New ECB Guidelines on Outsourcing Cloud Services

24 June 2024

Written by:Kit Burden

Introduction

The European Central Bank (ECB) has recently released a guide on the outsourcing of cloud services to cloud service providers. Whilst the ECB is at pains to stress that their guidance does NOT impose new legal obligations and specifically should be read as being subject to the detailed requirements of the EBA Guidelines on Outsourcing and the Digital Operational Resilience Act (DORA), the guidance is described as the ECB's "understanding" of those requirements as their "expectations" in relation to them. It would probably therefore be a brave person who chose to interpret the underlying regulations in a way which ran contrary to the ECB's!

So what then are the key take away's from the ECB Guidelines?

Governance

The ECB stresses the need for a robust governance framework, emphasising that the ultimately management body or board of an institution will remain responsible for the management of ICT risk, not least for the purposes of Article 5(2) of DORA. The level of governance and oversight should in particular by commensurate with that imposed in relation to functions which were retained in-house.

Pre-Outsourcing Analysis

Institutions are required to undertake thorough analyses to consider the relevant risks pertaining to outsourced cloud services; in this regard, the ECB has identified "best practice" as including an assessment of the following:

- The possibility of vendor "lock in" and challenges of moving to an alternative provider
- Data storage and processing risks
- Both physical risks and location specific risks (eg re the political stability of countries from which the cloud services will be hosted)
- Risks of drops offs in quality or "significant" increases in price
- Risks of multi tenanted environments

The mention of cost as a factor is interesting, as the regulators have largely left "commercial" issues for determination by the Institutions. They bare concerned here about the possibility of cost inflation in a "highly concentrated market" (by which we presume that they are referring to the IaaS market – which is dominated by the Hyperscalers – and the top end of the SaaS market).

Business Continuity

Business continuity continues to be a key concern of the regulatory community, as part of the wider drive to ensure operational resilience. The significance of the ECB Guidance in this regard is that they stated that in

order to maintain the security of network and information systems, back ups of critical or important services should NOT be stored in the same cloud environment which hosts the underlying services…which will likely require more back up capability to be maintained inhouse or via a secondary provider.

Insofar as the BCP tests themselves are concerned, the ECB have emphasised that the tests should include some of the most stressed scenarios, eg where an exit from the cloud services is required in circumstances where the cloud service provider is NOT still around to help out (eg to cater for their potential insolvency)

In relation to resilience more generally, the ECB has stated that resilience measures "may" include:

- Having multiple data centres in different geographies or in different availability zones
- Using hybrid cloud architecture (eg maintaining a partial private cloud environment)
- Engaging multiple cloud providers rather than just one

Much emphasis is placed upon ensuring that the retrieval of data and/or migration from a cloud provider must be able to be achieved within the maximum tolerable downtimes identified by the relevant Institutions (and as would in the UK be required to be identified for all important business services pursuant to Supervisory Statement SS1/21). This may in practice push more Institutions more in the direction of a multi provider solution

Lock In Risk

The ECB states that the analysis of concentration risk and associated potential reliance upon particular cloud service providers is not a one off activity but instead has to be repeated, not least to take account of potential changes in the overall supply chain. The three main risks the ECB has identified in this regard are:

1. Concentration of services with a particular provider;
2. Concentration in a particular geographic location; and/or
3. Concentration in a particular service or functionality (especially if dependant on a supplier's proprietary IP)

The suggestion here again is to avoid over use of single or larger providers, regardless of the price or technical benefits that such a strategy may otherwise have delivered.

Ensuring ICT/Data Security

Not surprisingly, ensuring the adequate protection and security of cloud based systems and data is squarely in the cross hairs of the ECB. This will need to include the consideration of appropriate encryption and cryptographic key management processes, all of which will need to be backed by appropriately documented policies and procedures.

