Microsoft Cloud Services

Compliance with APRA Prudential Standard CPS 234 Information Security

Version: 26 February 2019

Introduction

Microsoft welcomes the introduction by the Australian Prudential Regulation Authority (APRA) of the Prudential Standard CPS 234 Information Security.

New prudential standard CPS 234 will help to shore up APRA-regulated entities' resilience against information security incidents, and their ability to respond swiftly and effectively in the event of a breach.

CPS 234 requires APRA-regulated entities to:

- clearly define information-security related roles and responsibilities;
- maintain an information security capability commensurate with the size and extent of threats to their information assets;
- implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls; and
- promptly notify APRA of material information security incidents.

CPS 234 closely mirrors the core Microsoft security framework: protect, detect and respond.

Microsoft is a leader in information security, and we embrace our responsibility to make the digital world a safer place. Deploying to Microsoft cloud services gives an APRA-regulated entity access to world-leading security technology, resources and controls, to help secure its data and operations, and comply with its CPS 234 regulatory obligations.

Microsoft cloud services deliver this information security capability and resilience against threats through:

- **Operations**: over 3,500 dedicated Microsoft cybersecurity professionals help protect, detect, and respond to threats – delivering security operations that work for your organisation.
- **Technology**: We use our experience to provide you with enterprise-class security technology.
- **Partnerships**: Microsoft is driving a broad set of technology, industry, and policy partnerships for a heterogeneous world.

This paper sets out each of the relevant CPS 234 regulatory obligations, and maps against it the Microsoft cloud service controls, capabilities, functions, contract commitments and supporting information to help your APRA-regulated entity comply with its regulatory obligations under CPS 234.

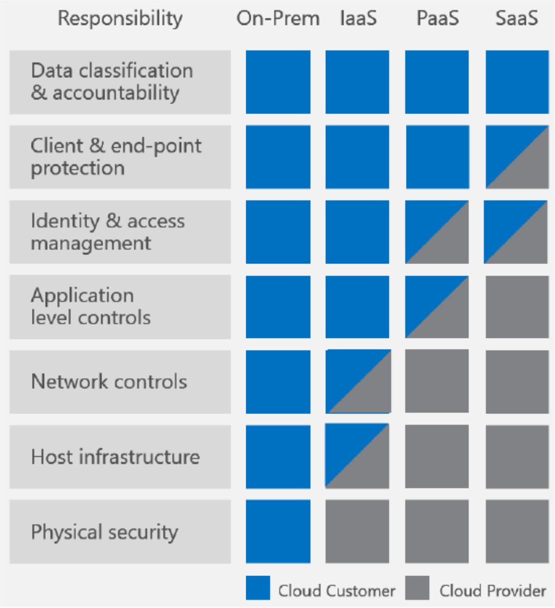
Furthermore, Microsoft Consulting Services offers many information security consulting offerings, in addition to the Microsoft cloud product features and offerings described in this paper, that can help your APRA-regulated entity comply with its obligations under CPS 234.

APRA-regulated entities should also consult Microsoft response to the APRA Information Paper on Cloud and Compliance checklist for financial institutions in Australia to round out the picture of how Microsoft cloud services help achieve and exceed regulatory compliance.

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

Microsoft Cloud Services: Compliance with APRA Prudential Standard CPS 234 on Information Security

Issue	CPS 234 Provisions	Compliance using Microsoft Cloud Services
Information security capability	15. An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity. 16. Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets. 17. An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.	There are several avenues through which APRA-regulated entities can assess the information security capability of Microsoft and evaluate the design of the information security controls of Microsoft cloud services. Together they ensure that you can meet your regulatory requirements and supervise the cloud services. 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 Azure 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. Furthermore, 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. The Microsoft Security Policy Governance White Paper provides an overview of Microsoft's Security Policy Framework, with links to the key Microsoft Security Policy documents. Customers can refer to the Azure Response on Security, Privacy and Compliance to assess Microsoft security capability for Azure, and underpinning Office 365 / Microsoft 365 and Dynamics 365 cloud services.

