistency between its cloud strategy and its overall strategy.

2.1.1 Full responsibility of supervised entities

Supervised entities should ensure that they establish an appropriate governance framework[5] for – and thus control and monitoring of – the outsourcing of cloud services. This should include definitions of the roles and responsibilities of the relevant functions and bodies.

The outsourcing of cloud services creates operational responsibilities for both the CSP and the supervised entity, making a clear and unambiguous allocation of responsibilities more challenging. Nevertheless, under Article 5(2) of DORA the supervised entity's management body bears the ultimate responsibility for the management of ICT risk. The supervised entity should ensure that when procuring

[5] A governance framework is considered appropriate if it complies with the requirements of Article 5 of DORA and Article 74 of the CRD.

cloud services, roles and responsibilities are clearly understood and defined internally and contractually agreed.

Under Article 28(1) of DORA, supervised entities are required to manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework. The ECB considers it good practice for supervised entities that outsource ICT services to apply the same level of diligence regarding risk management practices, processes, and controls (including ICT security) as if they had decided to keep the relevant services in-house. Consequently, it is good practice for supervised entities to ensure that their CSPs have established equivalent risk management practices, processes, and controls.

2.1.2 Ex ante risk assessment

Under Article 28(4) of DORA, supervised entities are required to conduct a risk analysis – known as an "ex ante risk assessment" – that covers certain specified elements prior to entering into a new cloud outsourcing arrangement with a CSP. In order to adequately identify and assess all of the relevant risks relating to the outsourcing of cloud services, it is good practice for supervised entities to:

- perform a thorough analysis of the control processes to be established for the relevant risks identified and of the way controlling mechanisms of both the supervised entity and its CSP will be effectively integrated;
- assess the CSP's ability to provide the information required for these controls;
- ensure that the CSP has itself properly implemented the relevant controls;
- assess whether the supervised entity has the expertise and human resources required to implement and perform these controls;
- in the case of ICT services supporting critical or important functions, assess the risks associated with long and complex sub-outsourcing chains, bearing in mind the requirements set out in Article 29(2) of DORA.

It is good practice for an ex-ante risk assessment to take account of the following risks:

- vendor lock-in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required;
- data storage and processing risks, as well as the potential for sensitive data to be lost, altered, destroyed or disclosed without authorisation;
- physical risks and region-specific risks (e.g. risks relating to the political stability of the country where the services are provided and/or the data are stored);
- the risk of a considerable fall in quality or a significant increase in price (both of which are potential scenarios in a highly concentrated market);

- the risks of a multi-tenant environment.

Box 1

Assessment of concentration risk and provider lock-in risk

As referred to in Section 2.1.2, Article 28(4)(c) of DORA requires supervised entities to perform an ex ante risk assessment to identify and assess all relevant risks relating to the contractual arrangement, including the assessment of ICT concentration risk as referred to in Article 29., The ECB considers it good practice for supervised entities, when performing risk assessments, to consider typical risks relating to cloud services (such as increased provider lock-in, less predictable costs, increased difficulty of auditing, concentration of provided functions and lack of visibility regarding the use of sub-providers), alongside aspects of location of data. The ECB believes that, especially when it comes to concentration risk, it is good practice for supervised entities to perform such a risk assessment on a regular basis, as providers' practices may change over time, given among other things the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with a potential impact on concentration risk). A regular review of the supervised entity's dependence on individual service providers (including procured services that are sub-outsourced to specific CSPs) is strongly advisable. Concentration risk may be exacerbated by a lack of knowledge about other CSPs' proprietary technology, which creates difficulties and increases the cost of switching or exiting contracts ("lock-in risk"). Such concentration risk should ideally also be incorporated in the policy on the use of ICT services supporting critical or important functions.[6]

2.1.3 Consistency between a supervised entity's cloud strategy and its overall strategy

Article 6(3) of DORA requires supervised entities to minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools. Furthermore, under Article 28(2) of DORA, a supervised entity must have in place a strategy that covers ICT third-party risk, including the risk of outsourcing to CSPs. The strategy required by DORA can be included in the supervised entity's digital operational resilience strategy or integrated into its general outsourcing strategy addressing cloud-related issues. Recital 45 of DORA implies that any strategy on ICT third-party risk should be consistent with the supervised entity's general strategy. At the same time, it is good practice that the strategy on ICT third-party risk is consistent with the supervised entity's digital operational resilience strategy and its internal policies and processes, including its ICT risk appetite.

