

In this issue:

[Overview of APRA's guidance on the management of security risk in information and information technology](#)

[Transitional period for compliance with group purchasing bodies class order extended](#)

[AFSL application for margin lending lenders and advisers](#)

[New anti-corruption legislation](#)

[CGT Rollover relief](#)

Overview of APRA's guidance on the management of security risk in information and information technology

The Australian Prudential Regulation Authority (APRA) has published a prudential practice guide (PPG) on the management of security risk in information and information technology (IT) by institutions supervised by APRA: http://www.apra.gov.au/Policy/upload/PPG_PPG234_MSRLT_012010_v7.pdf.

A draft PPG and discussion paper on this topic were released for public consultation on 8 May 2009 as *Prudential Practice Guide PPG 234 Management of IT Security Risk*. Response to the consultation package was positive and no material issues were raised.

The final PPG aims to target areas where APRA's ongoing supervisory activities continue to identify weaknesses. Topics addressed include the importance of an overarching framework, systematic IT asset life-cycle management, effective monitoring processes and robust IT security reporting and assurance mechanisms.

The PPG is designed to provide guidance to senior management, risk management and IT security specialists (management and operational). It does not seek to provide an all-encompassing framework nor to replace or endorse existing industry standards and guidelines.

Please refer below for a summary of the key points:

- In APRA's view, IT risk exposures that could have a material impact on a regulated institution would typically be controlled/mitigated to a level that ensures the institution's ability to meet regulatory and prudential requirements or operate as a going concern is not compromised by an incident.
- APRA envisages that a regulated institution would adopt a set of high-level IT security principles in order to establish a sound foundation for the IT security risk management framework. Common IT security principles are provided on page 9 of the guide.
- APRA recommends that a regulated institution should establish policies with supporting standards, guidelines and procedures in a particular area, details of which are provided on page 10 of the guide, with higher level policies normally linked to desired business outcomes.
- APRA believes that a regulated institution would normally implement processes that ensure compliance with regulatory and prudential requirements and the internal IT security risk management framework. APRA envisages that this would include ongoing checks by the compliance function (or equivalent), supported by reporting mechanisms (eg metrics, exceptions) and management reviews.

- APRA believes that a regulated institution would normally implement an exemption policy for handling instances of non-compliance with the IT security risk management framework including: management of the exemption register; authority for granting exemptions; expiry of exemptions; and the review of exemptions granted. Where exemptions are granted, APRA envisages that an institution would review and assess the adequacy of compensating controls initially and on an ongoing basis. Compensating controls would normally reduce the residual risk in line with the institution's risk appetite.
- APRA envisages that control gaps identified in the IT security risk management framework would be addressed in a systematic way. This may involve the formulation of an IT security program that specifies target IT security metrics, timeframes for resolution and associated action plans for closing the gaps. Typically, action plans would be prioritised and tracked.
- APRA believes a regulated institution could benefit from developing an initial, and ongoing, training and IT security awareness program. This would typically incorporate any changes in IT security vulnerabilities or the institution's IT security risk management framework. Sound practice would involve the tracking of training undertaken and the testing of staff understanding as to the relevant IT security policies (both on commencement and periodically). The guide provides a list of training common areas on page 11.
- In APRA's view, wholesale access to sensitive data/information would be highly restricted to reduce the risk exposure to significant data leakage events. Industry experience of actual instances in this area includes the leakage of debit/credit card details and the sale/trade or exploitation of customer identity information.
- In APRA's view, cryptographic techniques would normally be used to control access to sensitive data/information, both in storage and in transit.
- APRA envisages that a regulated institution would ensure that IT security is considered at all stages of an IT asset's life-cycle (i.e. from planning to disposal).
- APRA believes a regulated institution would normally have monitoring processes in place to identify events and unusual patterns of behaviour that could impact on the security of IT assets. Common monitoring processes are included on page 16 of the guide.
- APRA envisages that a regulated institution would develop appropriate processes to manage all stages of an incident that could impact on services including detection, identification, containment, investigation, evidence gathering, resolution, return to business-as-usual and reducing the risk of similar future events. Common incident types are included on page 17 of the guide.
- A regulated institution would normally have clear accountability and communication strategies to limit the impact of IT security incidents.
- Incidents would typically be subject to root cause analysis, where the underlying cause(s) of the incident is identified and analysed and controls adjusted to reduce the likelihood and impact of a future occurrence.
- APRA envisages that a regulated institution would ensure audit trails exist for IT assets that: satisfy the institution's business requirements (including regulatory and legal); facilitate independent audit; assist in dispute resolution (including non-repudiation); and assist in the provision of forensic evidence if required.
- A regulated institution would typically develop a formalised IT security reporting framework that provides operational information and oversight across the various dimensions of the IT security risk management framework.
- Reporting may include: risk profile(s); exposure analysis; progress against strategy; incident analysis; system capacity and performance analysis; recovery status; infrastructure and software analysis; project assessment and analysis; audit findings and ageing reports; and fraud analysis.
- APRA envisages that the use of metrics would be targeted towards the areas of greatest criticality and sensitivity as determined through the risk assessment process. Effective metrics are specific, measurable, business-impact oriented, controllable and reportable. In addition, a comprehensive set of metrics would include both backward – and forward-looking measures (i.e. key performance indicators (KPIs) and key risk indicators (KRIs)).

