Implications of draft prudential standard CPS 234 Information Security

Building a better working world

APRA's view is that, despite no regulated entity having yet suffered material losses as a result of an information security incident, this "is not grounds for complacency" and "preparedness is vital".[1]

Introduction

Draft prudential standard CPS 234 Information Security aims to improve the resilience of regulated entities against information security threats. It fills a gap in the existing prudential framework, supplementing the existing prudential standards CPS and SPS 220 Risk Management. It extends and elevates to a prudential standard the existing practice guide, CPG 234 Management of Security Risk in Information and Information Technology. This distinction is important: regulated entities will have to demonstrate compliance with the new standard across all of its provisions, rather than simply follow the guidance.

Key points

Draft prudential standard CPS 234 requires a regulated entity ("entity") to demonstrate the maintenance of an information security capability that:

- is commensurate with the vulnerabilities and threats to which its information assets are exposed
- enables the continued, sound operation of the entity

It focuses on minimum standards for managing information security and places ultimate responsibility for information security with the Board. Entities will need to consider their extended business environment, including third parties which manage its information assets. Specific requirements include:

- Clear definitions of information security-related roles and responsibilities
- Implementation of controls across the extended business environment, which are commensurate with the criticality of assets and the threat
- Systematic testing and assurance of controls effectiveness
- Notification to APRA of both material incidents and material controls weaknesses

APRA intends to finalise the proposed standard towards the end of 2018, with a view to implementing CPS 234 from 1 July 2019.

1. APRA Discussion Paper, "Information security management: A new cross-industry prudential standard", published 7 March 2018, paragraph 1.1

What are the key requirements?

The threats are evolving, and so must your capabilities

CPS 234 makes it incumbent on an entity to understand the key information security threats to its information assets, and to ensure this understanding is current, against the backdrop of a constantly evolving threat environment.

Recent major cyber attacks demonstrate the need for entities to consider an ever-wider set of threats and threat actors.

It is not sufficient to only consider threats which target you specifically. This goes beyond indiscriminate "spray and pray" campaign by unsophisticated actors, such as commoditised ransomware campaigns. 2017's "Not-Petya" and "WannaCry" malware attacks showed how businesses could become collateral damage where state actors are believed to have deployed cyber weapons as a sub-kinetic strategic option. Take the Not-Petya attack: this was a suspected Russian operation, targeting Ukrainian businesses with weaponsgrade, data-destroying malware. However, the effects were felt far beyond the Ukrainian target set, disrupting businesses across the world and, in some cases, causing very significant financial losses.

1. Clear definitions of roles and responsibilities, including for the Board

CPS 234 requires that an entity clearly defines the information security-related roles and responsibilities of the Board, and of senior management, governing bodies and individuals. This requirement expressly places ultimate responsibility for information security on the Board, reflecting APRA's intention to close an observed gap in Board engagement on information security.[2] To address this gap, Boards will need to ensure that they are provided with the information they require to fulfil their legal and regulatory responsibilities. This may involve board education to ensure the Board has a strong grasp of information security fundamentals, and ongoing provision of appropriate reporting and controls metrics, as well as briefings on the changing threat.

The requirement will drive entities to focus on the operating models for their information security and risk functions, including the implementation of three lines of defence. More mature entities are already evolving their cyber functions and increasing the scope and scale of their second line cyber risk functions. All entities will need to develop a clear information security operating model with appropriately defined roles and responsibilities.

2. Maintaining capabilities that keep pace with the evolving threat

The draft standard requires that an entity maintains an information security capability commensurate with the size and extent of the threats to its information assets, and which enables the continued sound operation of the entity. Information security "capability" refers to resources, skillsets and controls.Underlying this requirement is the need for an entity to understand both its information assets and the threats to which they are exposed.

Understanding your assets ...

