Comparison of FCA, CEBS and EBA Guidelines on Outsourcing			
	FCA Guidance for firms outsourcing to the "cloud" and other third-party IT services ("FCA Guidelines")	**CEBS Guidelines on Outsourcing ("CEBS Guidelines")**	**EBA Draft Guidelines on Outsourcing arrangements ("EBA Guidelines")**
Application of Guidelines	Firms authorised under FMSA other than: banks, building societies, designated investment firms or IFPRU investment firms.	Credit institutions	Credit institutions; and now Investment firms (subject to CRD); Payment institutions; and Electronic money institutions.
Governance Framework			
Governance requirements	Firms retain full accountability for discharging all of their responsibilities under the regulatory system and cannot delegate responsibility to the service provider. Importantly, services should be organised in such a way that they do not become a barrier to the resolution or orderly wind-down of a firm, or create additional complexity in a resolution.	Ultimate responsibility lies with senior management.	Ultimate responsibility remains with Senior Management. Additional requirements of Payment and Electronic Money Institutions: to ensure regulatory compliance and designate senior staff member to monitor outsourcing arrangements.
further detail	At a high level, a firm should: • be clear about the service being provided and where responsibility and accountability between the firm and its service provider(s) begins and ends; • allocate responsibility for the day-to-day and strategic management of the service provider; • ensure staff have sufficient skills and resources to oversee and test the outsourced activities; identify, monitor and mitigate against the risks arising; and properly manage an exit or transfer from an existing third-party provider; and verify that suitable arrangements for dispute resolution exist.	**Guideline 2** The ultimate responsibility for the proper management of the risks associated with outsourcing or the outsourced activities lies with an outsourcing institution's senior management. 1. All outsourcing regimes should ensure that the outsourcing of functions to an outsourcing service provider does not impair the supervision of the outsourcing institution. 2. Responsibility for outsourced functions must always be retained by the outsourcing institution. The outsourcing of functions does not relieve an outsourcing institution of its regulatory responsibilities for its authorized activities or the function concerned. 3. Outsourcing institutions should be required to retain adequate core competence at a senior operational level in house to enable them to have the capability to resume direct control over an outsourced activity, in extremis. 4. Outsourcing shall not affect managers' full and unrestricted responsibilities under applicable legislation (e.g. under banking law). **Guideline 3** Outsourcing arrangements can never result in the delegation of senior management's responsibility. • The outsourcing of core management functions is considered generally to be incompatible with the senior management's obligation to run the enterprise under their own responsibility. Core management functions include, inter alia, setting the risk strategy, the risk policy, and, accordingly, the risk-¬bearing capacity of the institution. Hence, management functions such as the setting of strategies and policies in respect of the authorised entity's risk profile and control, the oversight of the operation of the entity's processes, and the final responsibility towards customers and supervisors should not be outsourced.	**Guideline 3** Outsourcing of functions cannot result in the delegation of the management body's or bodies' responsibilities. Institutions and payment institutions remain fully responsible and accountable for complying with all of their regulatory obligations. In particular, the ability to oversee the outsourcing of critical or important function must always be retained by the institution and the payment institution. The management body is at all times fully responsible and accountable for at least: 1. ensuring that the institution or the payment institution meets on an on-going basis the conditions with which it must comply in order to remain authorised, including any conditions imposed by the competent authority; 2. the internal organisation of the institution or the payment institution; 3. the identification, assessment and management of conflicts of interest; 4. the setting of the institution's or payment institution's strategies and policies (e.g. the business model, the risk appetite, the risk management framework); 5. the day to day management of the institution or payment institution, including the management of risks associated with the outsourcing; and 6. the oversight role of the management body in its supervisory function. Institutions and payment institutions should: a) clearly assign the responsibilities for the documentation and control of outsourcing arrangements; b) allocate sufficient resources to ensure compliance with the regulatory requirements, including these guidelines, the documentation and monitoring of all outsourcing arrangements; and c) establish an outsourcing function or designate a senior staff member (e.g. Key Function Holders) who is directly accountable to the management body or at least ensure a clear division of task and responsibilities for the monitoring of outsourcing arrangement.
