Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018

EXPLANATORY STATEMENT

Prepared by the Australian Prudential Regulation Authority (APRA)

Banking Act 1959, section 11AF
Insurance Act 1973, section 32
Life Insurance Act 1995, section 230A
Private Health Insurance (Prudential Supervision) Act 2015, section 92
Superannuation Industry (Supervision) Act 1993, section 34C

APRA may, in writing, determine a prudential standard that applies to an APRA-regulated institution under:

(1) subsection 11AF(1) of the *Banking Act 1959* (Banking Act), in relation to authorised deposit-taking institutions (ADIs) and authorised non-operating holding companies (authorised NOHCs);

(2) subsection 32(1) of the *Insurance Act 1973* (Insurance Act), in relation to general insurers and authorised non-operating holding companies (authorised insurance NOHCs);

(3) subsection 230A(1) of the *Life Insurance Act 1995* (Life Insurance Act), in relation to life companies (including friendly societies) and registered non-operating holding companies (registered life NOHCs);

(4) subsection 92(1) of the *Private Health Insurance (Prudential Supervision) Act 2015* (Health Insurance Act), in relation to private health insurers; and

(5) subsection 34C(1) of the *Superannuation Industry (Supervision) Act 1993* (SIS Act), in relation to RSE licensees.

On 30 November, APRA made cross-industry (prudential standard) determination No. 1 of 2018 (the instrument) which determines *Prudential Standard CPS 234 Information Security* (CPS 234).

The instrument commences on 1 July 2019.

1. Background

Sound risk management is a key foundation to APRA's prudential framework across all APRA-regulated entities, and includes the management of information security. Effective information security is increasingly critical as information security threats and attacks escalate in frequency, sophistication and impact.

2. Purpose and operation of the instrument

APRA has made a new prudential standard designed to ensure that APRA-regulated entities have in place appropriate information security capabilities to be resilient against information security incidents. APRA has previously released guidance on

managing security risk in information and information technology. However, given the criticality of information security to the operation of entities in the regulated financial sector and the varying levels and sophistication of information security in APRA-regulated entities, APRA considers it appropriate to set out its expectations as to minimum standards in a prudential standard.

CPS 234 will require an APRA-regulated entity to:

- classify its information assets by criticality and sensitivity to determine the potential impact of an information security incident on the entity and the interests of beneficiaries and other customers;

- clearly define the information-security related roles and responsibilities of the Board, senior management, governance bodies and individuals;

- maintain an appropriate information security capability;

- implement controls to protect information assets commensurate with the size and extent of threats to its information assets; and

- notify APRA of material information security incidents and certain information security control weaknesses.

In finalising CPS 234, APRA has made a number of modifications to the original draft version of the standard to address concerns raised by submissions. These changes will assist APRA-regulated entities in both implementing and complying with CPS 234 while continuing to meet the original objectives set out by APRA in proposing information security requirements. The key changes include:

- inclusion of definitions of key concepts underlying the standard, including criticality, sensitivity, confidentiality, integrity and accessibility;

- providing a transition period in relation to information assets managed by third parties on behalf of APRA-regulated entities;

- extending the maximum allowable timeframes from 24 hours to 72 hours for APRA-regulated entities to notify APRA of information security incidents that either materially affected, or had the potential to materially affect, the entity or the interests of depositors, policyholders, beneficiaries or other customers, or that had been notified to other regulators; and

- extending the maximum allowable timeframe from five to ten business days for APRA-regulated entities to notify APRA of a material information security control weakness which the entity expects will not be remediated in a timely manner.

APRA also made a number of additional drafting changes to the final CPS 234 to provide greater clarity.

Where CPS 234 refers to an Act, Regulation or prudential standard, this is a reference to the document as it exists from time to time, and which is available on the Federal Register of Legislation at www.legislation.gov.au.

3. Consultation

APRA has consulted extensively on its proposed information security proposals. APRA undertook a public consultation from March to May 2018, met with a number of interested parties and made a number of presentations at industry forums. APRA received a total of 39 submissions from APRA-regulated entities, industry bodies and also a number of other interested parties.

The key concerns raised in submissions focused on:

- the nature and extent of the classification of information assets required under the standard;
- application of the standard to third-party arrangements and situations where a third-party service provider engages another provider to manage information assets of an APRA-regulated entity;
- notification requirements; and
- requests for transition, notably in relation to information assets managed by third parties.

4. Regulation Impact Statement

APRA prepared a Regulation Impact Statement which has been lodged as supporting material.

5. Statement of compatibility prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

A Statement of compatibility prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* is provided at Attachment A to this Explanatory Statement.

ATTACHMENT A

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*

Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018

The legislative instrument is compatible with the human rights and freedoms recognised or declared in the international instrument listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* (HRPS Act).

Overview of the Legislative Instrument

The purpose of the instrument is to make a new *Prudential Standard CPS 234 Information Security* (CPS 234).

CPS 234 sets out requirements for authorised deposit-taking institutions, general insurers, life insurance companies, private health insurers and registrable superannuation entities to adopt practices designed to promote resilience against information security incidents by maintaining appropriate information security capabilities. CPS 234 does not prescribe any measures relating specifically to the treatment of personal information.

Human rights implications

APRA has assessed the instrument and is of the view that they it does not engage any of the applicable rights or freedoms recognised or declared in the international instruments listed in section 3 of the HRPS Act. Accordingly, in APRA's assessment, the instrument is compatible with human rights.

Conclusion

The instrument is compatible with human rights as it does not raise any human rights issues.