Exit and Termination

The ECB Guidelines give over a considerable amount of space to the consideration of termination related concerns. Interestingly, the ECB again brings into play commercial considerations which go beyond what has been expressly stated in either the EBA Guidelines or the provisions of DORA, by also mooting that termination might be merited when there is "an excessive increase in expenses under the contractual arrangements that are attributable to the [cloud service provider]". They go on to list a series of changes to the original circumstances which "could" lead to a termination, including:

- Mergers or sales involving the cloud service provider
- Materials changes to the sub-contracting chain

- Relocation of the cloud service provider's HQ to a new geography
- Changes to data centre locations or significant changes to a host country's socio-political climate
- Changes to the underlying national legislation impacting upon the outsourced services
- "continuous failures" to meet service levels
- Failures to conduct test migrations at agreed times

In the event of such terminations, the cloud service provider must be committed to support a smooth and effective transition (which we know from experience is often not explicitly stated in the standard contract terms offered by such providers).

Significantly, the ECB expectations re subcontractors go WIDER than have been set out elsewhere in the regulations which they themselves have referred to, in that the ECB state in para 2.4.1 of their guidelines that "institutions should ensure that all suppliers of subcontracted services supporting the CSP comply with the same contractual obligations which apply between the institution and the CSP (including obligations relating to confidentiality, integrity, availability, the retention and destruction of data, configurations and back up) if termination rights are exercised" (our emphasis added). Note in particular that this goes beyond the flow downs required by the EBA Guidelines in relation to sub-outsourcings of critical or important functions.

In terms of exit planning, the ECB again offers up its view of "best practice" as to what exit plans should include, stating that this should cover:

- Critical milestones
- Tasks and skill sets required
- Estimates of time and costs likely to be required

Given the recognition of the risk of cloud service providers themselves exercising rights of suspension or termination (with such rights tending to be more far reaching than those given to suppliers in "traditional" outsourcing deals), the ECB state that business continuity planning should expressly include such "stressed" scenarios and establish that the Institution will still have the ability and data necessary to continue its operations without undue disruption.

Audit and Inspection

The ECB has expressed concern that many cloud service providers do not provide sufficient information to enable Institutions to understand their processes and controls, such that the Institutions become excessively reliant upon the service provider's own statements and third party certifications. The ECB accordingly stresses the need for the Institutions to both maintain AND exercise their own audit and inspection rights (and notes also the need for the involvement of appropriate external/third party expertise and/or the use of pooled audit resources, rather than relying solely upon the Institution's internal audit team capabilities).

Contractual Clauses

The move to more commoditised cloud services has caused difficulties for financial institutions who have been used to working off their own contract templates or at least to have significant bargaining power/leverage in the negotiation process; instead, they have found themselves having to work off the standard terms proposed by the cloud service providers, often with very limited scope for movement/compromise.

The EBA Guidelines and DORA have pushed back against this to some degree already, by mandating the inclusion of certain provisions vis a vis audit, monitoring and reporting, termination rights and sub-outsourcing (which many cloud service providers have responded to by creating standard addenda to their usual terms, as

can then be rolled out when they are contracting with a financial services entity). The ECB Guidelines have however gone further and have “recommended” that Institutions use “standard contracting clauses when outsourcing cloud computing services”. The actual content of such “standard” terms has not been set out, but the ECB has said that “best practice” in this regard would include:

- Provisions to enable Institutions to follow up on ineffective service provision and demand remedial action
- Mandatory monitoring of deterioration of services (and again to require remedial action)
- Details of how the costs of any audit would be assessed, “ideally” including a maximum cost
- The prevention of any unilateral changes of any contract terms stored online

Conclusion

Whilst much of the ECB’s Guide can be seen to be derived from and to be consistent with the provisions of the EBA Guidelines and/or DORA, there are plainly some cases where they are pushing the envelope of what those regulations might be said to (strictly speaking) require, and which may also be taken to indicate a direction of travel for the regulators, leading potentially to standardised sets of minimum required contract provisions across a broader set of clauses. In the short term we can anticipate that cloud service providers will point to the fact that the Guide is expressly stated as NOT being legally binding, but Institutions subject to the ECB’s oversight will need to be cognizant of its views – in particular to what they have expressly stated as being “best practice” – and in the case of the most important and critical services, it would be wise to treat them as being in effect mandatory (especially for those jurisdictions which require a positive grant of permission from the relevant regulatory before the proposed cloud services outsourcing can continue).

Related capabilities