Microsoft

Microsoft's response to APRA's 2018 Information Paper on Cloud

Contents

Navigating a path to the cloud

In 2015, when APRA released its first Information Paper on cloud, it expressed reservations about the use of cloud for initiatives with heightened or extreme inherent risk.

With the release in September of the 2018 Information Paper: Outsourcing involving cloud computing services, APRA updated its cloud guidance for regulated entities. Much has changed since 2015.

The 2018 Information Paper reflects APRA's more open stance on cloud usage. It acknowledges advances in cloud safety and security, as well as the increased appetite for using the cloud, especially among new and aspiring entities that want to take a cloud-first approach to data storage and management.[1]

In the 2018 update, APRA states: 'Since 2015, there has been continuous evolution of both cloud computing service offerings and APRA-regulated entities' risk management. Generally, service providers have strengthened their control environments, increased transparency regarding the nature of the controls in place, and improved their customers' ability to monitor their environments. APRA-regulated entities have also improved their management capability and processes for assessing and overseeing the services provided.'[2]

The 2018 update brings greater clarity to APRA's guidance. APRA shares the lessons of the last three years' experience supervising numerous regulated entities in their successful transitions to the cloud. This helps guide regulated entities through thoughtful cloud adoption strategies, with effective governance arrangements, thorough risk assessment and regular assurance processes.

At Microsoft Australia, we're pleased to have participated in many compliance conversations with APRA-regulated banks, insurers and superannuation trustees – many of whom now use Microsoft cloud services. We welcome APRA's growing openness to cloud services as a platform for digital innovation and transformation in the Australian financial services sector. We also appreciate the greater clarity from APRA about its expectations.

This document is a further contribution to those conversations. Following the structure and topics outlined in APRA's 2018 Information Paper, we provide a detailed response to each issue raised and demonstrate how Australian financial services organisations can move to Microsoft cloud services in a manner consistent with APRA's guidance.

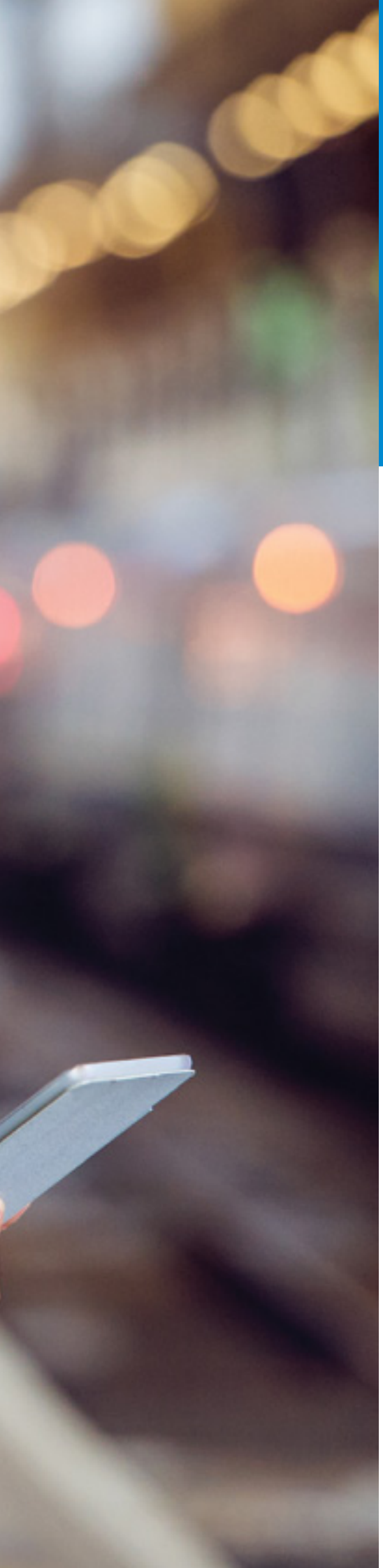
We hope you find our response useful, and we look forward to continuing the cloud conversation with you.

Duncan Taylor
Director, Financial Services
Microsoft Australia

Tom Daemen
Director, Corporate, External, and Legal Affairs
Microsoft Australia

1. Wayne Byres, 24 Sep 2018, speech: Peering into a cloudy future, https://www.apra.gov.au/media-centre/speeches/peering-cloudy-future
2. APRA, 2018, Information Paper: Outsourcing involving cloud computing services, p4

Cloud offerings by different providers can vary significantly in their delivery models, as can individual customer implementations of those offerings.



1. Risks must be understood and managed

Like APRA, Microsoft has observed a noticeable increase in the uptake of cloud services by financial services providers recently. We have also seen a wide variety of use cases emerge, from low-risk scenarios, such as test and development, to systems of record, which APRA has identified as involving extreme inherent risk.

In Chapter 1 of the 2018 Information Paper, APRA confirms that any risk analysis must be grounded in the proposed usage of the cloud service under consideration. Cloud offerings by different providers can vary significantly in their delivery models, as can individual customer implementations of those offerings. So for organisations considering a cloud computing service, it is key to start with a detailed understanding of the nature of the service, and the planned usage of it.

APRA identifies three risk categories into which usages typically fall: low risk, heightened inherent risk and extreme inherent risk. It is important to note that cloud services are not prohibited by any risk category. Rather, 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.

In practical terms, this means that you can consider Microsoft cloud services for the full range of usages across your business. Indeed, one of the most notable developments in this Information Paper is the shift in posture towards arrangements involving critical workloads such as systems of record: see page 12 for more information.