APRA expects that a regulated institution would seek regular assurance that IT assets are appropriately secured and that its IT security risk management framework is effective.

Source

Australian Prudential Regulation Authority, APRA releases guidance on the management of security risk in information and information technology, 1 February 2010.

http://www.apra.gov.au/media-releases/10_02.cfm

Transitional period for compliance with group purchasing bodies class order extended

Group purchasing bodies arrange or hold cover under risk management products for others but do not issue risk management products or provide any financial product advice other than as a result of providing certain general information.

Group purchasing bodies include sporting and other not-for-profit organisations which arrange insurance for third parties (eg players or volunteers).

Australian Securities & Investments Commission (ASIC) released a class order CO 08/1 in September 2008 to provide conditional relief only to a limited class of group purchasing bodies who organise insurance on a non-commercial basis from holding a financial services license and complying with section 601ED of the Act in relation to the operation of a risk management scheme.

ASIC has issued Class Order CO 10/45 (Variation of CO 08/1 Group purchasing bodies), extending the transitional period for compliance with the breach reporting requirement in Class Order 08/1 (Group purchasing bodies (CO 08/1)) until 28 February 2010.

The transitional period for compliance with this requirement was due to expire on 31 January 2010. CO 08/1 gives conditional relief from the Australian Financial Services licensing regime and Chapter 5C of the Corporations Act for some group purchasing bodies who arrange or hold risk management products for the benefit of third parties. Regulatory Guide 195 Group purchasing bodies for insurance and other risk management products (RG 195) explains ASIC's policy underlying the conditional relief granted in CO 08/1.

Source

Australian Securities & Investments Commission, ASIC further extends transitional period for compliance with group purchasing bodies class order, 28 January 2010.

<http://www.asic.gov.au/ASIC/asic.nsf/byHeadline/10-11AD%20ASIC%20further%20extends%20transitional%20period%20for%20compliance%20with%20group%20purchasing%20bodies%20class%20order?opendocument>

AFSL application for margin lending lenders and advisers

Issuers and advisers of margin lending facilities have from 1 February to 30 June 2010 to apply for an Australian Financial Services licence (AFSL), or a variation to an existing licence.

Existing margin lenders and advisers on margin loans must apply to ASIC for an AFSL authorisation within this timeframe if they intend to continue to provide a margin lending financial service after the application period closes on 30 June 2010. Industry participants who fail to do so will have to cease providing such services.