[6] Which is also set out in Article 1(h) of the RTS on ICT TPPs. See Commission delegated regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (OJ L, 2024/1773, 25.6.2024).

2.2 Availability and resilience of cloud services

In order to be able to operate on an ongoing basis in the event of severe business disruption, a supervised entity must have in place adequate ICT business continuity measures as part of its overall business continuity policy. The ECB considers it good practice for supervised entities to have a holistic perspective on business continuity measures for cloud solutions. In addition, the ECB provides in this Guide good practices for the implementation of cloud resilience measures supporting critical or important functions, in particular regarding the assessment of the CSP's disaster recovery plan.

Moreover, as a result of the particular way in which cloud services are set up, the CSP has the technical ability to terminate any service/access for any customer at any point in time in such a way that the service cannot be resumed by another CSP and the supervised entity itself. The ECB considers it good practice for supervised entities to draw up an appropriate business continuity policy in order to ensure that they are able to withstand such a scenario and have access to the data required to operate the service in question.

2.2.1 Holistic perspective on business continuity measures for cloud solutions

As specified in Article 85(2) of the CRD, a supervised entity must have contingency and business continuity plans that ensure it is able to continue operating and limit losses in the event of severe disruption to its business. Article 11(1) of DORA also requires supervised entities to put in place a comprehensive ICT business continuity policy. When selecting cloud services– especially for critical or important functions – a supervised entity should ensure business continuity, resilience, and disaster recovery capabilities.

In the context of Article 12 of DORA, the ECB considers it good practice for supervised entities' response and recovery planning for cloud services to include backup policies and procedures, as well as restoration and recovery procedures and methods, in order to mitigate a failure by the CSP to provide services or the failure of the CSP as a whole. The scope of the data that are subject to the backup and the minimum frequency of the backup should be based on the criticality of information or the confidentiality level of the data. The ECB considers good practice that the risk assessment is taken into account when selecting the solution to store and restore backup data and systems. Furthermore, the ECB recommends supervised entities to consider in their risk assessment that backup data and systems are stored into ICT systems physically and logically segregated from the source ICT systems. Depending on the outcome of the risk assessment, backup methods may make use of resources offered by the same CSP, by another CSP, by a non-cloud service provider or on-premises. The backup procedures and restoration and recovery procedures and methods should be tested periodically in accordance with Article 12(2) of DORA. It is good practice that tests are validated with regard to the

accuracy, completeness and practicality of restoration and recovery procedures and methods.

To complement Article 12(6) of DORA, the ECB considers it good practice for business continuity management (BCM) measures to address an extreme scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available.

2.2.2 Proportionate requirements for critical or important functions

For the purposes of the requirements of Article 85(2) of the CRD and Article 6(8) of DORA, the supervised entity should assess the resilience requirements for the cloud outsourcing services provided and the data managed and, following a risk-based approach and in accordance with the principle of proportionality, decide on appropriate cloud resilience measures. These may include the following measures, which are provided as good practices of currently available, common cloud business continuity patterns. The list is not intended to be exhaustive or to cover all scenarios:

- Multiple active data centres in different geographical locations with independent power supply and network connections, allowing a switch to a data centre in another physical location if a data centre becomes unavailable. Having two hot-synced data centres in the same physical location might not suffice if a function is critical or important.
- Use of hybrid cloud architecture.
- Multiple CSPs or backup providers, as long as data centres and physical locations do not overlap as a result of services being spread across multiple vendors that share data centres.

For the purposes of Article 12 of DORA, the ECB considers it good practice that the supervised entity will ensure that, for critical or important functions, abrupt discontinuation of a CSP's outsourced cloud services does not lead to business disruption beyond the maximum tolerable downtime or data loss as defined in the supervised entity's ICT business continuity plan.

2.2.3 Oversight of the planning, establishment, testing and implementation of a CSP's disaster recovery strategy

Under Article 11(6) of DORA, supervised entities' testing plans must include, among other things, scenarios involving cyberattacks and switches between the primary ICT infrastructure and the redundant capacity. The ECB considers it good practice for a supervised entity to assess its CSP's disaster recovery plans and tests and not rely exclusively on relevant disaster recovery certifications. When assessing a CSP's disaster recovery test, the supervised entity is recommended to assess the CSP's readiness for an actual disaster event. It is advisable that the testing plan covers a variety of disaster recovery scenarios, including component failure, full site loss, loss

of a region and partial failures. Under Article 11(6)(a), these scenarios must be tested at least yearly in accordance with the supervised entity's strategy and in line with its business continuity policy and requirements.