In the sections that follow, we focus on two of APRA's risk categories: heightened inherent risk and extreme inherent risk. We do not focus on the low-risk category, as this is not an area of concern and only requires post-contract notification (except if offshoring is involved). However, our view is that an APRA-regulated entity should still undertake an appropriate and proportionate level of diligence in relation to the use of the cloud service and cloud service provider for low-risk usage activities.

Heightened inherent risk is a focus because, in APRA's view, exposure to non-financial industry tenants (as is normal in the case of public cloud services) typically gives rise to heightened inherent risk. And extreme inherent risk is a focus because APRA cites hosting certain systems of record in the public cloud as an example of such usage. This is a scenario that attracts a high level of interest from our customers and from APRA in its supervisory role.

How Microsoft cloud services relate to APRA's heightened inherent risk factors

APRA's guidance is that heightened inherent risk will be present in outsourcing arrangements involving highly critical and/or sensitive IT assets that result in either an increased likelihood of disruption, or where a disruption would result in a significant impact. To help with applying this guidance, APRA lists a range of factors that typically indicate 'heightened inherent risk'. We discuss how these factors relate to Microsoft cloud services below.

Public cloud

Exposure to 'untrusted' environments which are available to non-financial industry entities (i.e. 'public cloud') as distinct from financial sector 'community clouds'.

Consistent with its 2015 Information Paper, APRA distinguishes the 'heightened risk' factor of public cloud arrangements which are not targeted to service a single market vertical, from community clouds, where tenants are restricted to users with comparable security requirements, risk profiles and risk appetites.

Microsoft Azure is the only hyperscale cloud provider to offer services restricted solely for Australian and New Zealand governments, critical infrastructure organisations and their suppliers. Since April 2018, Microsoft customers that are Australian-regulated financial service providers can access two new Microsoft Azure cloud regions that are specifically designed to support this restricted community. Known as Azure Australia Central Regions, they are located within the highly secure, resilient Australian-owned facilities of Canberra Data Centres (CDC). Access is by invite or application only, enforcing a community of 'whitelisted' members who have the opportunity to guide future service deployment and share expertise and experiences.

Azure Australia Central Regions deliver high availability and performance, low latency, disaster resilience and the opportunity for real-time data streaming and analysis. Highly secure and with the leading security certifications, these regions were built with the challenging demands and specific risk profiles of mission-critical computing in mind.

These regions are the only commercial data centre facilities in Australia that are designed with the physical security controls necessary for classified data, which demands a higher degree of physical and personnel security controls along with complete transparency on supply chain integrity. Additionally, the presence of Microsoft data centres in multiple regions in Australia means that we can offer high levels of geographical redundancy, providing greater assurance that our critical infrastructure customers can continue their key operations in the face of disruption scenarios.

Microsoft is also the first public cloud to achieve Protected Certification with the Australian Signals Directorate. We now have 25 Azure and 10 Office 365 services certified for classified information datasets. This means our regulated financial services customers can be confident that we can expertly handle the sensitive information that they host.

Microsoft Azure is the only global cloud provider to offer services restricted for the use of governments and critical infrastructure organisations, delivered from Australian-owned facilities designed and accredited for classified data.

Public cloud (continued)

Exposure to 'untrusted' environments which are available to non-financial industry entities (i.e. 'public cloud') as distinct from financial sector 'community clouds'.

We believe these first-rate security, compliance, flexibility and connectivity features of Azure Australia Central Regions offer our customers in highly regulated and sensitive industries a specialised cloud service designed to facilitate the highest levels of compliance.

We are happy to discuss your needs and how Microsoft Azure and our partners can address them. As part of our commitment to transparency, we run tours of the CDC facilities, so you can see why Azure Australia Central Regions offers the ideal home for your applications and infrastructure.

More information

Azure Australia Central Regions
aka.ms/aacr

Track record

Unproven track record of: the provider, service, specific usage, control environment, or APRA-regulated entity in managing an arrangement of comparable size, complexity, and/or risk profile.

Microsoft and its cloud services Azure, Office 365 and Dynamics 365 have a proven track record in the financial services sector. This is evidenced by a list of prestigious customers that includes APRA-regulated banks, insurers and superannuation trustees. Some are outsourcing their systems of record to Microsoft Azure.

Microsoft also provides unique on-premises, hybrid and pure cloud solution options to our customers. Hybrid solutions that integrate cloud services into on-premises IT infrastructure are popular among our financial services customers as they allow them to leverage their existing investments and know-how to design an environment that takes account of their specific risk tolerance and readiness for the cloud.

Transition arrangements

High degree of difficulty in transitioning to alternate arrangements.

Transition arrangements are important because cloud service users may want or need the flexibility to bring their activities back in-house or move to another provider. A high degree of difficulty in making that transition typically gives rise to 'heightened inherent risk' in APRA's view.

It is not difficult to transition from Microsoft cloud services to alternative arrangements. Microsoft cloud services are designed to ensure that you can retrieve your customer data at any time and for any reason without requiring assistance from or notification to Microsoft. Customer data stored within Microsoft cloud services is directly portable to on-premises versions of the same products and we make tools available to make this even easier. Our contractual commitments specify that when your subscription expires or is terminated, we will store your customer data in a limited-function account for a 90-day retention period to give you time to export the data or renew your subscription. After the 90-day retention period ends, we will disable your account and delete all customer data within a further 90 days for Azure, Office 365 and Dynamics 365. You may also elect to extend the online services on a month-to-month basis for up to one year from the date of termination or expiration.

Microsoft contractually commits to provide assistance with any transition to alternate arrangements through Microsoft's professional services organisation, including at any time during any extended service period as described above.

