Cloud Compliance Center - United Kingdom

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

UNITED KINGDOM

*This content was last reviewed around April 2023.*

**Cloud friendly**

**1. Are financial institutions legally permitted to use cloud services?**

Yes, there is no prohibition on using cloud services under applicable regulatory laws.

**2. Are there any rules which apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

Yes, all regulated entities in the UK must comply with the Financial Conduct Authority ("**FCA**") Handbook when using cloud services. The FCA recognizes that these requirements should be enforced in a risk-based and proportionate manner considering the scale and complexity of the services.

Chapter 8 of the FCA's Senior Management Arrangements, Systems and Controls sourcebook ("**SYSC 8**") provides that a firm must ensure that it takes reasonable steps to avoid undue operational risk. Firms cannot outsource operational functions that would impair the quality of internal controls or the regulator's ability to monitor its compliance.

In addition, where the cloud services are considered as the outsourcing of critical or important functions, firms must exercise skill, care and diligence in selecting, managing and terminating those outsourcing arrangements. In particular, the institution must take steps to ensure that the service provider fulfills the following:

Has sufficient capacity and capability to deliver the outsourced function

Carries out the services effectively and compliantly, and in a way that the firm can assess on an ongoing basis

Supervises the outsourced functions and manages risk

Discloses developments that have material impacts on the service provider's ability to perform the function

Grants effective audit rights

Protects confidential information

Establishes and implements business continuity and disaster recovery plans and appropriate exit arrangements

Allows the firm to terminate the arrangement where necessary

Where firms are dual regulated (e.g., banks, large investment firms and insurers), the provisions of the FCA Handbook and the Prudential Regulation Authority ("**PRA**") Rulebook apply.

Similar to the FCA Handbook, the PRA Rulebook specifies a number of high-level "fundamental rules" that firms have to comply with, including obligations to act in a prudent manner, have effective risk strategies and to control their affairs responsibly.

Section 2 of the Outsourcing Part of the PRA Rulebook has rules that are broadly consistent with those set out in SYSC 8.1.1R of the FCA Handbook.

The PRA Rulebook also incorporates Articles 30-31 of Commission Delegated Regulation (EU) 2017/565 (Retained EU Legislation) ("**MIFID Organization Regulation**") and applies these rules to all firms regulated by the PRA. These obligations broadly reflect the SYSC 8 obligations.

**PRA SS2/21 on "Outsourcing and third-party risk management" implementing the EBA Guidelines on Outsourcing**

Despite Brexit, the FCA expects firms to continue to comply with the guidelines on outsourcing (including cloud) that were published by the European Banking Authority ("**EBA**") in February 2019.

The EBA guidelines apply to a broad range of regulated institutions, including banks and investment firms, but not asset management firms. The EBA guidelines identify the steps that firms must take to conduct outsourcing activity in a compliant manner (e.g., including due diligence requirements, notification to a regulator of material outsourcings and internal governance obligations).

The PRA has published a Supervisory Statement SS2/21 on Outsourcing and third-party risk management, which took effect from 31 March 2022. It complements the requirements and expectations on operational resilience in the PRA Rulebook, seeks to facilitate greater resilience and adoption of the cloud and other new technologies and implements (and expands) the EBA guidelines.

**PRA SS2/21 on "Outsourcing and third-party risk management" implementing the EBA Guidelines on ICT and Security Risk Management**

The EBA has established information and communication technology and security risk management guidelines that supplement the EBA Guidelines on Outsourcing.

The FCA has confirmed that these continue to apply in the UK. PRA Supervisory Statement SS2/21 implements relevant sections of these ICT guidelines from 31 March 2022.

The ICT guidelines focus on organizational measures that regulators expect firms to have in place. For example, there are requirements to establish sound internal governance processes and an ICT strategy that is aligned with the firm's overall business strategy.

**PRA expectations in SS2/21 regarding the cloud**

Certain sections of SS2/21 refer specifically to the use of cloud services by regulated firms, setting out the PRA's expectations that regulated firms implement robust controls for data-in-transit, data-in-memory and data-at-rest. Guidance and expectations in respect of outsourcing to cloud services include the following:

The shared responsibility model — firms are expected to define, document and understand their and the cloud service provider's respective responsibilities.

The PRA expects all firms to keep records of their outsourcing arrangements.

In material outsourcing arrangements, the PRA expects firms to retain contractual rights to perform onsite audits at their discretion.

Firms are expected to assess business continuity for material cloud outsourcing arrangements.

Outsourcers are expected to take reasonable steps to test exit plans, especially "stressed" exits.

Since 31 December 2021, under the EBA Outsourcing Guidelines banks are expected to maintain a register of their cloud outsourcing arrangements.