In the view of the ECB, it is good practice for supervised entities to ensure that, in order to ensure awareness of their responsibilities and ensure that they have appropriate skills, staff at the supervised entity and the CSP who are involved in disaster recovery procedures have designated roles and training. When assessing the CSP's disaster recovery tests, the supervised entity should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the CSP.

It is also good practice for any deficiencies identified during testing to be documented and analysed in order to identify corrective measures. This includes the appropriate governance bodies establishing and monitoring a remediation plan (including details of relevant roles and responsibilities).

2.3 ICT and data security, confidentiality and integrity

When supervised entities connect their internal systems to cloud-based applications, they expand their secure areas to include the cloud. In such cases, it is important for them to carefully assess the risks and make informed decisions about managing these risks. This process should also consider the requirements outlined in Article 9 and Article 28(5) of DORA as well as Article 11 of Commission Delegated Regulation (EU) 2024/1774 supplementing DORA[7]. Consequently, supervised entities need to protect their data (including relevant backups) against unauthorised access by maintaining high levels of data encryption, for example, and constantly adapting to cyber threats. Under Article 6 of Commission Delegated Regulation (EU) 2024/1774 supplementing DORA, this involves encrypting data in transit, at rest and, where feasible, in use, employing appropriate encryption methods in line with the supervised entity's data sensitivity classification policy and following a risk-based approach.

The security and accuracy of data in transit and data at rest are key requirements when relying on cloud-based services, including cloud infrastructure. A failure to fulfil these requirements could potentially cause severe reputational damage and have a significant financial impact.

Supervised entities that outsource to the cloud retain responsibility for their data. In a similar manner as the requirements set out in the General Data Protection

[7] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework (OJ L, 2024/1774).

Regulation (GDPR)[8] and the guidelines[9] of the European Data Protection Board for personal data, the ECB considers it good practice for supervised entities to restrict the locations where CSPs can store their data and to apply appropriate tracing mechanisms to monitor compliance with those restrictions, while also ensuring that data can be accessed when needed.

2.3.1 Establishment of adequate data security measures

Under Article 9(4)(d) of DORA, supervised entities are required to implement protection measures involving cryptographic keys whereby data are encrypted on the basis of approved data classification and ICT risk assessment processes. This requirement is further developed in Articles 6 and 7 of Commission Delegated Regulation (EU) 2024/1774 supplementing DORA. In order to complement those provisions, the following can be regarded as good practice in terms of ensuring the establishment of adequate encryption and cryptographic key management processes:

- Detailed policies and procedures are in place governing the entire lifecycle of encryption and cryptographic controls which include a key access justification process that has the characteristics identified in Article 9(3) of DORA.
- Details of encryption algorithms, corresponding key lengths, data flows and processing logic which follow contemporary standards and are regularly reviewed as appropriate by subject matter experts to identify potential weaknesses and points of exposure. Only non-obsolete encryption methods and keys of sufficient length are used for encryption.
- Cryptographic keys are controlled to ensure that they are generated and managed securely and are reviewed regularly in accordance with industry best practice.
- Encryption keys used for the encryption of supervised entity data are unique and not shared with other users of the cloud service.

In addition to encryption technology, supervised entities may also (i) use multi-cloud technologies that enhance their data security, (ii) apply appropriate network segmentation, or (iii) adopt other data loss prevention measures.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[9] Such as Guidelines 10/2020 on restrictions under Article 23 of the GDPR or Guidelines 05/2021 on the Interplay between application of Article 3 and provisions on international transfers as per Chapter V of the GDPR.

2.3.2 Risks stemming from the location and processing of data

Under Article 26(2)(h) of Commission Delegated Regulation (EU) 2024/1774 supplementing DORA, the ICT response and recovery plans of supervised entities need to take into account a scenario of political and social instability, including, where relevant, in the ICT third-party service provider's jurisdiction and the location where the data are stored and processed. Furthermore, since some CSPs may be heavily affected by third-country legislators, the ECB considers it good practice for these risks to be explicitly taken into consideration. Supervised entities are advised, therefore, to draw up a list of countries[10] where their data can be stored and processed[11], depending on the data in question. That assessment should ideally take account of legal and political risks surrounding outsourcing (e.g. the risk of litigation or sanctions).