<table>
<tr><th>Issue</th><th>CPS 234 Provisions</th><th>Compliance using Microsoft Cloud Services</th></tr>
<tr>
<td><b>Policy framework</b></td>
<td>18. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.
19. An APRA-regulated entity’s information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.</td>
<td>Microsoft cloud services comply with several security frameworks, such as ISO 27001, PCI- DSS and FedRAMP etc. These frameworks mandate Microsoft to implement a comprehensive Vulnerability Management Framework for continuous assessment of known and unknown threats. Microsoft cloud security policy framework compliance offerings are committed in the “<i>Security Practices and Policies</i>” section of the Online Services Terms and are summarised at the Trust Center Compliance Offerings page.
An APRA-regulated entity’s information security policy framework should include roles for Microsoft, as cloud services provider, consistent with the customer-side and service-side controls in the shared responsibility model (see diagram below), and with contractual commitments in the Online Services Terms.
The figure below describes how shared responsibility works across the cloud service models.

<table>
<tr><th>Responsibility</th><th>On-Prem</th><th>IaaS</th><th>PaaS</th><th>SaaS</th></tr>
<tr><td>Data classification & accountability</td><td>🟦</td><td>🟦</td><td>🟦</td><td>🟦</td></tr>
<tr><td>Client & end-point protection</td><td>🟦</td><td>🟦</td><td>🟦</td><td>◩</td></tr>
<tr><td>Identity & access management</td><td>🟦</td><td>🟦</td><td>◩</td><td>◩</td></tr>
<tr><td>Application level controls</td><td>🟦</td><td>🟦</td><td>◩</td><td>⬛</td></tr>
<tr><td>Network controls</td><td>🟦</td><td>◩</td><td>⬛</td><td>⬛</td></tr>
<tr><td>Host infrastructure</td><td>🟦</td><td>◩</td><td>⬛</td><td>⬛</td></tr>
<tr><td>Physical security</td><td>🟦</td><td>⬛</td><td>⬛</td><td>⬛</td></tr>
</table>
🟦 Cloud Customer ⬛ Cloud Provider
For more information, see our White Paper on Shared Responsibilities for Cloud Computing and related Blog Post.</td>
</tr>
</table>

Issue	CPS 234 Provisions	Compliance using Microsoft Cloud Services
Information asset identification and classification	20. An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.	Microsoft has implemented and commits to maintain specified security measures for Customer Data in the Core Online Services, including Asset Inventory and Asset Handling practices and other security commitments set out in the Microsoft Online Service Terms (OST). Additionally, Microsoft has cloud service offerings that leverage data classification and protection technologies to help APRA-regulated entity discover, classify, protect and monitor their sensitive data, across devices, apps, cloud services and on-premises. Examples of Microsoft Information Protection solutions can be found here, including Azure Information Protection, Office 365 Information Protection, Windows Information Protection, and Microsoft Cloud App Security. Office 365 / Microsoft 365 also has further advanced capabilities that helps APRA-regulated entity meet higher level of assurance and compliance requirements. Examples include: • Advanced electronic discovery • Data governance and retention • Bring-your-own service encryption key • Control how Microsoft support engineer access your data • Privileged access management For Azure SQL, there are data security capabilities that support data discovery and classification, along with data masking and encryption.
Implementation of controls	21. An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with: (a) vulnerabilities and threats to the information assets; (b) the criticality and sensitivity of the information assets; (c) the stage at which the information assets are within their life cycle; and (d) the potential consequences of an information security incident. 22. Where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party's information security controls that protects the information assets of the APRA-regulated entity.	To evaluate the design of Microsoft's information security controls, regulated customers should review: • Microsoft Security Policy Governance White Paper, which provides an overview of Microsoft's Security Policy Framework, with links to the key Microsoft Security Policy documents. • Information Security Management System for Microsoft's Cloud Infrastructure • Office 365 Security Incident Management • Azure Security Response in the Cloud • Assessment of Azure and the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) security, privacy, compliance, and risk management requirements Microsoft Secure Score helps the APRA-regulated entity to find, assess and mitigate risks, and proactively manage security controls of Microsoft cloud services. Secure Score analyses an organisation's security based on regular activities and security settings of respective Microsoft cloud service offerings, giving APRA-regulated entity security posture visibility, report on areas that require attention, as well as recommendations for actions to further reduce the attack surface in your organization. Microsoft Secure Score covers a number of Microsoft cloud service workloads, devices, identity: see Office 365, Azure Security Center, Windows 10, and Azure Active Directory.