In June 2022, HM Treasury issued a policy statement on "Critical third parties to the finance sector." The policy statement proposed a framework to enable financial regulators to manage the risks to financial stability posed by unregulated parties providing critical services to regulated entitles, including cloud-based computing services. Under the proposed regime, HM Treasury will — in consultation with the financial regulators — be able to designate certain third parties that provide services to firms as "critical third parties" ("**CTPs**"). The financial regulators will then be able to make rules, gather information and take enforcement action, in respect of certain services that CTPs provide to firms of particular relevance to the regulators' objectives (i.e., "material" services). Following publication of the policy paper, the Financial Services and Markets Bill ("**FSM Bill**") was introduced in parliament on 20 July 2022; the FSM Bill sets out a statutory framework for managing systemic risks posed by CTPs through direct regulatory oversight and operational resilience requirements. At the time of writing, the FSM Bill has not completed its passage through parliament, and there is no timescale for it to receive royal assent.

**3. Are there any specific contractual requirements for cloud outsourcing?**

Under the Financial Conduct Authority's ("**FCA**") Senior Management Arrangements, Systems and Controls sourcebook ("**SYSC**") at SYSC 8.1.9R, firms must ensure that the parties' rights and obligations are clearly allocated and described in a written agreement. Aside from that requirement, SYSC 8 does not contain any other requirements regarding the contractual arrangements firms must undertake when performing an outsourcing.

The European Banking Authority ("**EBA**") guidelines are more prescriptive and set out specific matters that must be addressed in a written contract between the firm and the services provider. Some of the contractual requirements are dealt with briefly and are of the type one commonly sees in any commercial agreement, for example, a clear description of the outsourced function, term, the governing law, financial obligations, service levels, information about whether the service provider has taken out insurance, requirement to implement and test business continuity and disaster recovery (BCDR) plans, and reporting obligations when material impacts affect the service provider's ability to carry out the services.

Other contractual requirements are more specific to the regulated nature of the institution, including that the contract should specify the following:

Whether the sub-outsourcing of a critical or important function is permitted; if the sub-outsourcing of a critical or important function is permitted, the agreement must specify the following:

What types of activities are excluded from the sub-outsourcing

Any conditions that must be complied with

That the service provider is responsible for the activities of their sub-outsourcers

That the service provider must inform the institution of any planned sub-outsourcing or material changes, and that the institution can object to this

That the institution has the right to terminate in the event of any undue sub-outsourcing (e.g., where the risks are materially increased for the institution without prior notification)

The locations where the critical or important function will be provided and/or where relevant data will be kept and processed, and a requirement that the service provider notifies the firm if it intends to change this during the term

The accessibility, availability, integrity, privacy and safety of relevant data (institutions must define data and system security requirements within the agreement)

That the institution can monitor the service provider's performance on an ongoing basis

That the data owned by the institution can be accessed by the institution in the event of the service provider's insolvency

That the service provider cooperates with competent authorities

That the institution can rely on its rights under the Bank Recovery and Resolution Directive regimes that apply to it in a resolution or ring-fencing scenario

The unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider; the EBA guidelines are expressed as requiring a risk-based approach to audit, but where there is the outsourcing of a critical or important function then they specifically require the following:

The service provider to grant full access to all relevant business premises and devices, systems, networks and data used for providing the outsourced function

Unrestricted inspection and auditing rights to ensure compliance with regulatory and contractual requirements

Contractual arrangements cannot limit the effective exercise of audit rights by the institution, competent authority or third parties appointed by them. Where relevant, commonly accepted audit standards should be applied, although it is permissible to use pooled audits and third-party certifications to allow more efficient audit processes to take place. Generally, institutions must give prior notice of the audit, but not where there is an emergency or crisis situation or the audit would not be effective. The EBA guidelines also recognize that care must be taken when performing audits in multitenanted environments to ensure that risks for other clients are avoided or mitigated. There is also a separate requirement for the service provider to subject its internal audit reports to the institution as appropriate, and specific termination rights are required where any of the following apply:

The service provider breaches applicable law or the contract.

Impediments capable of altering the performance of the outsourced function are identified.

There are material changes affecting the outsourcing arrangement or service provider (e.g., change of subcontractors).

There are weaknesses regarding the management and security of confidential, personal or other sensitive information.

The competent authority requires this.

The outsourcing agreement must also clearly set out the obligations of the service provider where there is to be an exit and transfer to a successor supplier, set out an appropriate transition period to minimize disruption and set out an obligation on the service provider to support an orderly transfer of the outsourced function following the termination.