Also, standalone, non-cloud products of like or similar functionality can easily and quickly be acquired from Microsoft (or third parties) as substitutes for a Microsoft cloud service. For example, Microsoft makes available a full suite of on-premises Office products that can be used in place of Office 365 where necessary. Microsoft Dynamics 365 is also available in on-premises, cloud or hybrid models. Microsoft also has Azure Stack, which allows a seamless extension between cloud and on-premises products, enabling ease of portability of applications without changing your code base. Microsoft uniquely offers comprehensive on-premises, hybrid and public cloud solution options for its customers.

More information

Online Services Terms
microsoft.com/contracts

Assessment of the control environment

Inability for an APRA-regulated entity to assess the design and ongoing operational effectiveness of the control environment.

There are several avenues through which APRA-regulated entities can assess the control environment of Microsoft cloud services. Together they ensure that you can meet your audit requirements, supervise the service and have ongoing accountability with Microsoft.

First, Microsoft provides many built-in service capabilities to help you examine and verify access, control and service operation as part of your regular assurance processes. These include:

- **Service Trust Portal** – for deep technical trust and compliance information, including recent audit reports for our services, as well as the International Standards Organisation (ISO) Statements of Applicability
- **Compliance Manager** – a tool that provides detailed information about our internal controls, including test status and most recent test dates, and allows you to create your own assessments and monitor your own controls
- **Office 365 Audited Controls** – for detailed information about our internal control set, including mapping to international standards, and the most recent test dates
- **Office 365 Management Activity API** – for visibility of user, admin, system and policy actions and events from your Office 365 and Azure Active Directory activity logs
- **Office 365 Health Dashboard** – to immediately check service health, including current known services issues and ongoing resolution plans in progress
- **Azure Security Center** – for visibility into the security state of your Azure resources and the ability to respond to threats and vulnerabilities
- **Azure Advisor** – for continuous intelligent recommendation for how to further secure your environment
- **Microsoft Trust Center** – for information about data protection and security, including the location of our primary and backup data centres, subcontractor lists, and rules for when Microsoft service administrators have access to customer data.

Second, our extended contract terms for financial services customers add the ability for your internal compliance officers to examine the service more deeply to meet regulatory requirements. Through the optional compliance program for regulated financial services customers, customers have the opportunity to examine the control framework of the service, review its risk management framework, hold one-to-one discussions with Microsoft's auditors and obtain in-depth views directly from Microsoft subject matter experts (SMEs).

More information

Service Trust Portal
trustportal.office.com

Office 365 Service Assurance, including Office 365 Audited Controls
protection.office.com

Office 365 Management Activity API
msdn.microsoft.com/library/office/mt227394.aspx

Office 365 Service Health Dashboard
https://status.office365.com/

Azure Security Center
azure.microsoft.com/en-us/services/security-center

Trust Center
microsoft.com/trustcenter

Office 365 Service Health Dashboard
https://status.office365.com/

Jurisdictional, contractual or technical considerations

Factors which may inhibit operational oversight or business continuity in the event of a disruption.

Many of our Australian financial services customers take advantage of the cloud services available from our Australian data centres, including Azure, Office 365 and Dynamics 365. We make specific contractual commitments to store categories of data at rest in the Australian geography in the Online Services Terms. Information about service health (both real time and historical) is also available to our customers at any time via the Administration Portal or service health dashboard. Microsoft also provides transparency on continuity testing on the Service Trust Portal.

Our cloud services are engineered to be highly resilient, and we have robust recovery procedures in place that are discussed on page 22 of this paper. For example, to help maintain high service levels, service continuity provisions are built into Office 365. These provisions enable Office 365 services to recover quickly from unexpected events such as hardware or application failure, data corruption or other incidents that affect users. The service continuity provisions presented in this service description apply specifically to when a catastrophic event occurs, such as a natural disaster or fire within a Microsoft data centre that renders the entire data centre inoperable.

Microsoft has documented Business Continuity Plans (BCPs) for Azure, Office 365 and Dynamics 365, which provide detailed procedures for recovery and reconstitution of systems and are subject to regular independent audit and verification in published third party audit reports.

Microsoft also provides the support and services needed to help restore our customers' and partners' operations, as well as assisting in local community efforts to respond and recover. In the unlikely event of a sustained service disruption, there are no contractual impediments to taking control of your data, ceasing to use the Microsoft cloud service, and transitioning back to on-premises installations using established pathways. You can retrieve a copy of all your customer data at any time and for any reason without requiring assistance or notification from Microsoft. When you leave the service or your subscription expires, we will store your customer data in a limited-function account for a 90-day retention period to give you time to export the data or renew your subscription. After the 90-day retention period, we will disable your account and delete all customer data within a further 90 days for Azure, Office 365 and Dynamics 365.

More information

Online Services Terms
microsoft.com/contracts

Transition arrangements

Transition involves a complex, resource intensive and/or time-constrained program of work.

We can work with your organisation in various ways to reduce complexity and resource demands, and plan a successful transition program to Microsoft cloud services. Have a look at the 'Transition approach' section on page 17 of this paper for some initial advice and the Microsoft resources that can assist with this process.

How Microsoft cloud services relate to APRA's extreme inherent risk scenario

In the 2018 Information Paper, APRA uses the example of hosting systems of record in the cloud, holding information essential to determining obligations to customers and counterparties (such as current balance, benefits and transaction history) as an extreme inherent risk scenario. We discuss this scenario in the context of Microsoft cloud services below.