Policy and Procedure Requirements			
	Firms should have in place appropriate arrangements to ensure it can continue to function and meet its regulatory requirements in the event of unforeseen interruption of the outsourced serviced. Firms also need to have a comprehensive change management process and exit strategy in place.	Clear policies on approach to outsourcing, including contingency and exit plans. Outsourcing institutions required to conduct business in controlled/sound manner.	Stronger approach - outsourcing policy to be approved and maintained, and implemented at all levels of the business. Institutions and Payment Institutions to ensure policy covers potential effects on risk profile. Contingency and Exit strategies to be developed separately.
	Firms should: • consider the likelihood and impact of an unexpected disruption to the continuity of its operations	**Guideline 6**	**Guideline 4**
Restrictions on outsourcing			
		Authorisation required from supervisory authority, excluding non-material outsourcing.	No authorisation required from supervisory authority. Institutions and Payment Institutions to ensure continuity and contingency arrangements are in place.
		Guideline 4 4.1 An authorised entity may not outsource services and activities concerning the acceptance of deposits or to lending requiring a licence from the supervisory authority according to the applicable national banking law unless the outsourcing service provider either (i) has an authorisation that is equivalent to the authorisation of the outsourcing institution; or (ii) otherwise allowed to carry out those activities in accordance with the relevant national legal framework. 4.2 Any area of activity of an outsourcing institution other than those identified in Guidelines 2 and 3 may be outsourced provided that such outsourcing does not impair: 1. the orderliness of the conduct of the outsourcing institution's business or of the financial services provided; 2. the senior management's ability to manage and monitor the authorised entity's business and its authorised activities; 3. the ability of other internal governance bodies, such as the board of directors or the audit committee, to fulfil their oversight tasks in relation to the senior management; and 4. the supervision of the outsourced institution. 4.3 An outsourcing institution should take particular care when outsourcing material activities. The outsourcing institution should adequately inform its supervisory authority about this type of outsourcing.	No restrictions set out within EBA guidelines.
Non-material outsourcing		**Guideline 5** There should be no restrictions on the outsourcing of nonmaterial activities of an outsourcing institution. In such cases the outsourcing institution does not need to adequately inform its supervisory authority.	Objective 35 of the EBA Guidelines confirms that institutions and payment institutions need to have business continuity and contingency arrangements in place to ensure that their material business activities can be performed on a continuous basis. It follows that the guidelines are not intended to apply to non-material services.
Contractual and Due Diligence Requirements			
	Before acceptance, Firms should review the contract with the outsource provider to ensure it complies with the FCA requirements, in doing so a Firm may wish to take account of the provider's adherence to international standards. The fundamental principle is that Firms should identify and manage any risks introduced by their outsourcing arrangements.	All outsourcing arrangements subject to a formal & comprehensive contract. Outsourcing institutions also requitred to have written agreement in place, outlining key responsibilities of both parties.	Institutions and Payment Institutions required to perform pre-contractual due diligence. More detailed written agreement required, meeting minimum standards. Provisions required to be agreed permitting sub-outsourcing. Additional access, information, audit and termination rights.Institutions and Payment Institutions now also required to maintain a register detailing all outsourcing arrangements.