It is good practice that the requirements, processes and controls for the processing and storage of data are consistent across all agreed locations or zones. This should be assessed for the various zones and locations on a regular basis. Data processing controls should be in place for the retrieval, transformation or classification of (personal) information on behalf of the supervised entity or on behalf of the CSP (sub-processing).

Furthermore, the ECB considers it good practice for supervised entities to assess additional risks if a subcontractor relevant for the cloud services is located in a different country from the CSP. At the same time, they should take into account any risks associated with complex sub-outsourcing chains as outlined in paragraph 67(b) of the EBA Guidelines on outsourcing arrangements.[12]

2.3.3 Consistent inclusion of outsourcing assets in a supervised entity's inventory of ICT assets

Under Article 8(1) of DORA, supervised entities must identify, classify, and adequately document all ICT-supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions and their roles and dependencies in relation to ICT risk. Therefore, the ECB considers it good practice for supervised entities to adopt a clear policy on the classification of all ICT assets, including those that are outsourced to CSPs. This policy should be applied by the supervised entity in every case and should support the supervised entity's ability to assess and determine the controls that are necessary to ensure the confidentiality, integrity and availability of data, regardless of where the data are stored and processed.

---

10 The European Commission has drawn up a list of non-EU countries where the level of data protection is considered adequate on the basis of Article 45 of the General Data Protection Regulation (GDPR). The ECB advises supervised entities to broaden the scope beyond personal data to all data managed under a cloud outsourcing arrangement.

11 In case they are included in the contractual arrangement between the supervised entity and the ICT third-party provider in accordance with the Article 30(2)(b) of DORA.

12 Final report on EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).

As part of this practice, a supervised entity is recommended to keep an up-to-date inventory of all the ICT assets for which it is responsible under the policy in order to ensure that all operational processes (monitoring, patching, incident management, change management, etc.) are extended to cover cloud assets.

2.3.4 Identity and access management policies for cloud outsourcing arrangements

Unclear roles and responsibilities for the management of access and configuration rights and encryption keys are a major source of operational risk and disruption for cloud services, as commonly observed in supervisory activities. Consequently, the configuration of the cloud environment should be clearly defined and agreed between the parties, with a clear segregation of duties.

A supervised entity's identity and access management (IAM) policy should be extended to cover cloud assets and should encompass both technical and business users.

To complement Article 30 of DORA, the ECB considers it good practice for supervised entities, when entering into a cloud outsourcing arrangement, to consider adding individual clauses in the contract with the CSP requiring it to align with the supervised entity's IT and IAM policies. If this is not feasible, the supervised entity is recommended to look at how the IAM structure provided by the CSP for the cloud services fits with the supervised entity's roles and responsibilities to ensure the effective segregation of duties. Any deviations from the effective segregation of duties can then be analysed and addressed using risk mitigation measures.

Box 2

Access management, remote access and authentication of users

To complement Articles 20 and 21 of Commission Delegated Regulation (EU) 2024/1774 supplementing DORA, the ECB recommends supervised entities to consider the following good practices:

- Supervised entities' users – especially those with privileged access rights – are clearly identified and authenticated using a strong authentication solution (i.e. multi-factor authentication) considering the applicability of such solution when connecting to cloud systems supporting critical or important functions. Access rights are subject to regular user access reviews. Re-certification and access withdrawal processes are applied to review access rights in order to prevent users from having excessive privileges. The frequency of such processes reflects the criticality of the function in question.
- Privileged users' access is clearly tracked in real time and reported. Access/change requests are subject to agreed approval processes when they entail access to the supervised entity's data. Access reviews should adopt a broad perspective, looking at in-house systems as well.
- Unambiguous business owners are identified in order to ensure accountability for, and ownership of, each specific role.

- Access security measures (such as two-factor authentication and virtual private network (VPN) encryption) are implemented.
- Appropriate monitoring and logging tools are employed to properly document and monitor a CSP's access to any of the supervised entity's systems or data. Such tools are reviewed on a regular basis.

