EUROPEAN CENTRAL BANK

BANKING SUPERVISION

ECB Guide on outsourcing cloud services to cloud service providers

1 Introduction

1.1 Purpose

The motivation for the ECB Guide on outsourcing cloud services to cloud service providers (hereinafter, the "ECB Guide") is threefold:

- Firstly, Institutions are increasingly moving from the use of internal information and communication technology (ICT) infrastructure and resources to the use of cloud computing services offered by cloud service providers (CSPs).[1] While the use of cloud services can bring numerous benefits to the banking industry (including access to innovative technologies, scalability and flexibility), it also increases institutions' exposure to several risks. The cloud services market is highly concentrated, with many CSPs relying on proprietary technologies, and those technologies must be understood, assessed and monitored by the institutions in question.

- Secondly, The European Central Bank (ECB) has identified deficiencies in the operational resilience frameworks of supervised institutions as regards the outsourcing of ICT services, as highlighted in ECB Banking Supervision's supervisory priorities for 2024-26.

- Finally, the EU legislator has recently adopted new legal acts – such as the Digital Operational Resilience Act (DORA)[2] – which focus on establishing qualitative rules protecting against ICT-related incidents, including those stemming from outsourcing. The requirements of Article 5 of DORA and Article 74 of the Capital Requirements Directive (CRD)[3] are driven by the need to establish effective governance of outsourcing risk, as well as ICT security and cyber resilience frameworks, in order to proactively tackle any unmitigated risks which could lead to material disruption of critical functions or services.

With this document, the ECB provides its understanding of those legal requirements. The aim of the ECB Guide is to explain the ECB's understanding of those specific

1 When discussing the relationship between supervised institutions 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).

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).

rules and provide clarity on its expectations regarding institutions' outsourcing of cloud services, thereby fostering supervisory consistency and helping to ensure a level playing field.

The ECB Guide sets out detailed supervisory expectations, drawing on risks observed in the context of ongoing supervision by Joint Supervisory Teams, as well as on-site inspections. Where appropriate, those expectations are complemented by examples of effective practices observed during supervisory activities.

Definitions of terms for the purposes of this Guide	
cloud service provider (CSP)	A service provider that is responsible for delivering cloud services under an outsourcing arrangement.
cloud services	Services provided using cloud computing – that is to say, a model 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	Cloud infrastructure available for exclusive use by a specific community of undertakings (e.g. undertakings belonging to a particular group).
critical or important function	Activities, services or operations whose discontinuance is likely to lead to disruptions of services that are essential to the real economy in one or more member states or the disruption of financial stability, given the size, market share, external and internal interconnectedness, complexity or cross-border nature of an institution or group's activities, particularly as regards the substitutability of those activities, services or operations.
hybrid cloud	Cloud infrastructure that is composed of two or more distinct substructures.
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 an IaaS 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	A software or hardware asset that is found in the business environment.
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	Cloud infrastructure available for the exclusive use of a single undertaking, which can be installed either on or off the premises.
public cloud	Cloud infrastructure available for use by the general public.
service provider	A third-party entity that performs or provides a process, service or activity (or part 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.

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

1.2 Scope and effect

The supervisory expectations set out in the ECB Guide are addressed to institutions that are supervised directly by ECB Banking Supervision. When applying these expectations, account should be taken of the principle of proportionality. The supervisory regime under DORA that will enter into force on 17 January 2025 has been taken into consideration to the extent possible. Also, the ECB Guide may be complemented by publications produced by other supervisory authorities within the Single Supervisory Mechanism (SSM), such as national competent authorities (NCAs). References to Union directives within the ECB Guide should be regarded as covering all legislation that transposes those directives into national law.

The ECB Guide does not lay down legally binding requirements. It does not replace the relevant legal requirements stemming from Union or national law, nor should it be construed as introducing new rules or requirements over and above those currently imposed by Union and national law. Although the European Banking Authority (EBA) Guidelines on outsourcing arrangements (EBA/GL/2019/02) are also applicable to cloud outsourcing (incorporating the EBA recommendations on outsourcing to cloud service providers that were initially published in 2017), cloud technologies are so important that a comprehensive description of prudent risk mitigation practices is warranted. The ECB Guide should be read in conjunction with the DORA regulatory framework (including implementing legislation), which takes precedence over this ECB Guide, and the EBA Guidelines on outsourcing arrangements. Where applicable, reference has been made to the relevant provisions of the Union framework, as interpreted in accordance with the EBA Guidelines on outsourcing arrangements.