The EBA's ICT guidelines state that firms are required to ensure the following in their contracts:

Appropriate information security related objectives and measures (e.g., minimum cybersecurity requirements, location of data centers, encryption requirements, monitoring processes and data retention policies)

Incident handling processes, together with appropriate escalation and reporting mechanisms

The Prudential Regulation Authority's ("**PRA**") Supervisory Statement SS2/21 came into effect on 31 March 2022 but applies to all outsourcing arrangements entered into after 31 March 2021. The PRA rules are not "materially divergent" with the EBA Guidelines on Outsourcing but provide more granularity in certain areas. The differences include the following:

There is a requirement to specify the renewal date and the start and end date of the contract.

There is a requirement to specify the forum and the governing law.

There is a specific requirement for the contract to address the confidentiality of data and accessibility, availability, etc.

The right to monitor should be based on KPIs.

There is no obligation for the service provider to submit its internal audit reports to the institution.

The BCDR obligations are mutualized, and the requirement to test BCDR plans is softened to a requirement to take reasonable steps to support the test of the plans.

Termination rights should cover both stressed and non-stressed scenarios and both parties are expected to take reasonable steps to support the testing of customers' termination plans.

When it comes to sub-outsourcing, the PRA does not expect firms to directly monitor fourth parties in all circumstances, but the potential impact of large, complex sub-outsourcing chains on firms' operational resilience will need to be considered.

For material outsourcings, there is a requirement on the institution to make the PRA aware if the service provider is unable or unwilling to contractually facilitate the institution's compliance with regulatory obligations.

There is greater flexibility to interpret audit rights in a manner proportionate to materiality of the outsourcing. Firms can choose an appropriate audit method if it enables them to meet their obligations. The level of assurance should be in keeping with the significance of the firm and materiality of services. Where an on-site audit could create unmanageable risk for the provider or other clients, the parties should agree alternative ways to provide an equivalent level of assurance, while not removing contractual rights for an on-site audit. There is no mandatory right for the firm to conduct penetration testing. However, the provider should be required to provide results of any penetration testing.

There should be a clear reference to the Bank of England's resolution powers under the Banking Act 2009 (implementing Articles 68 and 71 of the Bank Recovery and Resolution Directive (2014/59/EU) ("**BRRD**")), and in particular, a description of the "substantive obligations" of the written agreement in the sense of Article 68 of the BRRD.

The PRA also makes clear that an imbalance in negotiating power is not justification for a firm to accept clauses and terms that do not meet the outsourcing requirements. Firms should make the PRA aware if the service provider is unable or unwilling to "contractually facilitate" the PRA requirements. The PRA expects written agreements for material outsourcing to indicate whether material sub-sourcing is permitted, and if a service provider must obtain specific or general written authorization from the firm before transferring data (Article 28 of the General Data Protection Regulation).

**4. When does cloud outsourcing fall within the scope of the rules?**

The concept of "outsourcing" is broadly defined but is slightly differently defined by the Financial Conduct Authority ("**FCA**"), the Prudential Regulation Authority ("**PRA**") and the European Banking Authority ("**EBA**"). The FCA's definition requires the use of a person to provide customized services to a firm other than a member of the firm's governing body acting in their capacity as such or an individual employed by a firm under a contract of service. The PRA defines outsourcing as an arrangement of any form between a firm and a service provider by which that service provider performs a process, service or activity that would otherwise be undertaken by the firm. The EBA's definition requires an arrangement between a firm and a service provider by which the service provider performs a process, service or activity that would otherwise have to be undertaken by the regulated firm.

The use of cloud services will be caught where, if its services were not being used to host, for example, a firm's risk management systems, that firm would need to perform these activities itself. However, this is an issue that will be circumstance dependent and fact specific.

The PRA's Policy Statement 7/21 "Outsourcing and third-party risk management" of March 2021 clarifies that while one-off purchases, such as software licenses that often rely on underlying cloud infrastructure, should not be considered outsourcing (because they are not recurrent), they should still qualify as a third-party arrangement subject to appropriate risk-based controls.

The EBA Guidelines on Outsourcing help to determine whether activities performed by a third party constitute an "outsourcing." The following activities are expressly excluded as outsourcing:

Functions that are legally required to be performed by a service provider (e.g., statutory audit)

Provision of market information services

Purchase of access to "global network infrastructures" (e.g., payment card schemes)

Clearing and settlement arrangements

Correspondent banking services

Services that an institution would not be expected to perform itself (e.g., legal services, cleaning, maintenance of premises, medical services, post-room services, vending machine services, servicing of company cars, receptionists or provision of goods or utilities).

**5. Does the outsourcing need to be notified to the regulator?**

The regulatory position in the UK is complex and depends on the activities of the regulated entity in question (e.g., asset management/investment businesses or operating as a banking entity).