Hosting systems of record in the public cloud

In the 2015 Information Paper, APRA expressed caution about hosting systems of record in the public cloud, stating that 'it is not readily evident that risk management and mitigation techniques for public cloud arrangements have reached a level of maturity commensurate with usages having an extreme inherent risk'.[3]

Now, in the 2018 updated Information Paper, APRA has adopted a far more open stance to hosting systems of record in the cloud, stating instead: 'APRA would expect that entities can demonstrate that their risk management and mitigation techniques and capabilities are sufficiently strong.'[4] This is a major shift in stance, and it reflects the successful system of record cloud transitions seen in the market over the interim three-year period.

Numerous financial institutions worldwide are hosting their systems of record on Microsoft Azure, and APRA-regulated entities are already working on migrating their systems of record to Microsoft Azure.

Microsoft's public cloud services offer an increased level of operational security, risk management and compliance relative to a private or hosted cloud service provider. This is due to the scale and sophistication of security investments in services like Azure, Office 365 and Dynamics 365, as well as the pace of innovation in security practices, and the rigour of compliance and risk management, that we apply to those public cloud services.

Microsoft is a sophisticated hyperscale cloud provider with a proven track record in the financial services sector. We also continue to evolve our specialised offering to regulated financial services customers to assist with meeting their regulatory needs. In Azure, Microsoft provides the best platform for APRA-regulated entities who wish to host systems of record in the cloud to meet the very highest standard of risk management and mitigation techniques and capabilities demanded by APRA.

We welcome the opportunity to work with APRA-regulated entities to explore how systems of record can be moved to Microsoft cloud services in a manner that is consistent with APRA's expectations and guidance. We are confident that our comprehensive control environment and contractual commitments provide the right framework for APRA-regulated entities to do so.

3. APRA, 2015, Information Paper: Outsourcing involving shared computing services (including cloud), p6
4. APRA, 2018, Information Paper: Outsourcing involving cloud computing services, p9

APRA is now much more open to hosting systems of record in the public cloud, though still demands the highest standards of risk management and mitigation. Microsoft is a sophisticated hyperscale cloud provider with a proven track record in the financial services sector, and can help you achieve that high standard.

2. Risk management considerations

In Chapter 2 of the 2018 Information Paper, APRA highlights key risk management topics that regulated entities need to consider as part of their due diligence activities.

APRA requires your due diligence review to be targeted and proportionate. Microsoft would add that you should also take account of the relative risk of the cloud service under consideration.

To understand the relative risk, you need to assess the risks associated with maintaining the status quo (which may involve continuing to run your application or servers on-premises) and other alternatives under consideration, and compare those assessments with the risks associated with the proposed cloud computing service.

Our experience is that conducting a risk assessment of the status quo can be illuminating in revealing processes and controls that have not kept pace with evolving business practices and compliance requirements. Similarly, risk assessments that consider different alternatives (which may include a public cloud service, on the one hand, and a private or community cloud, on the other) ensure an informed choice is made, rather than relying on generalisations about the relative risk exposure of different options, which do not always withstand scrutiny.

Strategy

APRA recommends an appropriate amount of rigour is applied to planning your cloud IT environment and your transition.

We agree with APRA that a successful and considered transition to the cloud starts with a clear articulation of your organisation's strategic intent and a deep understanding of your internal context.

Infrastructure cost reduction is a common benefit of moving to the cloud, but there are many others, such as the ability to modernise service delivery, take advantage of improved mobile security, and redirect ICT staff to higher value work. One way to clarify your organisation's strategic intent is to classify the expected benefits of moving to the cloud as efficiency, effectiveness or performance benefits across the affected business areas. This helps to concisely and clearly convey the overall strategic intent to your stakeholders (including the Board and senior management), alongside the thorough risk assessment that you are also required to provide.

Understanding your organisation's internal context is crucial, since the decision to move to the cloud does not occur in an organisational vacuum. APRA's 2018 Information Paper acknowledges the importance of understanding the required changes in organisational capability. We think some of the key structural, cultural and technological factors can be brought to the surface and integrated into your cloud adoption strategy by asking questions such as those set out below.

Structural

- Which business units and processes will be affected by the solution under consideration?
- What resource limitations exist?
- How flexible is the organisation to structural change and resource reassignment?

Cultural

- Is the workforce culture receptive or resistant to technology innovation?
- What is the workforce awareness of risk and security process?
- What is the organisation's adoption of work-at-home and work-remote practices?

Technological

- What technology platforms are deployed within the organisation today?
- How will the cloud service be integrated with existing IT assets that will remain part of the overall architecture, particularly in areas like identity and access control, management and monitoring, and information protection?
- How modern is the existing technology experience of users within the organisation?

Governance

APRA encourages financial services institutions to develop a governance framework that takes into consideration immediate and future needs.

In the 2018 Information Paper, APRA outlines specific categories of information that your organisation is expected to provide to your governance authority to support its review and decision-making on the proposed outsourcing. A broad range of detailed information must be provided, including the business case for the proposed solution, high-level risk and control assessments, a summary of the due diligence undertaken, and governance and assurance frameworks.

This information is necessarily specific to your proposed use scenario, and it will address the people and process aspects of the outsourcing, as well as the technology dimension.

We offer a range of resources to help you communicate relevant information about Microsoft cloud services during your due diligence process. These include recent audit reports, ISO Statements of Applicability, and checklist tables mapping the contractual requirements set out in the Outsourcing Prudential Standards[5] to the relevant terms in Microsoft cloud contracts. We can best contribute to your due diligence process by being looped in early and having visibility into your assessment. Please contact your Account Manager to let us know how we can help.

5. Prudential Standards CPS 231 and SPS 231

Solution selection process

APRA advises the selection of cloud computing services should be conducted in a systematic and considered manner.