When discussing the relationship between supervised institutions 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. Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply.

2 Supervisory expectations

2.1 Governance of cloud services

2.1.1 Full responsibility continues to lie with the institution in question

Institutions should ensure that they establish an appropriate governance framework[5] for – and thus control and monitoring of – the outsourcing of cloud services, including 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 institution, making a clear and unambiguous allocation of responsibilities more challenging. Nevertheless, the institution's management body bears the ultimate responsibility for the management of ICT risk under Article 5(2) of DORA. To protect its information, the institution should ensure that roles and responsibilities are clearly understood and defined internally and contractually agreed when procuring cloud computing services.

The ECB understands Article 28(1)(a) of DORA as meaning that institutions which outsource ICT should apply the same level of diligence regarding risk management, processes, and controls (including ICT security) as those which decide to keep the relevant services in-house. Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls.

2.1.2 Pre-outsourcing analysis

Under Article 28(4) of DORA, institutions are required to conduct risk analysis that covers certain specified elements – termed a "pre-outsourcing analysis" – 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, institutions should:

- perform thorough analysis of the control processes that will be established;
- assess the CSP's ability to provide the information required for these checks;
- ensure that the CSP has itself properly implemented the relevant checks;
- assess whether the institution has the expertise and human resources required to implement and perform these checks;

[5] That is, a governance framework that complies with the requirements of Article 5 of DORA and Article 74 of the CRD.

- 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 a pre-outsourcing analysis to consider 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 common scenarios in a highly concentrated market);
- the risks of a multi-tenant environment.

2.1.3 Consistency between an institution's cloud strategy and its overall strategy

Under Article 28(2) of DORA, an institution must have in place a strategy that covers ICT third-party risk including the risk of outsourcing to cloud service providers. Further, Article 6(3) of DORA requires appropriate strategies to minimise the impact of ICT risk. In the ECB's opinion, this can be a specific cloud strategy or cloud aspects can be integrated into the institution's general outsourcing strategy. Given the wording of recital 45 of DORA, the ECB is of the view that any outsourcing strategy should be consistent with the institution's general strategy. At the same time, the outsourcing strategy should also be consistent with the institution's general strategy frameworks and its internal policies and processes, including as regards the management of operational and ICT risk.

2.2 Availability and resilience of cloud services

2.2.1 Holistic perspective on business continuity measures for cloud solutions

As referred to in Article 85(2) of the CRD, an institution 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. Under Article 21(2)(c) of the

NIS 2 Directive[6], measures aimed at managing risks to the security of network and information systems must include business continuity and back-up management. Article 11(1) of DORA also requires that institutions put in place a comprehensive ICT business continuity policy. When selecting a CSP – especially for the outsourcing of critical or important functions – an institution should ensure that business continuity, resilience and disaster recovery capabilities can be maintained, including for all outsourced cloud services.

The ECB understands Article 12 of DORA as meaning that institutions' response and recovery planning for cloud services involving the storage of data should include back-up procedures and restoration and recovery procedures in order to mitigate a failure of the CSP to provide services as well as the failure of the CSP as a whole, e.g., due to bankruptcy. In order to avoid jeopardising the security of network and information systems, the ECB considers that back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned. The back up procedures and restoration and recovery procedures should be tested periodically in accordance with Article 12(2) of DORA. Tests should be validated as regards the accuracy, completeness and practicality of recovery procedures.

For the purposes of Article 12(6) of DORA, the ECB understands that business continuity management (BCM) measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the institution has to perform an exit under stress or an exit without cooperation from the CSP(s) in question.