2.4 Exit strategies and termination rights

Under Article 28(8) of DORA, supervised entities are required to put in place exit strategies for ICT services that support critical or important functions. Significant challenges and risks can arise if a supervised entity decides to terminate a contractual arrangement with a CSP without having previously established a comprehensive exit plan on the basis of an overarching exit strategy for outsourcing arrangements supporting critical or important functions. Exit strategies with clearly defined roles and responsibilities and estimated costs should be drawn up for all outsourced cloud services supporting critical or important functions before those systems go live. The time required to exit should reflect the transition period indicated in the relevant contractual arrangement.

2.4.1 Termination rights

Contractual arrangements for the use of ICT services must allow the supervised entity the right of termination if any of the circumstances set out in Article 28(7) of DORA arises. The ECB understands that grounds for such a termination, which should be clearly stated in the cloud outsourcing contract with the CSP, could include (i) persistently inadequate performance; or (ii) significant breaches of the contractual terms, or of the applicable law or regulations.

Furthermore, for the purposes of Article 28(7) of DORA, the ECB considers it good practice for supervised entities to view the relocation of business units or data centres as grounds for termination. Beyond this provision, the ECB recommends supervised entities to consider that the following changes may also justify termination: (i) a merger or sale, (ii) relocation of the CSP's head office to another jurisdiction, (iii) relocation of the data centre hosting to another country, (iv) a change to national legislation affecting the outsourcing arrangement, (v) a change in the regulations applicable to data location and data processing if the CSP cannot or chooses not to modify its delivered services to comply with changed legislation, (vi) significant changes to the subcontractor's cybersecurity risk, and (vii) continuous failure to achieve agreed service levels or a substantial loss of service.

As a matter of good practice, contractual arrangements for the use of ICT services supporting critical or important functions should include a transition period in the event of termination. The purpose of this is to reduce the risk of disruption and to allow a switch to another provider or the insourcing or decommissioning of the

service. The ECB understands that, in order to allow for such a transition, it is advisable that the supervised entity ensures that the agreed transition terms reflect its exit plan.

If an outsourcing contract encompasses several services that can be managed independently, it should be possible, where feasible and beneficial, to terminate only some of those services.

In terms of the requirement concerning key contractual provisions contained in Article 30(2)(a) of DORA, the ECB considers it good practice for supervised entities to ensure that subcontractors of the CSP supporting critical or important functions comply with the same contractual obligations that apply between the supervised entity and the CSP. This includes obligations relating to confidentiality, integrity, availability, the retention and destruction of data, configurations and backups.

As good practice, the supervised entity should ensure that the CSP's termination rights are aligned with the supervised entity's exit strategy. In particular, the notice period set out in the contract with the CSP should be sufficient to allow the supervised entity (or any third-party service provider employed by the supervised entity that uses cloud services in its outsourcing chain) to transfer or insource the relevant services in accordance with the schedule in the exit plan.

2.4.2 Components of the exit strategy and alignment with the exit plan

With reference to Article 28(8) of DORA, the ECB considers it good practice for supervised entities to establish an overarching exit strategy with a view to ensuring operational resilience and mitigating relevant risks. Such a strategy should contain granular technical exit plans for individual cloud outsourcing arrangements that support critical or important functions. According to Article 10 of Commission Delegated Regulation (EU) 2024/1773 supplementing DORA, exit plan shall be realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the contractual arrangements. In that context, the ECB understands that supervised entities' exit plan should allow sufficient time for all the steps that need to be taken in the event of a planned or sudden exit to be completed. This includes the establishment of alternative arrangements, such as moving the services in-house or finding an alternative provider. While BCM measures should ensure the continuity of services in the short term, exit plans should ensure continuity in the long term.

Furthermore, Article 28(8) of DORA provides that supervised entities must develop transition plans enabling them to remove the contracted ICT services and the relevant data from the ICT third-party service provider and to securely and integrally transfer them to alternative providers or reincorporate them in-house. The ECB understands that supervised entities should retain the ability to reincorporate data and applications in-house or to transfer them to alternative providers. To this end, supervised entities may consider using solutions that enhance the portability of data and ICT systems, facilitating effective migration. Examples of IaaS portable

technologies include virtual machine and container-based applications, while portability aspects of PaaS and SaaS depend on the specific solutions.