Requirement to conduct pre- contractual due diligence	A firm should: • have a clear and documented business case or rationale in support of the decision to use one or more service providers for the delivery of critical or important operational functions or material outsourcing • ensure the service is suitable for the firm and consider any relevant legal or regulatory obligations, including where a firm is looking to change their existing outsourcing requirements • as part of the due diligence exercise, ensure that in entering into an outsource agreement, it does not worsen the firms operational risk • consider the relative risks of using one type of service over another e.g. public versus private 'cloud' • maintain an accurate record of contracts between the firm and its service provider(s) • know which jurisdiction the service provider's business premises are located in and how that affects the firm's outsource arrangements • know whether its contract with the service provider is governed by the law and subject to the jurisdiction of the United Kingdom. If it is not, it should still ensure effective access to data and business premises for the firm, auditor and relevant regulator (see below sections on access to data and business premises) • consider any additional legal or regulatory obligations and requirements that may arise such as through the General Data Protection Regulation (GDPR). • where these are related to the regulated activity being provided, identify all the service providers in the supply chain and ensure that the requirements on the firm can be complied with throughout the supply chain. Similarly, where multiple providers form part of an overall arrangement (as distinct from a chain) the requirements should be complied with across the arrangement. Firms should also: carry out a risk assessment to identify relevant risks and identify steps to mitigate them • • document this assessment • identify current industry good practice, including data and information security management system requirements, cyber risks, as well as the relevant regulator's rules and guidance to then use this to support its decision making • review whether the legal and regulatory risks differ if the customers, firms and employees involved in providing or using the services are in different geographic or jurisdictional locations e.g. UK, EEA or non-EEA • assess the overall operational risks associated with the regulated service for which the firm is responsible and assign responsibility for managing them • monitor concentration risk and consider what action it would take if the outsource provider failed10 • require prompt and appropriately detailed notification of any breaches or other relevant events arising including the invocation of business recovery arrangements • ensure the contract(s) provide for the remediation of breaches and other adverse events.		**Guideline 9** Before entering into any outsourcing arrangement, institutions and payment institutions should: a) assess whether the planned outsourcing concerns a critical or important function; b) undertake appropriate due diligence on the prospective service provider; c) identify and assess all relevant risks of the outsourcing arrangement; d) identify and assess conflicts of interest that the outsourcing may cause; e) consider the consequences of where the service provider is located (within or outside the EU); f) consider whether the service provider is part of the institution's accounting consolidation group and, if so, the extent to which the institution controls it or has the ability to influence its actions.
Requirement for a written contract		**Guideline 8** All outsourcing arrangements should be subject to a formal and comprehensive contract. The outsourcing contract should oblige the outsourcing service provider to protect confidential information. 1. Any outsourcing arrangement should be based on a clear written contract. 2. An outsourcing institution should make sure that the written contract takes account of the following (bearing in mind other specific national rules and legislation): **Guideline 9** In managing its relationship with an outsourcing service provider an outsourcing institution should ensure that a written agreement on the responsibilities of both parties and a quality description is put in place. 1. A written agreement should normally contain a mixture of quantitative and qualitative performance targets, to enable an outsourcing institution to assess the adequacy of service provision. 2. An outsourcing institution should also consider the need to evaluate the performance of its outsourcing service provider using mechanisms such as service delivery reports, self-certification or independent review by the outsourcing institution's, or the outsourcing service provider's, internal and/or external auditors. 3. An outsourcing institution should be prepared to take remedial action if the outsourcing service provider's performance is inadequate.	**Guideline 10** The respective rights and obligations of the institution, the payment institution and of the service provider should be clearly allocated and set out in a written agreement. The outsourcing agreement should set out at least for all outsourcing arrangements: a) a clear description of the outsourced function; b) the start and end dates of the agreement, including notice periods; c) the governing law of the outsourcing arrangement; d) whether the sub-outsourcing of a critical or important function is permitted and if so, the agreement should ensure that the sub- outsourcing is subject to conditions specified in Section 10.1; e) the location(s) where the critical or important function will be provided and/or where relevant data will be kept, including the possible storing locations, and processed and the conditions to be met, including a requirement to notify the institution or the payment institution if the service provider proposes to change the location(s); f) where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as further specified in Section 10.2 **Guideline 10.1** (Sub-outsourcing of critical or important functions) The outsourcing agreement should specify whether or not sub-outsourcing of critical or important function is permitted. If so, it should: a) specify any types of activities that are excluded from sub-outsourcing; b) specify the conditions to be complied with in the case of sub-outsourcing; c) specify that the service provider is obliged to oversee those services that it has sub- contracted in order to ensure that all contractual obligations between the service provider and the institution or the payment institution are still met; d) require the service provide to obtain prior approval from the institution and the payment institution before sub-outsourcing data subject to the GDPR; e) include an obligation for the service provider to inform the institution or the payment institution of any planned sub-outsourcing, or material changes thereto, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes to the sub-contractors and the respective notification period;