2.2.2 Proportionate requirements for critical functions

For the purposes of the requirements of Article 85(2) of the CRD and Article 6(8) of DORA, the institution should assess the resilience requirements for the cloud outsourcing services provided and the data managed and, following a risk-based approach, decide on the appropriate cloud resilience measures. Those measures may include the following:

- Multiple data centres in different geographical locations, allowing a switch to a data centre in another physical location. Having two hot-synced availability zones in the same physical location might not suffice if a function is critical. (A multi-region approach is even better, offering additional security relative to a set-up with multiple virtual zones in the same region.)
- Multiple active data centres in different availability zones within the same region, which allows the service provider to re-route services if a data centre becomes unavailable.

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

- Use of hybrid cloud architecture.
- Multiple CSPs or back-up 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 28(8) of DORA, it is the ECB's expectation that the institution will ensure that, for critical functions,[7] 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 institution's internal policies. A combination of the above measures should be used to enable the institution to remain fully operational,[8] including in cases where a failed CSP cannot provide the level of assistance that one would expect in an orderly transition under the exit plan. The institution must retain the ability to bring data and applications back on-premises. To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions.

2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy

Under the second subparagraph of Article 11(6) of DORA, financial entities' testing plans must include, among others, scenarios involving cyber-attacks and switches between the primary ICT infrastructure and the redundant capacity. Article 21(2)(c) of the NIS 2 Directive also provides that the measures taken to manage risks as required by Article 21(1) of that Directive must include, among others, business continuity, such as backup managements and disaster recovery. On the basis of these provisions, the ECB understands that an institution should test its CSP's disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications. When conducting disaster recovery tests with the CSP, the institution should perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event. The testing plan should cover a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures). These scenarios should be tested regularly in accordance with the institution's strategy and in line with its business continuity policy and requirements.

In the view of the ECB, it is good practice for personnel at the institution and the CSP who are involved in disaster recovery procedures to have designated roles and

7 As defined in paragraph 29(a) of the EBA Guidelines on outsourcing arrangements.

8 "Fully operational" means that all workflows that are necessary for the execution of critical functions can be performed as foreseen.

training, in order to ensure awareness of their responsibilities and ensure that they are capable of executing them. If joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution.

It is also good practice for any deficiencies identified during testing to be documented and analysed in order to identify corrective measures, with a remediation plan (including details of relevant roles and responsibilities) being established and monitored via the appropriate governance bodies. Such deficiencies should be addressed – for example, by renegotiating the contract with the CSP.

2.2.4 Assessment of concentration and provider lock-in risks

As referred to in paragraph 2.1.2, Article 28(4) of DORA, requires institutions to perform a risk analysis covering certain specified elements before entering into a contractual arrangement with a CSP. The ECB believes that, especially when it comes to concentration risks, it is good practice to perform such a risk assessment on a regular basis, as providers' practices and market shares may change over time. A regular review of the institution's dependence on individual service providers (including procured services that sub-outsource to specific CSPs) is strongly advisable. Concentration risks are generally 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"). These concentration risks will also need to be taken into consideration for the policy on the use of ICT services supporting critical or important functions, as set out in Article 1(h) of the proposed RTS on ICT TPPs.[9]

When performing risk assessments, the ECB considers it good practice to scrutinise 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 transparency regarding the use of sub-providers), alongside aspects of data residency. When assessing concentration risks, three main aspects may be considered: concentration in a specific provider, concentration in a specific geographical location and concentration in a specific functionality/service (also taking into account the fact that other outsourcing providers used by the supervised entity will also be reliant on the CSP's cloud services). In particular, concentration risks should be assessed not only on the basis of the number and nature of outsourced functions, but also by taking into account the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks).

[9] Draft of the Commission delegated regulation 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.

2.3 ICT security, data confidentiality and integrity

As referred to in Article 21(1) of the NIS 2 Directive, appropriate and proportionate technical, operational and organisational measures are to be taken by essential and important entities to manage risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact that incidents have on recipients of their services and on other services. As institutions effectively extend their trusted zones to the cloud environment when internal back-end systems need to communicate with cloud-outsourced applications, a careful risk assessment and a well-informed risk management decision are warranted, which should also take into account the requirements set out in Article 9 of DORA. Consequently, institutions need to protect their data (including relevant back-ups) from unauthorised access by maintaining high levels of data encryption and constantly adapting to external threats. This involves encrypting data in transit, at rest and, where feasible, in use, employing appropriate encryption methods in line with the institution's data sensitivity classification policy.