Where an exit strategy focuses on moving ICT services to another provider, the ECB recommends supervised entity to draw up a list of qualified alternative service providers. This list should be reviewed and updated on a regular basis using market reviews, looking, for example, at the advantages and disadvantages of the various providers. Where exit strategies involve bringing services in-house or migrating them to another provider, supervised entities are recommended to perform technical analyses and estimate the time required for such a transition. This should be in line with the termination dates and periods set out in the contract.

2.4.3 Granularity of exit plans

In the context of Article 28(8) of DORA, the ECB considers it good practice for a dedicated exit plan to contain provisions ensuring that a supervised entity is able to react quickly to a deterioration in the service provided by a CSP. It is good practice for exit plans to include, as a minimum, the critical milestones, a description of the tasks and skillsets that are required to perform the exit, and a rough estimate of the time required, and the costs involved. Exit plans should be reviewed and tested on a regular basis bearing in mind the principle of proportionality set out in Article 28(1)(b) of DORA, Furthermore, the ECB considers it good practice for supervised entities to, at a minimum, perform an in-depth desktop review, ensuring that such reviews are conducted by staff who have sufficient expertise in cloud technologies. Supervised entities are also recommended to review the volume of data and the complexity of the applications that would need to be migrated, giving consideration to the potential data transfer method, in order to produce meaningful estimates of the time required. Supervised entities should check that they have the staff required for their exit plans, be they internal or external, in light of the principle of proportionality. At the same time, they should conduct a walkthrough of the tasks involved to ensure that the staff available are able to perform the tasks outlined in the exit plan.

In order to check the employees' ability to perform the tasks assigned to their roles, it is good practice that the most critical steps in the migration process are tested periodically. Supervised entities should check, on a regular basis, whether internal members of staff have the skillsets required to perform the tasks set out in their exit plans or whether external consultants would be needed in order to exit a cloud outsourcing arrangement. It is good practice for the feasibility of each exit plan to be independently verified, meaning that it is reviewed by someone who is not responsible for drafting the plan in question.

2.5 Oversight, monitoring and internal audits

Supervised entities are required to have in place a sound ICT risk management framework, including sound monitoring of ICT third-party risk, which is subject to regular internal audits. In addition, the contractual provisions relating to incident

reporting are an essential part of a supervised entity's monitoring of ICT third-party risk. Under Article 6(4) of DORA, supervised entities are required to ensure appropriate segregation and independence of ICT risk management functions, control functions and internal audit functions, in accordance with the three lines of defence model.

2.5.1 Independent monitoring of CSPs

Under Article 6(10) of DORA, supervised entities may, in accordance with Union and national sectoral law, outsource the task of verifying compliance with ICT risk management requirements to intra-group or external undertakings. In such cases, the supervised entity remains fully responsible for the verification of compliance with the ICT risk management requirements. The ECB understands this to mean that responsibility for the verification of compliance with the ICT risk management requirements by the outsourced function cannot itself be outsourced. This remains the case even where cloud services are provided as managed services, with the CSP responsible for keeping operations running and complying with security standards. In order to ensure an adequate level of quality, the supervised entity should monitor the cloud services provided by the CSP. Relying solely on monitoring tools provided by a CSP to assess performance might not be sufficient where critical or important functions are outsourced. In such a scenario, independent tools should be employed in addition to the monitoring tools provided by the CSP to enhance the oversight of critical or important functions. Supervised entities should retain suitable expertise in-house to perform appropriate monitoring of CSPs. The monitoring and oversight metrics used should give the relevant team a comprehensive overview and should form the basis for internal reporting to the management body on the outsourcing activities of the supervised entity.

The supervised entity should ensure that all contractual arrangements for outsourcing – including intra-group outsourcing– take account of the reporting that is required for monitoring purposes in particular when using ICT services supporting critical or important functions, as set out in Article 9 of Commission Delegated Regulation (EU) 2024/1773 supplementing DORA.[13]

2.5.2 Incident reports and contractual details

Under Article 19(5) of DORA, supervised entities that decide to outsource their reporting obligations to a third-party service provider nevertheless remain fully responsible for the fulfilment of incident reporting requirements. The supervised entity's oversight function should be able to follow up in detail on any incident that occurs at the CSP and that may have an impact on the supervised entity, with clearly

[13] Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (OJ L, 2024/1773, 25.6.2024).

defined procedures, roles and responsibilities for incident management. Reports should include relevant details to enable affected services to be identified. These reports should allow the supervised entity to assess any potential impact on its business. All stages of the incident management process should be tracked in order to allow appropriate conclusions to be drawn and lessons to be learnt. Supervised entities are recommended to use contractual clauses to ensure that appropriate incident and monitoring reports are prepared, enabling ongoing assessment of outsourced functions.