			f) the notification period to be set under point (e) should allow the outsourcing institution and payment institution to carry out a risk assessment of the proposed changes before the changes come into effect; g) ensure, where appropriate, that the institution or the payment institution has the right to object against intended sub-outsourcing or that an explicit approval is required; h) ensure that the institution or payment institution have the contractual right to terminate the agreement in case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the institution and the payment institution or where the service provider sub-outsources without notifying the institution or the payment institution. Institutions and payment institutions should only agree to sub-outsourcing, if the sub-contractor undertakes to: a) comply with all applicable laws, regulatory requirements and contractual obligations; and b) grant the institution, payment institution and competent authority the same contractual rights of access and audit as those granted by the service provider. **Guideline 10.2** (Security of data and system) Institutions and payment institutions should ensure that service providers, where relevant, comply with appropriate information security standards. **Guideline 10.3** (Access, information and audit rights) Institutions and payment institutions should ensure, within the written outsourcing agreement, that the service provider grants them and their competent authorities and any other person, including the statuary auditor, appointed by the institution, the payment institution or the competent authorities the following: a) complete access to all relevant business premises (head offices and operations centers'), including the full range of devices, systems, networks, information and data used for providing the outsourced process, service or activity, financial information, personnel and the service provider's external auditors ('access rights'); and b) unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to comply with all applicable regulatory requirements. **Guideline 10.4** (Termination rights) The outsourcing arrangement should expressly allow the possibility for the institution or payment institution to terminate it, in accordance with national law, including in the following situations: a) the provider of outsourced services is in a breach of applicable law, regulation, or contractual provisions; b) identified impediments capable to alter the performance of the outsourced service; c) there are material changes affecting the outsourcing arrangement or the service provider (such as sub-outsourcings or changes of sub- contractors); d) there are weaknesses regarding the management and security of confidential data, personal data or otherwise sensitive data and information; and e) instructions of the institution or payment institution's competent authority, e.g. in the case that the competent authority is not in the position to effectively supervise the institution or the payment institution. The outsourcing arrangement should facilitate the transfer of outsourced function to another service provider or the reincorporation into the institution or the payment institution. To this end the written outsourcing arrangement should: a) set an appropriate transition period, during which the service provider would continue to provide the outsourced function, to reduce the risk of disruptions; b) clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or to the institution or payment institution, including the treatment of data; and c) include an obligation on the service provider to support the institution or payment institution in the orderly transfer of the activity in the event of the termination of the outsourcing agreement.
Requirement to maintain an outsourcing register			**Guideline 8** Institutions and payment institutions should maintain a register of all outsourcing arrangements at institution and group level and document and record all current outsourcing arrangements, distinguishing the outsourcing of critical or important functions and other outsourcing arrangements.
Implementation, monitoring and management of outsourcing arrangements			
	Firms should have effective access to data related to the outsourced activities, as well as to the business premises of the service provider.	Outsourcing Institutions should manage the risks with outsourcing arrangements through ongoing assessments.	More stringent requirements in place. Internal auditry functions now required to cover minimum standards. Outsourcing Institutions required to report periodically to management function on the performance of ongoing outsourcing arrangements, covering sub-outsourcing and regular pre-contractual risk assessment updates. Additional requirement for Institutions and Payment Institutions to maintain register detailing all outsourcing arrangements and this register to be made available in a common format for review and evaluation process, or upon request from competent authority. Additional activity reporting requirements.

Audit requirements	A firm should: • ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive • ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data • advise the service provider that the regulator will not enter into a nondisclosure agreement with the service provider but will treat any information disclosed in accordance with the confidentiality obligation set out in FSMA • ensure that, where a firm cannot disclose data for any reason, the contract enables the regulator or the firm's auditor to contact the service provider directly • ensure that data are not stored in jurisdictions that may inhibit effective access to data for UK regulators. Considerations should include the wider political and security stability of the jurisdiction; the law in force in the jurisdiction in question (including data protection); and the international obligations of the jurisdiction14. This should include consideration of the law enforcement provisions within a jurisdiction. • be able to request an onsite visit to the relevant business premises, in accordance with applicable legal and regulatory requirements. This right should not be restricted. • a regulator visit to an outsource provider's business premises will only take place if the regulator deems it necessary and required under applicable legal and regulatory requirements. Firms should not stipulate further conditions beyond this.		**Guideline 7** The internal audit function's activities should cover, following a risk based approach, the independent review of outsourced activities. The audit plan and programme should include in particular the outsourcing arrangements of critical or important function, including the appropriateness of data protection measures, controls, risk management and business continuity measures implemented by the service provider. With regard to outsourcing, the internal audit function should at least ascertain: a) that the institutions and payment institutions framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulation, the risk appetite and with the decisions of the management body; b) the adequacy, quality and effectiveness of the assessment of the criticality or importance; c) the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain within the risk appetite; d) the risk appetite, risk management and control procedure of the service provider are in line with the institution's or payment institutions' strategy; e) the appropriate involvement of governance bodies; and f) the appropriate monitoring and management of outsourcing arrangements.