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

Institutions that outsource to the cloud continue to own their data. For that reason, it is good practice for institutions to restrict the locations where CSPs can store their data and 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, such as encryption and cryptographic key management processes

Under Article 9(4)(d) of DORA, institutions 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. The following can be regarded as best practices 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 encrypted data (i.e. generation, storage, usage, revocation, expiry and renewal), as well as the archiving of cryptographic keys, including a key access justification process that has the characteristics identified Article 9(3) of DORA.
- Details of encryption algorithms, corresponding key lengths, data flows and processing logic 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 practices.
- Encryption keys used for the encryption of institution data are unique and not shared with other users of the cloud service.

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

2.3.2 Risks stemming from the location and processing of data

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. Institutions are advised, therefore, to draw up a list of acceptable countries[10] where their data can be stored and processed, 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).

Requirements, processes and controls for the processing and storage of data should be 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 institution or on behalf of the CSP (sub-processing).

Furthermore, the ECB also considers it good practice for institutions to assess additional risks if a sub-contractor relevant for the cloud services is located in a different country from the CSP, while taking into account any risks associated with complex sub-outsourcing chains as outlined in paragraph 25 of the EBA Guidelines on outsourcing arrangements.

2.3.3 Consistent inclusion of outsourcing assets in an institution's inventory of ICT assets

The ECB considers it good practice for institutions 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 institution in every case and should support the institution'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 data protection is considered adequate on the basis of Article 45 of the General Data Protection Regulation (GDPR). The ECB advises supervised entities to use that list.

As part of this practice, an institution should, as a matter of best practice, maintain an up-to-date inventory of all the ICT assets it is responsible for 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 (IAM) policies for cloud outsourcing arrangements

Unclear roles and responsibilities as regards 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.

An institution's IAM policy should be extended to cover cloud assets and executed when entering into a cloud outsourcing arrangement. This policy should cover both technical and business users.

2.3.4.1 Roles and responsibilities

The ECB considers it good practice for institutions to agree individual clauses with the CSP when configuring the cloud environment. If this is not feasible, the institution should, as a minimum, look at how the structure provided by the CSP for the cloud services fits with the institution's roles and responsibilities to ensure the effective segregation of duties. Any deviations can then be analysed and addressed using risk mitigation measures.

2.3.4.2 Access management, remote access and authentication for users

- Users – especially those with privileged access to the system – should be clearly identified and should always be authenticated using a strong authentication solution (i.e. multi-factor authentication) when connecting to cloud systems. They should be subject to regular user access reviews. Access rights should be checked using re-certification and access withdrawal processes to prevent users from having excessive privileges, and the regularity of those processes should be in line with the criticality of the function in question. Privileged users' access should be clearly tracked in real time and reported, and access/change requests should be subject to agreed approval processes when they entail access to the institution's data. Access reviews should adopt a broad perspective, looking at in-house systems as well.
- Clear business owners should be 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) should be implemented.
- If a CSP has access to any of the institution's systems or data, this should be properly documented and monitored using appropriate monitoring tools (which should also be reviewed on a regular basis).

2.4 Exit strategy and termination rights

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

2.4.1 Termination rights

Contractual arrangements on the use of ICT services must allow the institution 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) ongoing inadequate performance, (ii) serious breaches of the contractual terms, or of the applicable law or regulations, or (iii) an excessive increase in expenses under the contractual arrangements that are attributable to the CSP.