Box 3
Contractual clauses

Article 30(4) of DORA provides that, when negotiating contractual arrangements, supervised entities and ICT third-party service providers must consider the use of standard contractual clauses developed by public authorities for specific services. The specific recommendations listed below can be regarded as a guide to good practice in contractual clauses:

- Contractual clauses that allow supervised entities to follow up on ineffective provision of services and ask for remedial actions to be implemented.
- Contractual clauses that allow supervised entities to monitor any deterioration in services and ask for remedial actions to be implemented.
- Contracts that include details of how the cost of performing on-site audits is calculated.
- Both the supervised entity and the service provider should keep a copy of the original contract at the time of signing. Any subsequent amendments to the terms of the contract should be notified to and agreed by all parties to the contract, with copies retained by all parties.

2.5.3 Internal audits

Under Article 8(3) of Commission Delegated Regulation (EU) 2024/1773 supplementing DORA, a supervised entity must not over time rely solely on third-party audit reports made available by the CSP. If a supervised entity makes compromises on the audit rights regime, the supervised entity's audit function may no longer be able to conduct an independent review of an outsourcing arrangement. In a scenario where a CSP does not provide sufficient detail about its infrastructure processes and internal control systems, this may result in the supervised entity lacking detailed first-hand knowledge of the CSP's premises, information systems, proprietary technology, subcontractors and contingency plans, as most entities rely solely on the CSP's statements and third-party certifications. Therefore, it is not sufficient to rely solely on the CSP's statements and third-party certifications.

In the context of Article 6(6) of DORA, the ECB expects the internal audit function of the supervised entities to regularly review the risks stemming from the use of a CSP's cloud services. The ECB recommends That the review covers, among other

things, whether internal guidelines are applied appropriately, the risk assessment is conducted properly and the CSP's risk management is of sufficient quality. Following good practices ensuring that outsourced cloud services can be controlled and steered effectively, the ECB advises supervised entities to ensure that the contractual arrangement with a CSP clearly specifies that the supervised entity, its internal audit function and the competent authorities and resolution authorities have the right to access, inspect and audit the CSP. This is similar to what is required for contractual arrangements on the use of ICT services supporting critical or important functions under Article 30(3)(e)(i) of DORA.

With cloud infrastructure and services becoming increasingly complex, there is a greater need to pool expertise and resources given the skills and resources required for audits and the costs involved. As good practice, supervised entities should verify that auditors conducting the audit have a recognised professional certification. The related skills need to be updated frequently, given the fast pace of technological change. A supervised entity's internal audit function is recommended to ensure that risk assessments performed by the second line of defence are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews or input provided by third parties (e.g. security analysts). To carry out an audit of a CSP, the supervised entity could use its own internal audit function or an appointed third party, as set out in Article 8(2)(a) of Commission Delegated Regulation (EU) 2024/1773 supplementing DORA.

The ECB considers a good practice that supervised entities work together in line with Article 8(2)(b) of Commission Delegated Regulation (EU) 2024/1773 supplementing DORA, to audit a CSP, by forming a joint inspection team containing at least one technical expert from each supervised entity. The inspection plan could be agreed by the supervised entities concerned on a consensus basis. If specific issues raised during such a joint audit are only relevant to a single supervised entity, supervised entities should have the ability to follow up individually with the CSP on a bilateral basis. To prevent blind spots in the conduct of audits, the ECB recommends that the leadership of such inspection teams rotate among the supervised entities involved, on a regular basis.

Annex: Table of acronyms

Acronym	
BCM	Business continuity management
CRD	Capital Requirements Directive
CSP	Cloud service provider
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
ECB	European Central Bank
IAM	Identity and access management
IaaS	Infrastructure as a service
ICT	Information and communications technology
PaaS	Platform as a service
SaaS	Software as a service
TPP	Third-party provider

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.bankingsupervision.europa.eu

For specific terminology please refer to the SSM glossary (available in English only).

PDF ISBN 978-92-899-7096-9, doi:10.2866/3638533, QB-01-25-041-EN-N