Senior Management, Arrangements, Systems and Controls ("**SYSC**") sourcebook 8.1.1R in the Financial Conduct Authority ("**FCA**") Handbook provides that if a firm relies on third parties for the performance of "relevant services and activities," it must take reasonable steps to avoid undue operational risk. This provision also requires that firms cannot outsource operational functions that would impair the quality of internal controls or the regulator's ability to monitor a firm's compliance position. Section 2 of the Outsourcing Part of the Prudential Regulation Authority's ("**PRA**") Rulebook makes similar provisions. Under Rule 2.3(1)(e) in the Notifications Part of the PRA Rulebook, institutions must notify the PRA when "entering, or significantly changing a material outsourcing arrangement" (see paragraph 5.14 of PRA Supervisory Statement SS2/21). The PRA expects these notifications to be made before entering into the outsourcing arrangement.

**Material outsourcings**

Certain types of outsourcing are considered to be "material outsourcings." These are defined in the FCA Handbook and PRA Rulebook as outsourcings where, if there was a weakness or failure in the delivery of the services, this would cause the regulators to doubt whether the firm would be able to continue to comply with the conditions of its authorization or with the FCA Principles for Businesses or PRA Fundamental Rules. The PRA considers that a "material outsourcing arrangement" encompasses a "critical or important" outsourcing arrangement in relevant retained EU legislation.

Regulated entities cannot undertake a material outsourcing without giving appropriate notice to the regulator in advance of the outsourcing (notice would be dependent on the size, nature and materiality of the outsourcing). Where firms are dual regulated, separate notices are required for both the FCA and the PRA. Although the period for notification is not fixed and will depend on the event in question, the regulators expect this to happen at an early stage and before the firm has made any internal or external commitments.

Where the activity being outsourced is itself regulated, the regulated entity would need a Part 4A permission from the FCA to outsource this activity.

**6. What are the potential consequences for breaching financial services rules on cloud outsourcing?**

The Prudential Regulation Authority and the Financial Conduct Authority have wide ranging powers, including the following:

Withdrawing a firm's authorization

Prohibiting individuals from carrying on regulated activities

Suspending firms and individuals from undertaking regulated activities

Issuing unlimited fines against firms and individuals that breach rules

Making a public announcement when beginning disciplinary action and publishing details of warning, decision and final notices

Applying to the courts for injunctions, restitution orders, winding-up and other insolvency orders

**7. Are there any data privacy and/or data security laws that would apply?**

Yes, the UK General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018 apply to organizations established in the UK that process personal data.

For contracts with a cloud service provider as a data processor, such contracts would need to include provisions that address the mandatory requirements for contracts with data processors under Article 28 of the UK GDPR.

**8. Are there any restrictions under local data protection laws which would impact the overseas hosting of data?**

Yes, the UK General Data Protection Regulation ("**UK GDPR**") prohibits UK established processors or controllers from transferring personal data outside the UK, unless adequate safeguards are in place or derogations under the UK GDPR apply. All relevant legal requirements and standards apply to third-party ICT arrangements including but not necessarily limited to the UK GDPR and the UK Data Protection Act 2018.

For example, transfers of personal data to jurisdictions that are deemed as "adequate" for the purposes of the UK GDPR are permissible. These include transfers of personal data from the UK to the EU, for example.

If the transfer of personal data from the UK is to a jurisdiction that is not deemed to be "adequate" for the purposes of the UK GDPR, additional steps may be required such as entering into standard contractual clauses and conducting an assessment of the laws and practices of that third jurisdiction in relation to whether those laws/practices would impinge on the effectiveness of the standard contractual clauses. There are two mechanisms for transferring personal data from the UK under the UK GDPR: (a) a UK international data transfer agreement; and (b) a UK addendum to the new EU standard contractual clauses. The international data transfer agreement and UK addendum to the new EU standard contractual clauses came into force on 21 March 2022. For agreements entered into before 21 September 2022 on the basis of the previous EU standard contractual clauses approved under the previous EU Data Protection Directive, these remain valid until 21 March 2024, if the processing operations and the subject matter of the contract remain unchanged and reliance on those standard contractual clauses ensures that the transfer of personal data is subject to appropriate safeguards.

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

No, but there are proposals to subject cloud service providers to direct regulatory oversight where they provide critical functions to regulated entities.

**10. Are express consents from customers or other data subjects required before moving data to the cloud?**

No express customer consents are required, although institutions must consider broader financial regulatory and data protection compliance. Institutions will also need to check for any express prohibitions in client contracts.

**11. Are there any local laws which require a cloud service provider to be able to access the data it hosts?**

Yes. In particular, the Investigatory Powers Act 2016 ("**IPA 2016**") gives UK law enforcement agencies the ability to require a cloud service provider to access information held by it. The IPA 2016 applies to any "telecommunications operator" providing services into the UK.

