Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) United Kingdom

Microsoft has published guidance to help financial institutions in the UK achieve their compliance requirements for cloud adoption.

Microsoft and the FCA and the PRA

When financial institutions in the UK outsource business functions to the cloud, they must comply with the rules and guidance of the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA).

Microsoft has published two comprehensive papers that explain how Microsoft cloud services can help financial institutions in the UK that are authorized and regulated by the FCA and the PRA to outsource business functions to the cloud in a compliant manner. Reviewing the papers can help financial institutions adopt Microsoft cloud services with the confidence that Microsoft can help enable their compliance with applicable regulatory requirements.

- Enabling compliance: the Microsoft approach to FCA updated cloud guidance. In response to the FCA publication, *FG 16/5 – Guidance for firms outsourcing to the 'cloud' and other third-party IT services* (revised in July 2018), Microsoft updated its response paper to help financial institutions meet the FCA cloud guidance. The paper, amongst other aspects, describes Microsoft compliance with numerous recognized international standards, transparency around how we handle customer data to give customers control over it, and our contractual provisions that address specific financial services regulatory requirements.

  Sections in the paper map in depth to each area of interest in the FCA guidance. For example, a key outsourcing requirement is that financial firms must identify and manage any risks that outsourcing may introduce. Microsoft helps financial firms assess the relevant risks, identifies current best practices, and makes available a wide range of resources to facilitate their due diligence.

- A compliance checklist for financial institutions in the UK. This checklist helps financial institutions in the UK that are conducting due-diligence assessments of Microsoft cloud services. It includes:

  - An overview of the regulatory landscape for context.
  - A checklist that sets forth the issues to be addressed and maps Microsoft Azure, Microsoft Dynamics 365, and Microsoft 365 services against those regulatory obligations. The checklist can be used as a tool to help measure compliance against a regulatory framework for outsourcing to the cloud. It can also provide an internal structure for documenting compliance, as well as help customers conduct their own risk assessments of Microsoft cloud services.

Microsoft in-scope cloud services

- Azure
  Learn more
- Dynamics 365
  Learn more
- Intune
- Microsoft 365
  Learn more
- Power BI cloud service
  Either as a standalone service or as included in an Office 365 branded plan or suite

How to implement

- **Compliance checklist: the UK**
  Financial institutions can get help in conducting risk assessments of Microsoft cloud services.
  Learn more
- **Financial use cases**
  Use case overviews, tutorials, and other resources to build Azure solutions for financial services.
  Learn more
- **Risk Assessment & Compliance Guide**
  Create a governance model for risk assessment of Microsoft cloud services, and regulator notification.
  Learn more

About the FCA and PRA

The Financial Conduct Authority (FCA), an independent public body that is accountable to the UK Treasury and Parliament, regulates 58,000 financial firms and markets in the UK and serves as the prudential regulator for over 18,000 of those organizations. The Bank of England prudentially regulates financial services firms through the Prudential Regulation Authority (PRA), which was authorized under the Financial Services and Markets Act 2000. The PRA works alongside the FCA, supervising 1,500 of the larger financial services institutions such as banks, credit unions, insurers, and investment firms. (The FCA picks up prudential regulation for firms that do not fall under the PRA remit.)

The FCA and PRA also work in concert *with* the European Banking Authority (EBA), an independent EU authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. To that end, the EBA has outlined a comprehensive approach to the use of cloud computing by financial institutions in the EU, Recommendations on outsourcing to cloud services providers.

In July 2016, the FCA published guidance for firms considering adopting cloud services, which was revised in July 2018, FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services. The intent of the guidance is to help financial institutions understand FCA regulatory expectations: "The overall aim of the high-level regulatory obligations on outsourcing, and the detailed requirements that underpin them, is that a firm appropriately identifies and manages the operational risks associated with its use of third parties, including undertaking due diligence before making a decision on outsourcing." (page 4)

This document offers specific advice on how to evaluate, use, and monitor third parties that deliver cloud services. It divides considerations into thirteen areas of interest, ranging from legal and regulatory considerations and risk management to continuity planning and plans for exiting outsourcing arrangements.

Although the guidance is not binding, the FCA expects firms to use it where appropriate. (Note that the PRA has different statutory objectives, so firms it regulates must confirm their approach with the PRA.) Of course, firms that outsource their business activities remain fully responsible and accountable for discharging their regulatory responsibilities just as if they performed the outsourced functions themselves.

Whilst the FCA guidance of 2018 applies to financial institutions, it does not apply to banks, building societies, designed investment firms, or IFPRU investment firms that are subject to EBA Recommendations. To help enable compliance for banks and other outside-scope institutions, Microsoft has published a white paper on how our cloud services align with the EBA Recommendations: European Banking Authority Guidance Addresses Cloud Computing for the First Time.

Frequently asked questions

Is regulatory approval required?
No. The use of public cloud computing is permitted in the UK, subject always to compliance with the regulatory requirements We have summed these up in our compliance checklist. However, financial firms must notify the FCA or PRA (as applicable) of any proposal to enter into a material outsourcing arrangement and of any material changes to those arrangements. Although Microsoft is not a financial services business regulated by these authorities to carry on any of the activities for which prior authorization is required, we provide specific information as we are able to help firms meet their regulatory obligations.

Are there any mandatory terms that must be included in the contract with the cloud service providers?
Yes. Part 2 of our compliance checklist (page 66) contains a comprehensive list of the requirements that must be included in contracts with cloud service providers.

Can I use Microsoft responses to this framework in my organization's compliance process?
Yes. However, although Microsoft responses to this framework are confirmed compliant by third parties, customers are responsible for validating the compliance of solutions they have implemented on Microsoft cloud services.

Additional resources

Microsoft collaborates with ClearBank: Launch of first new UK clearing bank in over 250 years

Microsoft and the EU-Swiss-U.S. Privacy Shield

Microsoft Financial Services Compliance Program

Microsoft business cloud services and financial services

Financial services compliance in Azure

Azure Financial Services Cloud Risk Assessment Tool