To minimise risk where possible, APRA calls for a systematic and considered selection process that follows your existing processes for changing your IT environment, including engaging with risk, security, outsourcing and assurance functions.

Microsoft's SAFE Handbook is one tool that may assist your organisation in undertaking a selection process that is consistent with APRA's expectations. SAFE follows a five-step, vendor-neutral process that guides an organisation's evaluation of alternative options for their implementation of modern business applications (including cloud services), principally from the perspective of security assurance.

APRA urges regulated entities to consider Australian-hosted options, and services that are used only by parties that have comparable security requirements – often known as community clouds – as ways to minimise inherent risk.

Azure, Office 365 and Dynamics 365 are available from our Australian data centres, and we make specific contractual commitments to store categories of data at rest in the Australian geography in the Online Services Terms. This helps to mitigate country and compliance risks that APRA is concerned about in offshoring scenarios.

Microsoft also provides an option for APRA-regulated entities to deploy Azure from our Azure Australia Central data centre region, which is open only to Australian and New Zealand government entities and an exclusive whitelist of commercial customers that provide critical infrastructure services. As explained on page 6 of this paper, this option provides the equivalent of a community cloud offering for the financial services sector.

Furthermore, our extended contract terms and the optional compliance program provide our financial services customers with additional assurance. As explained on page 6 of this paper, our multi-tenant public cloud services are designed to facilitate compliance by our most highly-regulated customers, even if not all of our customers are subject to the same requirements.

Finally, it is important to not just analyse the risk associated with the service under consideration, but to compare that risk profile with the risk associated with maintaining the status quo or adopting an alternative. This is the only means by which accurate conclusions on relative risk exposure can be made.

More information

SAFE Handbook
aka.ms/safehandbook

Online Services Terms
microsoft.com/contracts

APRA access and ability to act

The 2018 Information Paper adds APRA access and ability to act as a new risk management consideration. This is an increasing concern of regulators around the world.

Microsoft contractually commits to provide your financial services regulators with a direct right to examine the online services, including the ability to conduct on-premises examinations, meet with Microsoft personnel and Microsoft's external auditors, and to access any related information, records, reports and documents. Regulators can then engage with us to help them understand the services and the relevant control frameworks that we have in place.

Transition approach

According to APRA, a cautious and measured approach should be adopted when transitioning to a cloud computing service.

Several of our financial services customers have piloted the use of Microsoft cloud services in discrete parts of their organisations before making adjustments, where necessary, and migrating fully to Microsoft cloud services. This approach is consistent with APRA's advice to adopt a measured transition strategy, and it is something that Microsoft is uniquely well placed to support given our customers' ability to move between on-premises and cloud versions of our products.

Microsoft makes available a range of tools and resources to assist our customers with an appropriate migration strategy. The Microsoft FastTrack Centre enables customers to request onboarding assistance and technical guidance, including architectural blueprints to embed in their control framework.[6] Project-based customer success plans support Microsoft, partners and customers in planning service rollouts across Azure, Office 365 and Dynamics 365. These plans often provide for customers to introduce cloud-based capabilities into their on-premises environments so that they can migrate to the cloud or adopt new features at a pace appropriate to their business. We also have in-house expertise at Microsoft Consulting Services and an extensive network of qualified partners who can assist with advanced requirements.

It is also important to bear in mind your organisation's own role in configuring and securing the service as part of the transition process. For example, you will need to configure the cloud service to meet your organisation's security requirements and establish your own on-premises controls and practices to support cloud adoption. Think about issues such as who will have administrative access to the cloud service, be capable of configuring the service, or adding new users? How will users be authenticated, and how will their credentials be distributed? How will user access be revoked if they leave the organisation?

6. See fastrack.microsoft.com for more information about our deployment assistance program

Risk assessments and security

APRA recommends that a regulated entity conduct thorough security and risk assessments initially, periodically and on material change.

When reviewing risk and security assessments, APRA has observed weaknesses in both the assessment of identified risk, and the strength and nature of the controls implemented to mitigate that risk. Microsoft agrees with APRA that the assessment process should result in clearly defined granular risks, and the implementation of proportionate controls. This allows for meaningful understanding and evaluation of the risk impact on your organisation, and effective risk treatment.

Microsoft makes available a variety of resources to help you identify common risk events associated with the use of cloud services. For example, the SAFE Handbook contains a risk event catalogue of approximately 50 of the most commonly assessed risks, which your organisation can add to, or subtract from, depending on circumstances. The handbook also provides an explanation of threat modelling, which is a useful technique for more deeply examining the possible conditions that may result in a risk being realised, and the security mitigations you can implement to reduce the event's probability or impact.

The Office 365 Customer Security Considerations Framework, which maps Office 365 security and compliance features to key risk events or threats, is another useful tool. It explains how customers can configure and implement controls to help treat the risks identified.

We also have Australian-specific factsheets and checklists prepared for APRA-regulated entities to assist with your risk assessment process.

Finally, we make available detailed information on the controls – both service-side and customer-side – that come with our services. By way of example, the table below details the data isolation controls in Azure, Office 365 and Dynamics 365. Data isolation is one of the specific areas of control weakness that APRA cites in the 2018 Information Paper.

Similar information is available for the other controls that underpin Microsoft cloud services, including through mapping documents for frameworks such as ISO/IEC 27001 and the Cloud Security Alliance's Cloud Control Matrix. In addition to reviewing Microsoft's service-side controls, we also recommend that our customers consider the customer-side controls, separate from the cloud services, that they can implement to further treat the risks identified as part of their risk and security assessments. Often these controls will involve organisational processes that are designed to ensure the ongoing secure use of cloud services.