Furthermore, the ECB understands Article 28(7) of DORA as meaning that the right of termination should also apply in cases where a reason for termination as described in the paragraph above is the result of the relocation of business units or data centres. Other changes that could also lead to such a reason for termination include (i) a merger or sale, (ii) a material change to the sub-contracting chain, (iii) relocation of the provider's headquarters to another jurisdiction, (iv) relocation of the data centre hosting to another country, or a significant change to the host country's social, political or economic climate, (v) a change to national legislation affecting the outsourcing arrangement, (vi) a change in the regulations applicable to data location and data processing, (vii) significant changes to the management of cybersecurity risk in the chain of sub-contractors, (vii) continuous failure to achieve agreed service levels or a substantial loss of service, and (ix) a failure to successfully execute cloud provider test migrations at the agreed times.

As a matter of best practices, contractual arrangements on the use of ICT services supporting critical or important functions should include a transition period in the case of termination, with the aim of reducing the risk of disruption and allowing the

switch to another provider, or the insourcing or decommissioning of the service. The ECB understands that, in order to allow for such a transition, the contract between the institution and the CSP should oblige the CSP to support a smooth and effective transition in accordance with the schedule in the agreed exit plan.

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

On the basis of the requirement concerning key contractual provisions contained in Article 30(2)(a) of DORA, institutions should ensure that all suppliers of subcontracted services supporting the CSP comply with the same contractual obligations that apply between the institution and the CSP, (including obligations relating to confidentiality, integrity, availability, the retention and destruction of data, configurations and back-ups) if termination rights are exercised.

The institution should ensure that the CSP's termination rights are aligned with the institution's exit strategy. In particular, the notice period set out in the contract with the CSP should be sufficient to allow the institution (or any third-party service provider employed by the institution 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

The ECB understands that for the purposes of compliance with the requirements set out in Article 28(8) of DORA, institutions should ensure operational resilience and mitigate relevant risks by establishing a principle-based exit strategy with granular technical exit plans for individual cloud outsourcing arrangements. Those exit plans should allow sufficient time for all the steps that need to be taken in the event of a planned or abrupt exit (including the establishment of alternative arrangements, such as moving the services in-house or finding a new provider). While BCM measures should ensure the continuity of services in the short term, exit plans should ensure continuity in the long term.

When an exit strategy focuses on moving cloud services to another CSP, the institution should draw up a list of qualified alternative service providers, reviewing and updating that list on a regular basis using market reviews (looking, for example, at the advantages and disadvantages of the various cloud outsourcing providers). Where exit strategies involve bringing services in-house or migrating them to another CSP, institutions should perform technical analysis and estimate the time required for such a transition (which should be in line with the termination dates and periods set out in the contract).

2.4.3 Granularity of exit plans

A dedicated exit plan as referred to in Article 28(8) of DORA should ensure that a supervised entity is able to react quickly to any 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 skill sets that are necessary 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 as described in Article 28(1)(b) of DORA. Supervised entities should at least perform an in-depth desktop review, ensuring that such reviews are conducted by staff who are sufficiently knowledgeable about cloud technologies. Institutions should also review the amount of data and the complexity of the applications that would need to be migrated, thinking about the potential data transfer method, in order to produce meaningful estimates of the time required. Institutions should check that they have the personnel required for their exit plans and, by conducting a walkthrough of the tasks involved, ensure that the staff available are able to perform the proposed tasks outlined in the exit plan.

For the most critical steps in the migration process, employees' ability to perform their assigned roles in the allotted time should be checked for a sample of tasks. Supervised entities should check, on a regular basis, whether the skill sets required to perform the tasks set out in their exit plans are represented among staff members, or whether external consultants would be needed in order to exit a cloud outsourcing arrangement. The feasibility of each exit plan should be independently verified (i.e. checked by someone who is not responsible for drafting the plan in question).

2.4.4 Exiting under stress

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 party. Regardless of any contractual agreement, such a termination could be caused by external events such as conflicting legislation.

In the exit strategies that are required under Article 28(8) of DORA, institutions should include a business continuity policy catering for such a situation in order to ensure that the institution is able to withstand that scenario and has access to the data required to operate the service in question.

2.5 Oversight, monitoring and internal audits

If an institution makes compromises with regard to the audit rights regime, that could lead to a situation where the institution's audit function is no longer able to conduct an independent review of an outsourcing arrangement. In many cases, CSPs do not provide sufficient detail about their infrastructure processes and their internal control systems, with the result that institutions often lack detailed first-hand knowledge of the CSP's premises, information systems, proprietary technology, sub-providers and contingency plans, as the majority of entities rely solely on the CSP's statements and third-party certifications.