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Yes. Under the Investigatory Powers Act 2016, disclosure may be required in the following circumstances:

Where an executive warrant has been obtained by a UK-based law enforcement agency

Where a notice has been issued by a "relevant public authority"

Where consent has been obtained from the sender and the intended recipient of the communication

Alternatively, disclosure could be mandated where a court order has been obtained by a UK-based law enforcement agency under the Crime (Overseas Production Orders) Act 2019.

Disclosure may also be required where mandated under laws from other countries that have extraterritorial effect (such as pursuant to the Cloud Act agreement in place with the US).

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

Yes, there is no prohibition on using cloud services under applicable regulatory laws.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

Yes, all regulated entities in the UK must comply with the Financial Conduct Authority ("**FCA**") Handbook when using cloud services. The FCA recognizes that these requirements should be enforced in a risk-based and proportionate manner considering the scale and complexity of the services.

Chapter 8 of the FCA's Senior Management Arrangements, Systems and Controls sourcebook ("**SYSC 8**") provides that a firm must ensure that it takes reasonable steps to avoid undue operational risk. Firms cannot outsource operational functions that would impair the quality of internal controls or the regulator's ability to monitor its compliance.

In addition, where the cloud services are considered as the outsourcing of critical or important functions, firms must exercise skill, care and diligence in selecting, managing and terminating those outsourcing arrangements. In particular, the institution must take steps to ensure that the service provider fulfills the following:

Has sufficient capacity and capability to deliver the outsourced function

Carries out the services effectively and compliantly, and in a way that the firm can assess on an ongoing basis

Supervises the outsourced functions and manages risk

Discloses developments that have material impacts on the service provider's ability to perform the function

Grants effective audit rights

Protects confidential information

Establishes and implements business continuity and disaster recovery plans and appropriate exit arrangements

Allows the firm to terminate the arrangement where necessary

Where firms are dual regulated (e.g., banks, large investment firms and insurers), the provisions of the FCA Handbook and the Prudential Regulation Authority ("**PRA**") Rulebook apply.

Similar to the FCA Handbook, the PRA Rulebook specifies a number of high-level "fundamental rules" that firms have to comply with, including obligations to act in a prudent manner, have effective risk strategies and to control their affairs responsibly.

Section 2 of the Outsourcing Part of the PRA Rulebook has rules that are broadly consistent with those set out in SYSC 8.1.1R of the FCA Handbook.

The PRA Rulebook also incorporates Articles 30-31 of Commission Delegated Regulation (EU) 2017/565 (Retained EU Legislation) ("**MIFID Organization Regulation**") and applies these rules to all firms regulated by the PRA. These obligations broadly reflect the SYSC 8 obligations.

**PRA SS2/21 on "Outsourcing and third-party risk management" implementing the EBA Guidelines on Outsourcing**

Despite Brexit, the FCA expects firms to continue to comply with the guidelines on outsourcing (including cloud) that were published by the European Banking Authority ("**EBA**") in February 2019.

The EBA guidelines apply to a broad range of regulated institutions, including banks and investment firms, but not asset management firms. The EBA guidelines identify the steps that firms must take to conduct outsourcing activity in a compliant manner (e.g., including due diligence requirements, notification to a regulator of material outsourcings and internal governance obligations).

The PRA has published a Supervisory Statement SS2/21 on Outsourcing and third-party risk management, which took effect from 31 March 2022. It complements the requirements and expectations on operational resilience in the PRA Rulebook, seeks to facilitate greater resilience and adoption of the cloud and other new technologies and implements (and expands) the EBA guidelines.

**PRA SS2/21 on "Outsourcing and third-party risk management" implementing the EBA Guidelines on ICT and Security Risk Management**

The EBA has established information and communication technology and security risk management guidelines that supplement the EBA Guidelines on Outsourcing.

The FCA has confirmed that these continue to apply in the UK. PRA Supervisory Statement SS2/21 implements relevant sections of these ICT guidelines from 31 March 2022.

The ICT guidelines focus on organizational measures that regulators expect firms to have in place. For example, there are requirements to establish sound internal governance processes and an ICT strategy that is aligned with the firm's overall business strategy.

**PRA expectations in SS2/21 regarding the cloud**

Certain sections of SS2/21 refer specifically to the use of cloud services by regulated firms, setting out the PRA's expectations that regulated firms implement robust controls for data-in-transit, data-in-memory and data-at-rest. Guidance and expectations in respect of outsourcing to cloud services include the following:

The shared responsibility model — firms are expected to define, document and understand their and the cloud service provider's respective responsibilities.

The PRA expects all firms to keep records of their outsourcing arrangements.

In material outsourcing arrangements, the PRA expects firms to retain contractual rights to perform onsite audits at their discretion.

Firms are expected to assess business continuity for material cloud outsourcing arrangements.