More information

SAFE Handbook
aka.ms/safehandbook

Trust Center
microsoft.com/trustcenter

Service Trust Portal
trustportal.office.com

Cloud service	Data isolation controls
Office 365	• All Office 365 services and workloads are built on top of Azure Active Directory and as a result they use the same authorisation and role-based access control (RBAC) model. • All Office 365 requests are mediated through authorisation and access control features in Azure Active Directory. • All Office 365 data sessions are either user-scoped or tenant-scoped, and users can't see outside the tenant scope. • Access to Office 365 objects is controlled via user account permissions that are enforced by Azure Active Directory. • The authorisation stack prevents people from accessing data without appropriate credentials. • There is no service code that allows a user from one tenant to execute commands against another tenant. • Encryption of Office 365 customer data at rest is provided by multiple service-side technologies. • Office 365 Service Encryption includes an option to use customer-managed encryption keys that are stored in Azure Key Vault. • For customer data in transit, all Office 365 servers negotiate secure sessions using TLS by default.
Azure	• Azure uses logical isolation to segregate each customer's environment and data. The core of this logical isolation is Azure Active Directory for authorisation and role-based access control (RBAC). • In addition to Azure Active Directory, individual Azure services provide additional data isolation measures which are outlined at https://docs.microsoft.com/en-us/azure/security/azure-isolation. • As an example, for compute resources, also known as virtual machines, the isolation is enforced by the hypervisor which grants customer access only to the virtual machine resources that belong to their Azure subscription. • Data in Azure Storage is controlled with a Storage Access Key (SAK). Shared Access Signature (SAS) tokens can be generated using SAKs to provide more granular, restricted access. • Network controls block customer-to-customer access to Azure services. No internet access is enabled by default.
Dynamics 365	• Dynamics 365 provides customers with logical data isolation through separate SQL databases. • Every Dynamics 365 customer also receives a unique identifier in the service, which restricts access by default to that customer's domain, for customer-to-customer data separation. • Microsoft uses encryption technology to protect customer data in Dynamics 365 while at rest in a Microsoft database. While in transit between user devices and our data centres, data is encrypted using industry-standard Transport Layer Security (TLS).

Implementation of controls

The 2018 Information Paper newly includes this risk management consideration with a specific emphasis on controls that a regulated entity is responsible for under the shared responsibility model.

As APRA explains, cloud services are based on a shared responsibility model which varies by the type of service.[7] A weakness APRA has observed is inadequate consideration of the roles and accountabilities under the shared responsibility model, in particular the controls for which the regulated entity is responsible. These will generally include ongoing monitoring for control effectiveness, customer-side information security, and data quality, among other areas of responsibility.

As discussed above, we provide visibility into customer-side and service-side controls. Compliance Manager is a useful tool which allows you to create your own assessments and monitor your own controls. With respect to service-side controls, we provide you with visibility and monitoring capability through the Service Trust Portal, Compliance Manager, Office 365 Audited Controls, Office 365 Management Activity API, Azure Security Center, Azure Advisor, and the Microsoft Trust Center, as well as audit logs. These are detailed further in the section below.

APRA identifies timely detection of unauthorised access and usage of the regulated entity's environment as a key control objective. Microsoft has clearly documented security incident response and notification contract commitments and procedures, available in the Online Services Terms and on the Service Trust Portal, respectively. Under such procedures, all security incidents are promptly notified to the designated security contacts of the impacted organisation(s). In situations that do not involve security incidents where a Microsoft engineer is required to access a customer environment, we have a clearly defined process that includes executive level approval and access via secure administrative workstations on a time-restricted basis. This process can be enhanced with our Customer Lockbox feature which gives the customer full control of access request approvals and provides a complete audit trail.

A key responsibility of the regulated entity is the ongoing evaluation of the design and operating effectiveness of controls. As part of this responsibility, APRA highlights the need for you to review third-party audit reports of the service provider, and supplement these as you consider necessary. Microsoft provides audit reports on the Service Trust Portal and beyond that enable access to information, Microsoft personnel, and Microsoft's external auditors, as well as opportunities for deeper monitoring, supervisory and audit rights through the Compliance Program.

More information

Online Services Terms
microsoft.com/contracts

Service Trust Portal
trustportal.office.com

Ongoing oversight

APRA recommends that entities manage material service providers proactively and receive sufficient information on a regular basis to enable effective oversight.

Transparency is a key pillar of Microsoft's Trusted Cloud strategy. Through a combination of service capabilities and contractual commitments, we provide visibility into how our cloud services are operating, so that you have sufficient information to maintain effective oversight over them.

Service health can be monitored through publicly available sources, such as the Office 365 Service Health Dashboard and Azure Status dashboard, or via the Administration Portal for the relevant service. This information helps you assess our performance against our contracted Service Level Agreements, which provide financially backed availability guarantees.

The Service Trust Portal and Office 365 Service Assurance give you access to the latest audit reports for our services, so that you can gain regular insight into the effectiveness of the controls we have implemented to meet the requirements of industry-leading control frameworks such as ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2.

7. APRA, 2018, Information Paper: Outsourcing involving cloud computing services, p18 (see table)

Ongoing oversight (continued)

APRA recommends that entities manage material service providers proactively and receive sufficient information on a regular basis to enable effective oversight.

We also provide service-specific features to assist with ongoing monitoring, including Office 365 Audited Controls, the Office 365 Management Activity API and the Azure Security Center.