Incident management	23. An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner. 24. An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans). 25. An APRA-regulated entity's information security response plans must include the mechanisms in place for: (a) managing all relevant stages of an incident, from detection to post-incident review; and (b) escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate. 26. An APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.	The Incident Management Implementation Guidance for Azure and Office 365 is a comprehensive document customers can use to harden the security posture of their Microsoft cloud environment. It outlines the best methods for configuring the tenant for optimal security incident management: prevention, detection, alerts, anomalous activity monitoring, and post-incident investigations, made possible by in-product logging capability. Microsoft's Office 365 Security Incident Management and Azure Security Response program documents also help you assess Microsoft's own incident management capabilities, policies and processes. Microsoft also supports your compliance through its "*Security Incident Notification*" commitments in the Online Services Terms: **"Security Incident Notification** If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. … Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident." "Microsoft has implemented and will maintain for Customer Data in the Core Online Services the following security measures: … **Incident Response Process** - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary." Furthermore, the optional Customer Compliance Program for regulated financial services customers provides for deeper information sharing by Microsoft about information security incidents and potential threats, including their nature, common causes and resolutions. Microsoft Threat Protection (MTP), and other Microsoft security products and capabilities, help APRA-regulated customers to comply with this obligation. MTP provides protection across Identities, Endpoint, User Data, Cloud Apps and Infrastructure. Microsoft facilitates compliance with the obligation to annually review and test the Microsoft cloud service information security response plans, to ensure they remain effective and fit-for-purpose, through our "Auditing Compliance" contractual commitments in the Online Services Terms, described further in the next section below.

Testing control effectiveness **&** **Internal Audit**	27. An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with: (a) the rate at which the vulnerabilities and threats change; (b) the criticality and sensitivity of the information asset; (c) the consequences of an information security incident; and (d) the risks associated with exposure to environments where the APRA-regulated entity is unable to enforce its information security policies; and (e) the materiality and frequency of change to information assets. 28. Where an APRA-regulated entity's information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, the APRA-regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs 27(a) to 27(e) of this Prudential Standard. 29. An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner. 30. An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists. 31. An APRA-regulated entity must review the sufficiency of the testing program at least annually or when there is a material change to information assets or the business environment. 32. An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance). 33. An APRA-regulated entity must ensure that the information security control assurance is provided by personnel appropriately skilled in providing such assurance. 34. An APRA-regulated entity's internal audit function must assess the information security control assurance provided by a related party or third party where: (a) an information security incident affecting the information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; and (b) internal audit intends to rely on the information security control assurance provided by the related party or third party.	Microsoft facilitates compliance with these regulations with respect to tests of the Microsoft cloud services thoughts its "Auditing Compliance" contractual commitments in the Online Services Terms: "**Auditing Compliance** Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows: • Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually. • Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework. • Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense. Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor." Furthermore, our extended contract terms for regulated financial services customers add the ability to examine the service more deeply to meet regulatory requirements. Regulated financial services customers that opt to join the Customer Compliance Program (including their internal and external auditors) have the right to conduct audits on Microsoft business premises, examine the control framework of the service, review its risk management framework, hold one-to-one discussions with Microsoft's independent auditors and obtain in-depth views directly from Microsoft subject matter experts.

Issue	CPS 234 Provisions	Compliance using Microsoft Cloud Services
APRA notification	35. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that: (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or (b) has been notified to other regulators, either in Australia or other jurisdictions. 36. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.	Microsoft supports compliance through its "*Security Incident Notification*" commitments in the Online Services Terms, which are excerpted in the above "Incident Management" section of this paper. When Microsoft notifies the APRA-regulated entity of an information security incident, the APRA-regulated entity then "becomes aware" of the incident, and so must notify APRA as soon as possible and, in any case, no later than 72 hours, after receiving notice from Microsoft and evaluating whether the incident requires APRA notification under the criteria in section 35. Furthermore, the optional Customer Compliance Program for regulated financial services customers provides for deeper information sharing by Microsoft about information security incidents and potential threats, including their nature, common causes and resolutions. It is important to note that security incident monitoring is a shared responsibility. Microsoft cloud customers are responsible to detect some types of security incidents, and are not dependent upon Microsoft to detect those incidents. Microsoft provides the tools and resources outlined in the above "Incident Management" section of this paper to empower our customers to identify security concerns and detect security incidents.