Outsourcers are expected to take reasonable steps to test exit plans, especially "stressed" exits.

Since 31 December 2021, under the EBA Outsourcing Guidelines banks are expected to maintain a register of their cloud outsourcing arrangements.

In June 2022, HM Treasury issued a policy statement on "Critical third parties to the finance sector." The policy statement proposed a framework to enable financial regulators to manage the risks to financial stability posed by unregulated parties providing critical services to regulated entitles, including cloud-based computing services. Under the proposed regime, HM Treasury will — in consultation with the financial regulators — be able to designate certain third parties that provide services to firms as "critical third parties" ("**CTPs**"). The financial regulators will then be able to make rules, gather information and take enforcement action, in respect of certain services that CTPs provide to firms of particular relevance to the regulators' objectives (i.e., "material" services). Following publication of the policy paper, the Financial Services and Markets Bill ("**FSM Bill**") was introduced in parliament on 20 July 2022; the FSM Bill sets out a statutory framework for managing systemic risks posed by CTPs through direct regulatory oversight and operational resilience requirements. At the time of writing, the FSM Bill has not completed its passage through parliament, and there is no timescale for it to receive royal assent.

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

Under the Financial Conduct Authority's ("**FCA**") Senior Management Arrangements, Systems and Controls sourcebook ("**SYSC**") at SYSC 8.1.9R, firms must ensure that the parties' rights and obligations are clearly allocated and described in a written agreement. Aside from that requirement, SYSC 8 does not contain any other requirements regarding the contractual arrangements firms must undertake when performing an outsourcing.

The European Banking Authority ("**EBA**") guidelines are more prescriptive and set out specific matters that must be addressed in a written contract between the firm and the services provider. Some of the contractual requirements are dealt with briefly and are of the type one commonly sees in any commercial agreement, for example, a clear description of the outsourced function, term, the governing law, financial obligations, service levels, information about whether the service provider has taken out insurance, requirement to implement and test business continuity and disaster recovery (BCDR) plans, and reporting obligations when material impacts affect the service provider's ability to carry out the services.

Other contractual requirements are more specific to the regulated nature of the institution, including that the contract should specify the following:

Whether the sub-outsourcing of a critical or important function is permitted; if the sub-outsourcing of a critical or important function is permitted, the agreement must specify the following:

What types of activities are excluded from the sub-outsourcing

Any conditions that must be complied with

That the service provider is responsible for the activities of their sub-outsourcers

That the service provider must inform the institution of any planned sub-outsourcing or material changes, and that the institution can object to this

That the institution has the right to terminate in the event of any undue sub-outsourcing (e.g., where the risks are materially increased for the institution without prior notification)

The locations where the critical or important function will be provided and/or where relevant data will be kept and processed, and a requirement that the service provider notifies the firm if it intends to change this during the term

The accessibility, availability, integrity, privacy and safety of relevant data (institutions must define data and system security requirements within the agreement)

That the institution can monitor the service provider's performance on an ongoing basis

That the data owned by the institution can be accessed by the institution in the event of the service provider's insolvency

That the service provider cooperates with competent authorities

That the institution can rely on its rights under the Bank Recovery and Resolution Directive regimes that apply to it in a resolution or ring-fencing scenario

The unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider; the EBA guidelines are expressed as requiring a risk-based approach to audit, but where there is the outsourcing of a critical or important function then they specifically require the following:

The service provider to grant full access to all relevant business premises and devices, systems, networks and data used for providing the outsourced function

Unrestricted inspection and auditing rights to ensure compliance with regulatory and contractual requirements

Contractual arrangements cannot limit the effective exercise of audit rights by the institution, competent authority or third parties appointed by them. Where relevant, commonly accepted audit standards should be applied, although it is permissible to use pooled audits and third-party certifications to allow more efficient audit processes to take place. Generally, institutions must give prior notice of the audit, but not where there is an emergency or crisis situation or the audit would not be effective. The EBA guidelines also recognize that care must be taken when performing audits in multitenanted environments to ensure that risks for other clients are avoided or mitigated. There is also a separate requirement for the service provider to subject its internal audit reports to the institution as appropriate, and specific termination rights are required where any of the following apply:

The service provider breaches applicable law or the contract.

Impediments capable of altering the performance of the outsourced function are identified.

There are material changes affecting the outsourcing arrangement or service provider (e.g., change of subcontractors).

There are weaknesses regarding the management and security of confidential, personal or other sensitive information.

The competent authority requires this.

The outsourcing agreement must also clearly set out the obligations of the service provider where there is to be an exit and transfer to a successor supplier, set out an appropriate transition period to minimize disruption and set out an obligation on the service provider to support an orderly transfer of the outsourced function following the termination.