Ongoing monitoring requirements		**Guideline 7** An outsourcing institution should manage the risks associated with its outsourcing arrangements. • Compliance with this Standard should include an on going assessment by the outsourcing institution of the operational risks and the concentration risk associated with all its outsourcing arrangements. An outsourcing institution should inform its supervisory authority of any material development.	**Guideline 11** Institutions and payment institutions should monitor on an ongoing basis the performance by the service provider and, where applicable sub-contractors, with regard to all outsourcing arrangements with a particular focus on the outsourcing of critical or important functions, including that the availability, integrity and security of data and information is ensured. Institutions should regularly update their pre contractual risk assessment and periodically report to the management body on any risks identified in respect of outsourcing of critical or important function. Institutions and payment institutions should monitor and manage their own concentration risk caused by outsourcing arrangements. Institutions and payment institutions should ensure that outsourcing arrangements meet appropriate performance and quality standards in line with their policies on an ongoing basis by: a) ensuring they receive appropriate reports from service providers; b) evaluating the performance of service providers using tools such as key performance indicators (KPIs), key control indicators (KCIs), service delivery reports, self-certification and independent reviews; and c) reviewing all other relevant information, including reports on business continuity measures and testing, received from the service provider.
Record keeping requirements / Duty to adequately inform supervisors			**Guideline 13** Institutions and payment institutions should make available the register of all existing outsourcing arrangements to the competent authority in a common data base format within each supervisory review and evaluation process, but at least every 3 years and in any case on request by competent authority. Institutions and payment institutions should adequately inform competent authorities in a timely manner of the following: • planned outsourcing of critical or important functions, including the outsourcing of critical or important cloud services, before they intend to enter into the new outsourcing agreement; • if a function under an existing outsourcing arrangement becomes critical or important; and • any material changes and severe events regarding their outsourcing arrangements which could have a material impact on the continuing provision of its services.
Supervisory Oversight			
		Supervisory authorities to consider associated risks and have access to Outsourcing Institution data and premises.	No further requirement for supervisory oversight.

		Guideline 10 10.1 Supervisory authorities should take account of the risks associated with “chain” outsourcing. 10.2 The supervisory authority should agree to chain outsourcing only if the subcontractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider, including obligations incurred in favour of the supervisory authority. 10.3 The outsourcing institution should take appropriate steps to address the risk of any weakness or failure in the provision of the subcontracted activities having a significant effect on the outsourcing service provider's ability to meet its responsibilities under the outsourcing 1. The sub-outsourcing of outsourced activities and functions to third parties (subcontractors) should be treated by the outsourcing institution like a primary outsourcing measure. Compliance with these conditions should be ensured contractually, for example by a clause in the outsourcing contract requiring the prior consent of the outsourcing institution to the possibility and the modalities of sub outsourcing. 2. The outsourcing institution should ensure that the outsourcing service provider agrees that the contractual terms agreed with the subcontractor will always conform, or at least not be contradictory, to the provisions of the agreement with the outsourcing institution. **Guideline 11** Supervisory authorities should require that the outsourcing institution has established supervisory authority access to relevant data held by the outsourcing service provider and, where provided for by national law, the right for the supervisory authority to conduct onsite inspections at an outsourcing service provider's premises. **Guideline 12** Supervisory authorities should take account of concentration risk. 1. Supervisory authorities should seek to identify any concentration risk on a sectoral level and seek to monitor these risks at a systemic level.	