The ECB understands for the purposes of compliance with Article 6(6) of DORA, the internal audit functions of the institutions should regularly review the risks stemming from the use of a CSP's cloud services. That review should cover, among other things, adequacy of the application of internal guidelines, the appropriateness of the risk assessment conducted and the quality of the provider's management. The outsourcing contract should clearly specify that the institution, its internal audit function, and the competent authorities and resolution authorities have the right to inspect and audit the CSP.

With cloud infrastructure and services becoming increasingly complex, there is an increased need to pool expertise and resources given the skills and resources required for audits and the costs involved. That expertise needs to be updated frequently given the fast pace of technological progress. An institution's internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts).

It is good practice for institutions to work together to audit a CSP, putting together a joint inspection team containing at least one technical expert from each institution. The inspection plan could be agreed by the institutions concerned on a consensual basis. If, during such a joint audit, specific issues are only relevant to a single institution, institutions should have the ability to follow up individually with the CSP on a bilateral basis. To prevent blind spots in the conduct of audits, leadership of those inspection teams should rotate among the supervised entities involved, changing every year.

2.5.1 Need for independent expert monitoring of CSPs

Under Article 6(10) of DORA, financial 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. That Article further provides that in such a case, the institution remains fully responsible for the verification of compliance with the ICT risk management requirements. The ECB understands this to mean that even where cloud services are provided as managed services, with the CSP responsible for keeping operations running and complying with security standards, accountability for verification of compliance with the ICT risk management requirements by the outsourced function cannot itself be outsourced. In order to ensure an adequate level of quality, the institution should monitor the cloud services provided by the CSP. Relying solely on monitoring tools provided by a CSP in order to assess performance might not be sufficient in the case of outsourcing of critical or important functions. In such a scenario, the monitoring tools provided should be complemented by independent tools to prevent manipulation by the CSP. In order to perform appropriate monitoring, supervised institutions should retain expertise in-house, with a centralised function or department being recommended for the monitoring of CSPs. The monitoring and oversight metrics used should give the relevant team a comprehensive overview and should be the basis for internal

reporting to the management body on the outsourcing activities of the supervised entity.

The institution should ensure that all contractual arrangements for outsourcing – including intra-group outsourcing, both with and without sub-outsourcing – take account of the reporting that is required for monitoring purposes.

2.5.2 Incident reports and contractual details

Under Article 19(5) of DORA, financial entities that decide to outsource the reporting obligations under Article 19 to a third-party service provider nevertheless remain fully responsible for the fulfilment of incident reporting requirements. The institution's oversight function should be able to follow up in detail on any incident that occurs at the CSP, with clearly defined procedures, roles and responsibilities when it comes to incident management. Reports should include relevant details to enable the identification of affected services. These reports should enable the institution to assess any potential impact on its business. All stages of the incident management process should be tracked in order to draw conclusions and learn lessons as appropriate. Institutions should use contractual clauses to ensure appropriate incident and monitoring reports, enabling ongoing assessment of outsourced functions.

2.5.3 Contractual clauses

Article 30(4) of DORA requires that when negotiating contractual arrangements, institutions and ICT third-party service providers must consider using standard contractual clauses developed by public authorities for specific services. Taking this into account, the ECB recommends that financial entities use standard contractual clauses when outsourcing cloud computing services. The specific recommendations below can be regarded as a guide to best practices in this respect:

- Contractual clauses should allow institutions to follow up on ineffective provision of services and ask for the implementation of remedial actions.
- Contractual clauses should allow institutions to monitor any deterioration in services and ask for the implementation of remedial actions.
- Contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indicating the maximum cost.
- If contractual provisions are stored online, the provider should be required to sign a separate digital or physical copy to prevent any risk of unilateral changes.

3 Annex: Table of acronyms

Acronym	
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 communication technology
NCA	national competent authority
NIS 2 Directive	Directive on measures for a high common level of cybersecurity across the Union
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).