Philip Catania, Corrs Chambers Westgarth

Philip Catania is the Partner-In-Charge of the Melbourne office of the Australian law firm, Corrs Chambers Westgarth. He has qualifications in law and computer science and prior to joining the legal profession was a computer programmer with the Australian Antarctic Division. He is Australia's representative on the International Technology Law Association and is on the Advisory Board of the University of Melbourne's Academic Centre for Cyber Security Excellence. Phil's practice is in technology transactions and data privacy and he represents many of the world's leading organisations in their AsiaPac data privacy matters.

MANAGING YOUR INFORMATION ASSETS

APRA's Prudential Standard CPS 234 Information Security

Philip Catania

With the frequency and seriousness of data breaches continuing to set new records each year in Australia and across the world, Australian regulators have begun laying down the law when it comes to data management, cyber resilience and information security practices.

The Australian Prudential Regulation Authority (APRA) *Prudential Standard CPS 234 Information Security*, which commenced on 1 July 2019, carries the force of law and establishes a host of information security requirements for authorised deposit-taking institutions such as banks and insurance providers (APRA entities). It signals APRA's increasing scrutiny of the way financial institutions manage and protect the data they hold.

However, those organisations that 'manage' the 'information assets' of APRA entities—including providers of cloud based services, IT infrastructure providers, IT implementation and support providers, data hosters and managers and so on—are also impacted by CPS 234, and need to understand their obligations in full.

Below is a snapshot of what we've learned about CPS 234 in practice to date.

Key requirements under CPS 234

CPS 234 establishes various security requirements in respect of an APRA entity's 'information assets'—essentially any form of information technology, including software, hardware and data. This term is defined in much broader terms than 'personal data' or 'personal information' (which is used in privacy and data protection laws and only applies to natural persons). Information assets are not subject to a materiality limitation, therefore APRA entities must ensure that any steps taken to comply with CPS 234 account for all the different forms of information assets relating to their business.

The core requirements under CPS 234 fall into two distinct categories.

Under the first set of requirements, APRA entities must establish the following information security practices:

- **Information security capability.** The APRA entity must actively maintain an information security capability which enables the continued sound operation of the ADI.
- **Implementation of controls.** The APRA entity must establish information security controls to protect the ADI's information assets across their life-cycle.
- **Testing control effectiveness.** The APRA entity must establish systemic testing programs which are able to test the effectiveness of its information security controls.

- **Incident management.** The APRA entity must establish robust mechanisms and plans to detect and respond to information security incidents that could plausibly occur.
- **Internal audit.** The APRA entity must ensure that their internal audit activities include a review of the design and operating effectiveness of information security controls.

Sitting neatly beside this is the second set of core requirements—where a service provider manages the information assets of an APRA entity, the APRA entity must assess and review the adequacy of the service provider's information security practices in protecting those information assets.

Who 'manages' the information assets of an APRA entity?

If an organisation is providing software, hardware, data or any service relating to the software, hardware or data of an APRA entity, then there is a good chance that the organisation is a service provider that 'manages' the information assets of the APRA entity and will be caught by the operation of CPS 234.

Third party implications of CPS 234

Rolling down requirements

APRA entities' responsibilities to comply with CPS 234 extend to all their information assets managed by third parties and entities that those third parties may sub-contract to. Therefore, in addition to setting out rights to review and assess, APRA entities will seek to roll down obligations for service providers to establish all of the above information security practices in respect of the particular information assets being managed by the service provider. In order to reduce the costs of compliance, service providers might need to consider categorising and segregating the assets it manages that belong to APRA entities from those that belong to other clients from other industries so that it can apply the relevant security practices selectively where required. This, we know, is often easier said than done.

Contractual considerations

APRA entities have until the earlier of the next contract renewal date or 1 July 2020 to ensure that their arrangements with third party service providers comply with CPS 234. Existing contractual arrangements with service providers are being reviewed and amended to incorporate CPS 234 obligations. These new contractual revisions will need to be consistent with any existing clauses relating to privacy, security, confidentiality, enforcement and termination.

Flexibility in compliance measures

Contractual considerations are but one part of the 'arrangements' that must be adopted in order to comply with CPS 234 and are, on their own, certainly not enough to establish compliance. It is important to understand that CPS 234 does not set out specific requirements to establish any contractual measures when dealing with service providers (unlike CPS 231 Outsourcing, which sets out a list of prescribed contractual requirements when threshold issues are satisfied). In contrast, the requirements under CPS 234 are framed in broad high-level terms which provide relevant entities with the flexibility to adopt any measures that are appropriate or commensurate with the nature of the information assets.

APRA's practice guide CPG 234

APRA has released a practice guide which provides examples of the types of information security practices that entities can adopt in complying with CPS 234. For example, the testing controls that might be established include:

- appropriate blocking, filtering and monitoring of electronic transfer mechanisms
- encryption and segregation of sensitive data sets
- continually updating software security and ensuring it complies with the information security policy framework
- establishing approval and verification processes whenever requests for access are made; and
- maintaining physical and environmental controls such as fire suppressant systems.

Other key considerations for APRA entities and service providers

Governance and responsibility for compliance

CPS 234 vests ultimate responsibility of an entity's information security management with the Board of the APRA entity, whose roles and duties must be clearly defined. The Board will need to be ready to evidence any steps taken to comply with CPS 234, and to be aware of enforcement actions that could be taken in the event of non-compliance, both by APRA and by ASIC for breaches of directors' duties relating to care, skill and diligence, which will now be framed by the obligations under CPS 234.

Synergies with CPS 231 Outsourcing

Where arrangements between APRA entities and service providers involve the outsourcing of a material business activity relating to the sharing or managing of information assets, both CPS 231 (relating to outsourcing) and CPS 234 will apply. Given that the obligations flowing from these dual regulations have a high degree of cross-over (such as the requirements to undertake auditing and reporting procedures, maintain information security and specify ownership and control of data), there are synergies that may be exploited in the process of uplifting agreements and implementing procedures in accordance with APRA's prudential standards.

Notification requirements

APRA entities must notify APRA of any information security control weaknesses or information security inci-

The quote

APRA entities have until the earlier of the next contract renewal date or 1 July 2020 to ensure that their arrangements with third party service providers comply with CPS 234.

dent that is material or has been notified to any other regulator (both Australian and foreign). Notification must be provided even where those information assets are being managed by third parties and, in the case of an information security incident, must be notified to APRA within 72 hours after the APRA entity becomes aware of the relevant incident or vulnerability; hence the obligations APRA entities place on service providers to notify them of such matters.

Extent of access to information security practices

Service providers should consider the extent to which they allow APRA entities to assess and review their information security practices. It is unclear what level of assessment and review will be required in order for APRA entities to satisfy their obligations under CPS 234. However, at a minimum, service providers can expect:

- APRA entities to push for some level of on-site inspections of their service providers' premises; and
- a requirement for service providers to produce a regular services report that clearly explains the information security practices being implemented.

APRA's ushering in of new information security practices for APRA entities and their service providers offers a glimpse into how Australian regulators will respond to the growing tsunami of data and information that businesses are accumulating. In the wake of stern admonishments under the Financial Services Royal Commission, APRA will look to rigidly enforce its new standard to stem the increasing flood of cyber risks posed by Big Data. Service providers to this industry need to be very aware of this. **FS**