The EBA's ICT guidelines state that firms are required to ensure the following in their contracts:

Appropriate information security related objectives and measures (e.g., minimum cybersecurity requirements, location of data centers, encryption requirements, monitoring processes and data retention policies)

Incident handling processes, together with appropriate escalation and reporting mechanisms

The Prudential Regulation Authority's ("**PRA**") Supervisory Statement SS2/21 came into effect on 31 March 2022 but applies to all outsourcing arrangements entered into after 31 March 2021. The PRA rules are not "materially divergent" with the EBA Guidelines on Outsourcing but provide more granularity in certain areas. The differences include the following:

There is a requirement to specify the renewal date and the start and end date of the contract.

There is a requirement to specify the forum and the governing law.

There is a specific requirement for the contract to address the confidentiality of data and accessibility, availability, etc.

The right to monitor should be based on KPIs.

There is no obligation for the service provider to submit its internal audit reports to the institution.

The BCDR obligations are mutualized, and the requirement to test BCDR plans is softened to a requirement to take reasonable steps to support the test of the plans.

Termination rights should cover both stressed and non-stressed scenarios and both parties are expected to take reasonable steps to support the testing of customers' termination plans.

When it comes to sub-outsourcing, the PRA does not expect firms to directly monitor fourth parties in all circumstances, but the potential impact of large, complex sub-outsourcing chains on firms' operational resilience will need to be considered.

For material outsourcings, there is a requirement on the institution to make the PRA aware if the service provider is unable or unwilling to contractually facilitate the institution's compliance with regulatory obligations.

There is greater flexibility to interpret audit rights in a manner proportionate to materiality of the outsourcing. Firms can choose an appropriate audit method if it enables them to meet their obligations. The level of assurance should be in keeping with the significance of the firm and materiality of services. Where an on-site audit could create unmanageable risk for the provider or other clients, the parties should agree alternative ways to provide an equivalent level of assurance, while not removing contractual rights for an on-site audit. There is no mandatory right for the firm to conduct penetration testing. However, the provider should be required to provide results of any penetration testing.

There should be a clear reference to the Bank of England's resolution powers under the Banking Act 2009 (implementing Articles 68 and 71 of the Bank Recovery and Resolution Directive (2014/59/EU) ("**BRRD**")), and in particular, a description of the "substantive obligations" of the written agreement in the sense of Article 68 of the BRRD.

The PRA also makes clear that an imbalance in negotiating power is not justification for a firm to accept clauses and terms that do not meet the outsourcing requirements. Firms should make the PRA aware if the service provider is unable or unwilling to "contractually facilitate" the PRA requirements. The PRA expects written agreements for material outsourcing to indicate whether material sub-sourcing is permitted, and if a service provider must obtain specific or general written authorization from the firm before transferring data (Article 28 of the General Data Protection Regulation).

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

The concept of "outsourcing" is broadly defined, but slightly differently defined by the Financial Conduct Authority ("**FCA**"), the Prudential Regulation Authority ("**PRA**") and the European Banking Authority ("**EBA**"). The FCA's definition requires the use of a person to provide customized services to a firm other than a member of the firm's governing body acting in their capacity as such or an individual employed by a firm under a contract of service. The PRA defines outsourcing as an arrangement of any form between a firm and a service provider by which that service provider performs a process, service or activity that would otherwise be undertaken by the firm. The EBA's definition requires an arrangement between a firm and a service provider by which the service provider performs a process, service or activity that would otherwise have to be undertaken by the regulated firm.

The use of cloud services will be caught where, if its services were not being used to host, for example, a firm's risk management systems, that firm would need to perform these activities itself.

However, this is an issue that will be circumstance dependent and fact specific.

The EBA Guidelines on Outsourcing help to determine whether activities performed by a third party constitute an "outsourcing." Activities expressly excluded as outsourcing are:

Functions that are legally required to be performed by a service provider (e.g., statutory audit)

Provision of market information services

Purchase of access to "global network infrastructures" (e.g., payment card schemes)

Clearing and settlement arrangements

Correspondent banking services

Services that an institution would not be expected to perform itself (e.g., legal services, cleaning, maintenance of premises, medical services, post-room services, vending machine services, servicing of company cars, receptionists or provision of goods or utilities)

# Regulatory notifications

## 5. Does the outsourcing need to be notified to the regulator?

The regulatory position in the UK is complex and depends on the activities of the regulated entity in question (e.g., asset management/investment businesses or operating as a banking entity).