With Audited Controls for Office 365, we map our Microsoft internal control system to international standards, such as ISO/IEC 27001 and ISO/IEC 27018. We also provide our customers with a Compliance Manager tool, which provides detailed information about each of our internal controls, including the test status and most recent test date. This puts our customers in the position of being able to perform their own assessment of the risks of using Office 365.

The Office 365 Management Activity API provides users with a high level of visibility into user, admin, system and policy actions and events from your Office 365 and Azure Active Directory activity logs. You can use the actions and events from these activity logs to create tailored solutions that deliver monitoring, analysis and data visualisation.

Finally, the Azure Security Center provides visibility into the security state of your Azure resources, and the ability to respond to threats and vulnerabilities. Azure Advisor provides continuously proactive and intelligent guidance on how you can further improve your security posture.

Contractually, we commit to promptly notifying you of security incidents that affect your data, so that you are empowered to take any further mitigation or remediation steps that you deem appropriate.

Our extended contract terms for financial services customers also add the ability for you and your regulators to examine the service to meet regulatory requirements. Through the optional compliance program for regulated financial services customers you can obtain an even deeper level of visibility into the operational aspects of our cloud services.

We provide participants with access to service operation data, insight into operational risks associated with the services, and notification of changes that may materially impact Microsoft's ability to provide the services. This is the type of ongoing engagement model that APRA notes would benefit regulated entities.

More information

Service Level Agreement, and Online Services Terms
microsoft.com/contracts

Office 365 Service Assurance, including Office 365 Audited Controls
protection.office.com

Office 365 Management Activity API
msdn.microsoft.com/library/office/mt227394.aspx

Office 365 Service Health Dashboard
https://status.office365.com/

Azure Security Center
azure.microsoft.com/en-us/documentation/services/security-center

Azure Status Dashboard
status.azure.com

Business disruption

APRA recommends that entities ensure that the IT environment can meet business recovery objectives in the event that IT assets become unavailable to reduce the impact of an incident.

APRA defines high availability as the techniques that ensure IT assets remain available in the event of the failure of individual components. This was previously referred to as 'resilience' by APRA in the 2015 Information Paper. Recovery, in turn, is the capability to ensure that the IT environment can meet business recovery objectives in the event that IT assets have become unavailable. APRA's view remains unchanged that, in assessing cloud computing services, regulated entities have typically relied too much on high availability, and inadequate consideration has been given to recovery. Regulated entities need to maintain recovery capability regardless of the availability of the solution.

Microsoft's Enterprise Business Continuity Management (EBCM) program is based on industry-leading practices. While Microsoft neither strictly endorses nor adheres to one specific set of external standards, Microsoft is actively engaged with various business continuity organisations, such as the ISO, Disaster Recovery International and the Business Continuity Institute. Our EBCM program covers business continuity, disaster recovery and service resiliency, and applies across all of Microsoft's business units. Business continuity plans are developed for our cloud services to document their critical processes and supporting dependences.

In accordance with the Microsoft EBCM policy and standards, Microsoft conducts testing of its business continuity and disaster recovery plans at least annually. Issues identified during testing are noted and managed to a resolution. Our testing and validation of plans is based on their criticality rating, in that all plans are required to validate at the level that is relevant to their criticality.

In addition to our own rigorous program of recovery across our all our cloud infrastructure, we provide mechanisms for customers to control backup and recovery themselves. For example, Azure Backup provides the ability to back up and restore virtual machines, and the Azure Import/Export service can be used to transfer large quantities of data residing in Azure Blob Storage to your on-premises installations. This gives you a great deal of control over how you choose to archive or even replicate data within your cloud computing services.

It's important to evaluate the sensitivity of your data along with your backup and integrity requirements. You may well find that the mechanisms for backup and recovery within a service like Office 365 are entirely capable of addressing your requirements. But you can also extend that service by configuring additional backup, recovery or integrity mechanisms to meet compliance or other obligations.

More information

Microsoft Enterprise Business Continuity Management Policy and Program, accessible via the Service Trust Portal
https://servicetrust.microsoft.com/

Audit and assurance

APRA recommends undertaking regular assurance activities that ensure risk and control frameworks, and their application, are designed and operating effectively in order to manage the risks associated with cloud computing.

Microsoft shares APRA's view that ongoing assurance of risk and control frameworks is critical to managing risk effectively. In a cloud service arrangement, building out an effective assurance model is a shared responsibility between customer and provider due to the fact that the control environments necessarily span both domains. The extent to which you interrogate different sources of assurance, and the weight that you place upon them, will vary with the specifics of the service you are implementing and the conclusions you draw about the associated risks.

Microsoft's multi-faceted approach to providing assurance starts with developing controls and features that our customers can deploy to reduce risk. This applies both on the service and the customer side. For example, on the service side, our Lockbox access control technology manages Microsoft engineering access to customer content without standing access – only on a just-in-time basis with limited and time-bound authorisation). On the customer side, Customer Lockbox for Office 365 is the customer-facing implementation of our Lockbox technology, which gives the customer explicit control to approve or deny access in the very rare instances when a Microsoft engineer may need to access customer content to resolve a customer issue. We provide transparency into 'what we do' via detailed architectural and operational information made available on the Trust Center and the Service Trust Portal, and 'what we did' via service features such as the Office 365 Management Activity API. We stand by our product by offering management attestations and contractual promises, and facilitate verification through our third-party audit reports and customer self-testing, which is made simple through service features such as Office 365 Audited Controls. These are all sources of assurance that you can build into your assurance model for your chosen service, and for many of our APRA-regulated customers, this multi-layered assurance from Microsoft is sufficient.

