Australian Prudential Regulation Authority (APRA)

Microsoft published guidance to help financial services clients comply with the outsourcing standards of the Australian Prudential Regulation Authority.

Microsoft and APRA

For financial institutions in Australia that are assessing cloud providers and their services, Microsoft has published the Microsoft response to the APRA Information Paper on Cloud and A compliance checklist for financial institutions in Australia. Together they demonstrate how financial firms can move data and workloads to Microsoft Azure with the confidence that they are complying with Australian Prudential Regulation Authority (APRA) regulations and guidance.

Microsoft response to the APRA information paper on Cloud

This Microsoft paper provides detailed guidance for financial services with a detailed response to each issue raised in the APRA information paper, Outsourcing involving shared computing services (including cloud). The APRA guidelines identify three risk categories into which usage typically falls—low risk, heightened inherent risk, and extreme impact if disrupted—and highlight key issues that regulated entities must consider as part of their risk assessment.

The Microsoft response focuses on the two highest risk categories. While cloud services are not prohibited by any risk category, APRA expects you to undertake a commensurately higher level of diligence, and you should expect an increasing level of APRA scrutiny, as you move up the risk categories. APRA lists a range of factors that typically indicate high risk for outsourcing. Microsoft addresses each of these factors in depth, providing information and tools to help you assess the risk of moving your data and workloads to Azure.

Microsoft also addresses each APRA risk management consideration: strategy, governance, selection process, transition approach, security, ongoing management, business disruption, and assurance. Point by point, we give advice and offer tools to help you respond to each issue when deploying Azure.

Navigating your way to the cloud: A compliance checklist for financial institutions in Australia

This Microsoft checklist introduces APRA regulatory requirements that financial firms must address when moving to the cloud. It maps Azure against not only the Prudential Standard CPS 231 Outsourcing, but other relevant APRA standards, such as for business continuity and risk management. Completing this checklist will help your financial service institutions adopt Azure with the confidence that it meets the relevant APRA requirements.

By relying on our comprehensive approach to risk assurance in the cloud, we are confident that Australian financial services organizations can move to Microsoft cloud services in a manner that is not only consistent with APRA guidance, but can provide customers with a more advanced security risk management profile than on-premises or other hosted solutions.

Microsoft in-scope cloud services

- Azure
  Learn more
- Intune
- Office 365
  Learn more

How to implement

- **Microsoft response to APRA**
  Get practical support for moving data and workloads to Azure in compliance with APRA regulations.
  Learn more

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

About APRA

The Australian Prudential Regulation Authority (APRA) oversees banks, credit unions, insurance companies, and other financial services institutions in Australia. Recognizing the momentum towards cloud computing, APRA has called on regulated entities to implement a thoughtful cloud-adoption strategy with effective governance, thorough risk assessment, and regular assurance processes.

Regulated institutions must comply with the APRA Prudential Standard CPS 231 Outsourcing when outsourcing a material business activity—any activity that has the potential, if disrupted, to have a significant impact on the financial institution's business operations or ability to manage its risks effectively. Based on its review of outsourcing arrangements involving shared computing services submitted to APRA, APRA published specific, detailed guidance in its information paper, Outsourcing involving shared computing services (including cloud), to help regulated entities assess cloud providers and services more effectively.

Frequently asked questions

Do financial institutions need APRA approval before outsourcing material business activities?

No. However, most regulated financial organizations must notify APRA after entering into agreements to outsource material business activities within Australia or consult with APRA before outsourcing those activities outside of Australia. In addition, if the cloud services are deemed to carry "heightened inherent risk" as described in the APRA information paper, Outsourcing involving shared computing services (including cloud), the financial institution is encouraged (but not required) to consult with APRA, regardless of whether the service is provided within or outside of Australia.

How can my organization get help complying with APRA outsourcing requirements?

To help our customers, Microsoft has published Microsoft Cloud Services: Compliance with APRA Prudential Standard CPS 2345 Information Security. This paper sets out each of the relevant APRA Prudential Standard CPS 234 regulatory obligations, and maps against them the Microsoft cloud service controls, capabilities, functions, and contract commitments to help APRA-regulated entities comply with those obligations.

Are transfers of data outside of Australia permitted?

Yes. General privacy legislation (which applies across all sectors, not just to financial institutions) permits transfers outside of Australia under certain conditions. Microsoft agrees to contractual terms in line with Australian Privacy Principles so that transfers of data outside of Australia are permitted when you use Microsoft cloud services. However, many of our Australian financial services customers take advantage of the cloud services available from our Australian datacenters, for which we make specific contractual commitments to store categories of data at rest in the Australian geography. These are outlined further in the compliance checklist.

Additional resources

- Microsoft Australia: Cloud in Financial Services
- Case study: Regtech meets Fintech; Perpetual and Microsoft transform the finance sector
- Microsoft Financial Services Compliance Program
- Financial services compliance in Azure
- Microsoft business cloud services and financial services
- Azure Financial Services Cloud Risk Assessment Tool