On 20 December 2017, the European Banking Authority (EBA) issued its Final Report on the Recommendations on outsourcing to cloud service providers (Recommendations) covering five key areas:

- the security of data and systems;
- the location of data and data processing;
- access and audit rights;
- chain outsourcing (i.e. supply chain and subcontracting); and
- contingency plans and exit strategies.

In order to clarify EU-wide supervisory expectations, the European Banking Authority has published its final guidance for the use of cloud service providers by financial institutions.

The guidance, which has a strong focus on risk management, builds on existing outsourcing Guidelines developed by the Committee of European Banking Supervisors and is intended to provide additional clarity on (and encourage the take-up of) cloud computing by credit institutions and investment firms.

The guidance will also foster supervisory convergence across the EU in this field.

Financial institutions should take note of, and make every effort to comply with, the European Banking Authority’s new cloud computing guidance which will be effective from 1 July 2018.
The Recommendations, which were developed in accordance with Article 16 of the EBA Regulation (Regulation (EU) No 1093/2010), which mandates the EBA to issue guidelines and recommendations for competent authorities to establish consistent, efficient and effective supervisory practices and to ensure the common, uniform and consistent application of European Union law, will take effect on 1 July 2018 and are part of the EBA’s broader work on FinTech. The Recommendations build on the Committee of European Banking Supervisors’ December 2006 outsourcing guidelines (CEBS Guidelines) which should be read together with the Recommendations.

The EBA says that whilst “cloud services can offer a number of advantages, such as economies of scale, flexibility, operational efficiencies and cost-effectiveness, they also raise challenges in terms of data protection and location, security issues and concentration risk, not only from the point of view of individual institutions but also at industry level, as large suppliers of cloud services can become a single point of failure when many institutions rely on them.”

Principles-based Guidance
The Recommendations are, for the most part, principles-based and as such are written at a high level. During the consultation stage, some respondents argued for a more detailed, prescriptive approach, however, the EBA’s stance enables each firm to take into account its own policies and procedures, IT infrastructure and organisational design, as well as industry best practices, when selecting and contracting for cloud computing and other cloud services.

The Recommendations apply to credit institutions and investment firms as defined in Article 4(1) of Regulation (EU) No 575/2013 (Capital Requirements Regulation – CRR). They are subject to the “principle of proportionality” and should be implemented in a manner which is “proportionate to the size, structure and operational environment of the institution, as well as the nature, scale and complexity” of the institution’s activities.

Material Outsourcing
In line with the CEBS Guidelines, it is the “materiality” of the planned cloud outsourcing which determines whether an institution has to inform its competent authority before proceeding. Only material cloud outsourcings will need to be notified whereas, currently, some EU supervisors require notification of non-material cloud outsourcings as well. The Recommendations provide detail of what needs to be notified and how.

Prior to any outsourcing, an assessment of the materiality of the proposed activities for outsourcing should be carried out on the basis of guideline 1(f) of CEBS Guidelines. In the context of the cloud, the following should also be considered:
In addition, each institution must also maintain a register of all cloud outsourcings, material and non-material. Information from the register, together with a copy of the cloud outsourcing agreement, should be made available to the regulatory authority on request.

The Five Key Areas

Security of Data and Systems

Cloud computing is singled out as a special case with the Recommendations providing guidance on the security of the data and systems used beyond the general requirements of the CEBS Guidelines. For instance, prior to any cloud outsourcing, the institutions should “define and decide on an appropriate level of protection of data confidentiality, continuity of activities outsourced, and integrity and traceability of data and systems in the context of the intended cloud outsourcing. Institutions should also consider specific measures where necessary for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture.” The written contract should record the agreement reached on these items, and, in line with the CEBS Guidelines, these aspects should be monitored on an ongoing basis so as to enable prompt action where any corrective measures are required.

Location of Data and Data Processing

Given the way in which cloud computing offers location-agnostic environments and the related data protection risks and risks to effective supervision by the supervisory authority, special care is needed, in line with the CEBS Guidelines, where personal data will be hosted outside the EEA. In the context of the cloud, the Recommendations require institutions to adopt a risk-based approach to data and data location considerations when moving to a third party’s cloud environment and to implement adequate controls and measures, such as the use of encryption technologies for data in transit, data in memory and data at rest.

Access and Audit Rights

The right to access, inspect and audit is a key principle as set out in the CEBS Guidelines. Cloud contracts must secure both the right to audit for institutions (including third parties they appoint for these purposes and their statutory auditors) and the right of physical access to the business premises of cloud service providers, and the exercise of these rights should not be impeded or limited by the contract’s terms. If the performance of audits or the use of certain audit techniques might create a risk for another client’s environment (i.e. in a multi-tenant environment), alternative ways to provide a similar level of assurance...
should be agreed and set out in the contract. The Recommendations provide various suggestions on this
point, including the use of third-party certifications and audit reports. The contract must also provide
unrestricted rights of access and audit for the competent authority supervising the outsourcing institution.

**Chain Outsourcing**
Specific requirements are set by the Recommendations for institutions in order to mitigate the risks
associated with “chain” outsourcing, i.e. where the cloud service provider subcontracts elements of the
service to other providers. The use of subcontractors by the cloud service provider should not affect the
services provided under the outsourcing agreement (i.e. the provider must retain the prime responsibility
for all services whether self-performed or subcontracted).

The institution must be notified of planned significant changes to subcontractors or subcontracted services
and have the right to terminate the cloud contract if the planned changes to subcontracted services would
have an adverse effect on the risk assessment of the outsourced services. The contract should specify any
types of activities that are excluded from potential subcontracting, and list the subcontractors or the
subcontracted services they provide.

**Contingency Planning and Exit**
Contingency plans and exit strategies form an important part of any cloud outsourcing arrangement. The
Recommendations require that the outsourcing contract includes an obligation on the cloud service
provider to sufficiently support the institution in the orderly transfer of the activity, data or services from
the subcontractor to another service provider or to the direct management of the institution in the event of
termination. The Recommendations also provide guidance for institutions on the contractual and
organisational arrangements for contingency plans and exit strategies that should be in place in the context
of cloud outsourcing.

**MiFID II**
In relation to institutions offering investment services, the EBA analysed the Recommendations to ensure
that they are fully consistent with the relevant provisions of MiFID II on outsourcing (in particular Article
16) and the related implementing regulation.

**Final Remarks**
The EBA has been busy of late, the Recommendations coming fast on the heels of the EBA’s Final
Report on the Guidelines on the security measures for operational and security risks of payment services,
which also cover outsourcing and, by implication cloud computing, this time in the context of the Payment

The cloud computing Recommendations strive to address the perception that firms are not adopting cloud
services due to a lack of clarity about the applicable regulatory requirements on an EU-wide basis, whilst
ensuring that risks are appropriately identified and managed. UK firms will also be aware that the Financial Conduct Authority published its own guidance on outsourcing to the cloud back in July 2016. Whilst the Recommendations do not set out a clear set of standards that institutions can comply with, what is clear is that the EBA has sought to address some of the lack of clarity that has often been seen as a key barrier preventing the outsourcing to cloud service providers.

Next steps for institutions looking to implement cloud computing include updating procurement policies, contractual templates and clauses in line with the Recommendations. Where applicable, existing cloud computing deals should also be reviewed and, where appropriate, terms should be renegotiated.