For those who require even greater insight, our compliance program for regulated financial services customers fits APRA's description of a 'collaborative assurance model' that goes beyond key control testing. The program provides an additional level of visibility into the design and operation of our services, through multiple channels and from several complementary perspectives (see page 27 for more detail).

3. APRA notification and consultation

In Chapter 3 of the 2018 Information Paper, APRA outlines the circumstances in which regulated entities must engage with APRA in relation to their outsourcing activities.

At the outset, it's important to note that APRA is concerned with cloud scenarios that involve outsourcing a 'material business activity'. If that threshold is not met, the Outsourcing Prudential Standards[8] do not apply, and there is no requirement for any consultation or notification process with APRA.

The APRA Outsourcing Prudential Standards define a 'material business activity' as one which 'has the potential, if disrupted, to have a significant impact on the regulated institution's business operations or its ability to manage risks effectively'.

Applying APRA's material business activity definition involves a very context-specific inquiry. Your organisation will need to look closely at the business processes and IT assets impacted by the proposed cloud service, as well as the service's projected uptake within your organisation. APRA also recommends scenario analysis of plausible security events as a useful technique for understanding the materiality of the arrangement.

If you conclude that your proposed use of Microsoft cloud services does involve the outsourcing of a material business activity, then you will need to assess risk and determine whether your outsourced service involves low, heightened or extreme inherent risk.

If your outsourced service involves low inherent risk (assessing the business function outsourced, and if deploying to the Azure Australia Central data centre region, with an exclusive whitelist of permitted customers – analogous to community cloud), and no offshoring (taking into account Microsoft's Australian data location contract commitments), then no consultation with APRA is required.

APRA encourages prior consultation after completing your internal governance processes if you are considering public cloud services or services with other heightened inherent risk factors, even if no offshoring is involved.

If your outsourced service involves extreme inherent risk, such as hosting of systems of record, then APRA encourages earlier consultation.

Microsoft is available to help you throughout any consultation or notification process with APRA. We're experienced in helping customers conduct risk assessments and engage with regulators to obtain approval. We can assist by providing resources to inform your business case and risk assessments, including the most recent audit reports for our cloud services, and checklist mapping tables that illustrate how the contracting requirements in the Outsourcing Prudential Standards are met in Microsoft contracts.

We are also happy to facilitate discussions with Microsoft subject matter experts to answer questions that arise in the course of your organisation's own due diligence or APRA engagement. Please contact your Account Manager to let us know how we can help.

8. Prudential Standards CPS 231 and SPS 231

Conclusion

APRA's updated 2018 Information Paper provides a more open regulatory approach to cloud, with specific guidance on how regulated entities can take up cloud computing services.

By relying on our comprehensive approach to risk assurance in the cloud, we are confident that Australian financial services organisations can move to Microsoft cloud services in a manner that is not only consistent with APRA's guidance but can provide customers with a more advanced security risk management profile than on-premises or other hosted solutions. This is due to the rigour and sophistication of the Microsoft control framework, the level of internal and external independent verification of those controls, and the pace of adoption of new security innovations capable of mitigating advanced threats.

Furthermore, prudent transition to cloud services can be the first and most important step for a financial institution on its digital transformation journey to optimise operations, empower employees, develop innovative products and services, and better engage customers.

Like APRA, we expect further innovation in how regulated entities manage risk in the cloud as new use cases and technologies emerge. We look forward to continuing to be at the forefront of that conversation for the benefit of our financial services customers in Australia and around the world.

Our compliance program for regulated financial services customers

This optional fee-based program provides additional monitoring, supervisory and audit rights, and additional controls over the online services, along with deeper, ongoing engagement with Microsoft, including:

- Ad hoc access to additional information from Microsoft subject matter experts (SMEs) – for instance, participants can ask questions or seek help or clarification about the standard service documentation.
- Access to additional compliance-related information that Microsoft may develop over time – such as customer FAQs, compliance summits or documents that provide insights into the underpinnings and plans for the compliance features of the online services.
- Opportunity to attend an annual compliance summit which includes technical presentations from senior engineering managers of the Office 365, Dynamics 365 and Azure services, audit and security tracks, data centre tours, and opportunities to engage deeply on audit issues.
- The opportunity for one-to-one discussions with Microsoft third-party auditors, if required.
- Participation in an annual webcast walk-through of ISO and Statement on Standards for Attestation Engagements (SSAE) audit reports with Microsoft SMEs. A recording of this webcast will also be made available for compliance program members.
- The option to view the Microsoft control framework for the services. This can enable a customer's risk officers to better understand and assess the scope and coverage of the framework (subject to more than 900 controls).
- The opportunity to recommend future additions to the audit scope of the service. All participants will be allowed to suggest new audit controls; the program's Financial Services Executive Committee (composed of one participant from each regulatory region) will agree on up to five controls for inclusion in future audits.
- Access to detailed reports of the external annual penetration tests conducted on the service.
- The option to assess overall service approach to risk management and the underlying risks associated with using the service.

Microsoft

Find out more

Australian Regulatory Compliance for Financial Services Customers
aka.ms/aufs

Asian Regulatory Compliance for Financial Services Customers
aka.ms/asiafs

Trust Center
microsoft.com/trustcenter

Service Trust Portal
https://servicetrust.microsoft.com/

Financial Services Amendment
Contact your Account Manager

Online Services Terms
microsoft.com/contracts

Compliance Program for Regulated Financial Services Customers
Contact your Account Manager

Service Level Agreements
microsoft.com/contracts

SAFE Handbook
aka.ms/safehandbook

Azure Australia Central Regions
aka.ms/aacr