Senior Management, Arrangements, Systems and Controls ("**SYSC**") sourcebook 8.1.1R in the Financial Conduct Authority ("**FCA**") Handbook provides that if a firm relies on third parties for the performance of "relevant services and activities," it must take reasonable steps to avoid undue operational risk. This provision also requires that firms cannot outsource operational functions that would impair the quality of internal controls or the regulator's ability to monitor a firm's compliance position. Section 2 of the Outsourcing Part of the Prudential Regulation Authority's ("**PRA**") Rulebook makes similar provisions. Under Rule 2.3(1)(e) in the Notifications Part of the PRA Rulebook, institutions must notify the PRA when "entering, or significantly changing a material outsourcing arrangement" (see paragraph 5.14 of PRA Supervisory Statement SS2/21). The PRA expects these notifications to be made before entering into the outsourcing arrangement.

**Material outsourcings**

Certain types of outsourcing are considered to be "material outsourcings." These are defined in the FCA Handbook and PRA Rulebook as outsourcings where, if there was a weakness or failure in the delivery of the services, this would cause the regulators to doubt whether the firm would be able to continue to comply with the conditions of its authorization or with the FCA Principles for Businesses or PRA Fundamental Rules. The PRA considers that a "material outsourcing arrangement" encompasses a "critical or important" outsourcing arrangement in relevant retained EU legislation.

Regulated entities cannot undertake a material outsourcing without giving appropriate notice to the regulator in advance of the outsourcing (notice would be dependent on the size, nature and materiality of the outsourcing). Where firms are dual regulated, separate notices are required for both the FCA and the PRA. Although the period for notification is not fixed and will depend on the event in question, the regulators expect this to happen at an early stage and before the firm has made any internal or external commitments.

Where the activity being outsourced is itself regulated, the regulated entity would need a Part 4A permission from the FCA to outsource this activity.

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

The Prudential Regulation Authority and Financial Conduct Authority have wide ranging powers, including:

Withdrawing a firm's authorization

Prohibiting individuals from carrying on regulated activities

Suspending firms and individuals from undertaking regulated activities

Issuing unlimited fines against firms and individuals that breach rules

Making a public announcement when beginning disciplinary action and publishing details of warning, decision and final notices

Applying to the courts for injunctions, restitution orders, winding-up and other insolvency orders

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes, the UK General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018 apply to organizations established in the UK that process personal data.

For contracts with a cloud service provider as a data processor, such contracts would need to include provisions that address the mandatory requirements for contracts with data processors under Article 28 of the UK GDPR.

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

Yes, the UK General Data Protection Regulation ("**UK GDPR**") prohibits UK established processors or controllers from transferring personal data outside the UK, unless adequate safeguards are in place or derogations under the UK GDPR apply. All relevant legal requirements and standards apply to third-party ICT arrangements including but not necessarily limited to the UK GDPR and the UK Data Protection Act 2018.

For example, transfers of personal data to jurisdictions that are deemed as "adequate" for the purposes of the UK GDPR are permissible. These include transfers of personal data from the UK to the EU, for example.

If the transfer of personal data from the UK is to a jurisdiction that is not deemed to be "adequate" for the purposes of the UK GDPR, additional steps may be required such as entering into standard contractual clauses and conducting an assessment of the laws and practices of that third jurisdiction in relation to whether those laws/practices would impinge on the effectiveness of the standard contractual clauses. There are two mechanisms for transferring personal data from the UK under the UK GDPR: (a) a UK international data transfer agreement; and (b) a UK addendum to the new EU standard contractual clauses. The international data transfer agreement and UK addendum to the new EU standard contractual clauses came into force on 21 March 2022. For agreements entered into before 21 September 2022 on the basis of the previous EU standard contractual clauses approved under the previous EU Data Protection Directive, these remain valid until 21 March 2024, if the processing operations and the subject matter of the contract remain unchanged and reliance on those standard contractual clauses ensures that the transfer of personal data is subject to appropriate safeguards.

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

No, but there are proposals to subject cloud service providers to direct regulatory oversight where they provide critical functions to regulated entities.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

No express customer consents are required, although institutions must consider broader financial regulatory and data protection compliance. Institutions will also need to check for any express prohibitions in client contracts.

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

Yes. In particular, the Investigatory Powers Act 2016 ("**IPA 2016**") gives UK law enforcement agencies the ability to require a cloud service provider to access information held by it. The IPA 2016 applies to any "telecommunications operator" providing services into the UK.

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Yes. Under the Investigatory Powers Act 2016, disclosure may be required in the following circumstances:

Where an executive warrant has been obtained by a UK-based law enforcement agency

Where a notice has been issued by a "relevant public authority"

Where consent has been obtained from the sender and the intended recipient of the communication

Alternatively, disclosure could be mandated where a court order has been obtained by a UK-based law enforcement agency under the Crime (Overseas Production Orders) Act 2019.

Disclosure may also be required where mandated under laws from other countries that have extraterritorial effect (such as pursuant to the Cloud Act agreement in place with the US).

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.