An entity will need to identify and classify its information assets by criticality and sensitivity, whether these assets are managed by the entity itself or by a third party on its behalf. Whilst many entities have developed an information asset inventory, few will be able to say with confidence that their inventory provides a comprehensive view of where all key information assets reside, whether self-managed or managed by a third party. Visibility may be further hindered where poor controls over procurement practices have led to information assets residing in 'shadow IT' or with third parties of which the security team has no knowledge. Entities will also need to ensure that their identification of assets extends to include unstructured data (e.g., spreadsheets, documents, PDFs, etc.), where information assets also reside.

... and the threats to which they are exposed

Having identified its information assets, an entity will need to understand the size and extent of the threat to which they are exposed. This will require rigorous analysis of the threat environment, focussing both on threats which specifically target them, and also on less discriminate threats to which they could exposed, even if they are not the intended target (see text box below). And of course the cyber threat environment is in constant flux: entities will need to regularly refresh their assessment of the threats.

2. APRA Discussion Paper, "Information security management: A new cross-industry prudential standard", published 7 March 2018, paragraph 3.1

3. Implementing controls that are commensurate to the threat — and testing their effectiveness

APRA will require that an entity's information security capability delivers controls to protect information assets, including those managed by third parties, which are commensurate with:

- Threats and vulnerabilities related to the information assets
- Criticality and sensitivity of the information assets
- Information asset lifecycle stage
- Potential consequences of a security incident[3]

APRA will also require entities to implement "systematic controls testing, performed by appropriately skilled and functionally independent specialists".[4] This will require many entities to implement a broader regime of controls testing beyond the mainstays of penetration testing and disaster recovery testing. Entities will need to develop a systematic approach towards determining which controls should be tested and at what cadence, taking into account how the threats are changing and the criticality of the relevant assets. APRA will require that entities' testing goes beyond the controls in their own environment, and that entities also assess whether key third parties are carrying out adequate testing.

Preparing for the worst

In terms of specific controls, the draft standard provides that entities must maintain information security response plans for plausible scenarios and annually confirm that these are effective. Accordingly, an entity will need to determine what constitutes a 'plausible' information security scenario for it, leveraging the analysis of its information assets and the threat environment (see paragraph 2 above). Effectiveness of plans can be determined to some extent by tabletop review, but there is probably no substitute for testing the plans through simulated scenario-based exercises at both leadership and operational levels in the organisation.

Bolstering the third line of defence

Most organisations will need to bolster their information security internal audit programs: CPS 234 requires that internal audit activities include a review of design and operating effectiveness of controls, including those maintained by related or third parties (e.g., IT service providers, cloud providers). This assurance should be provided by "personnel appropriately skilled in providing information security assurance".[5]

Given the tight market for information security skills which is felt across the three lines of defence, but arguably most acutely in internal audit, many organisations will seek external assistance with these assurance activities. The information security operating model should also facilitate internal audit bringing to the Board's attention concerns over lack of visibility of third party assurance over the entity's information assets or the robustness of that assurance.

3. Draft CPS 234, paragraph 20
4. Draft CPS 234, paragraph 26
5. Draft CPS 234, paragraph 32

4. Notification of incidents and controls weaknesses

This proposal marks a significant shift in that APRA will require notice not just of information security incidents (within 24 hours),[6] but also of material internal controls weaknesses that may not be addressed in a timely manner (within five business days of identification).[7] This is likely to cause a degree of concern amongst regulated entities over determining what constitutes a "material controls weakness", and how APRA will respond to such disclosures. APRA has promised guidance to provide further clarity on the notification requirements, and is seeking industry feedback on their feasibility.

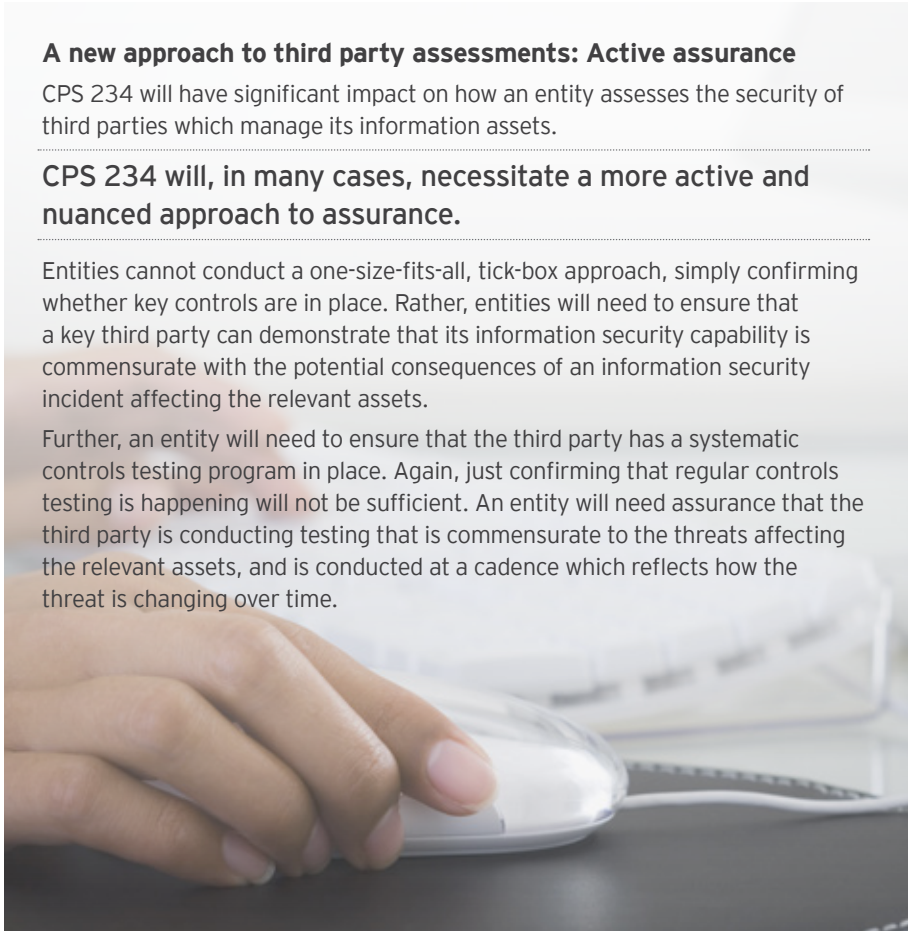
A new approach to third party assessments: Active assurance

CPS 234 will have significant impact on how an entity assesses the security of third parties which manage its information assets.

CPS 234 will, in many cases, necessitate a more active and nuanced approach to assurance.

Entities cannot conduct a one-size-fits-all, tick-box approach, simply confirming whether key controls are in place. Rather, entities will need to ensure that a key third party can demonstrate that its information security capability is commensurate with the potential consequences of an information security incident affecting the relevant assets.

Further, an entity will need to ensure that the third party has a systematic controls testing program in place. Again, just confirming that regular controls testing is happening will not be sufficient. An entity will need assurance that the third party is conducting testing that is commensurate to the threats affecting the relevant assets, and is conducted at a cadence which reflects how the threat is changing over time.



Contacts

Anthony Robinson
Sydney
+61 2 9248 5975
anthony.robinson@au.ey.com

Dinesh Santhiapillai
Melbourne
+61 3 9288 9195
dinesh.santhiapillai@au.ey.com

John Hare
Sydney
+61 2 9276 9247
john.hare@au.ey.com

Richard Watson
Sydney
+61 2 9276 9926
richard.watson@au.ey.com

Rohit Rao
Melbourne
+61 3 9655 2603
rohit.rao@au.ey.com

Georgina Crundell
Brisbane
+61 7 3011 3186
georgina.crundell@au.ey.com

6. Draft CPS 234, paragraph 35
7. Draft CPS 234, paragraph 34