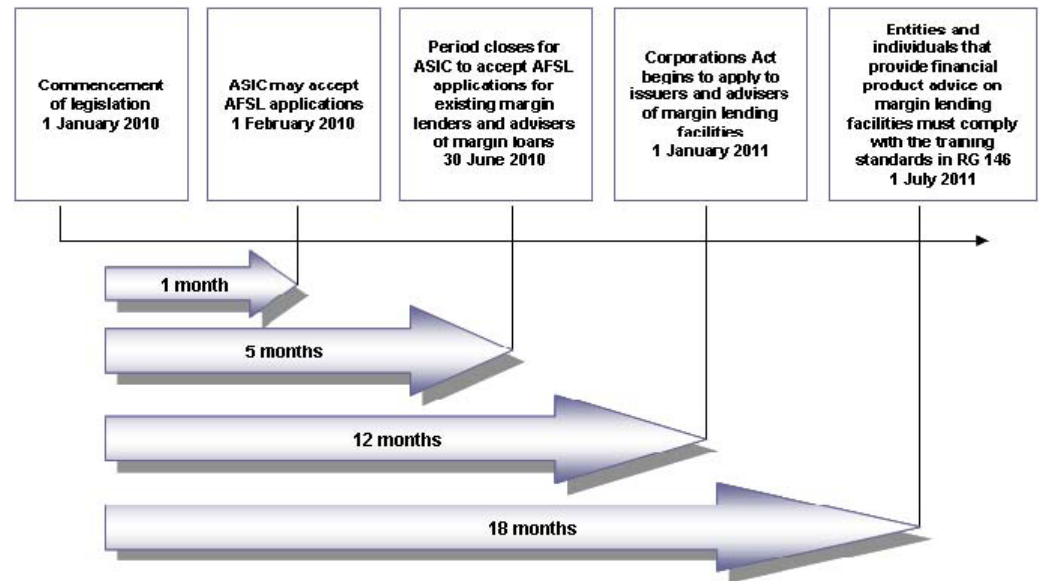
This follows the passage of the Corporations Legislation Amendment (Financial Modernisation) Act late last year which provides for the regulation of margin lending facilities. Amongst other things, the Act requires:

- issuers and advisers of margin lending facilities to be licensed by ASIC under an AFSL;
- advisers to only provide advice that is appropriate to the client's individual circumstances;
- margin lenders to meet new responsible lending requirements;
- consumers to have access to external dispute resolution services; and
- clarity around responsibility for notifying clients in the case of a margin call.

The new conduct and disclosure requirements for issuers and advisers of margin lending facilities, and the new responsible lending and margin call notification requirements, will take effect from 1 January 2011.

Please refer below for a detailed timeline of the changes to margin lending regulation.

Transition timeline for margin lending reforms



Source

Australian Securities & Investments Commission, Margin lending licensing commences, 1 February 2010.

<http://www.asic.gov.au/ASIC/asic.nsf/byHeadline/10-12AD%20Margin%20lending%20licensing%20commences?opendocument>

New anti-corruption legislation

In September 2009, the Federal Attorney-General, Robert McClelland, introduced the Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009 (No. 2). Among a raft of reforms aimed at preventing, investigating and prosecuting organised criminal activity, the Bill amends the Criminal Code Act 1995 (Cth) to strengthen the penalties for the offences of bribing foreign public officials (section 70.2) and Commonwealth public officials (s141.1).

Under the Bill, individuals who are found guilty of bribing a foreign or Commonwealth public official will be liable to a maximum of 10 years' imprisonment, a fine of \$1,100,000, or both (a significant increase from the current maximum fine of \$66,000). The Explanatory Memorandum to the Bill explains that, '[t]he inclusion of a significant monetary penalty for individuals is to deter bribery of foreign public officials where the existing financial penalty may be perceived as "a cost of doing business" when international transactions worth millions of dollars occur.'

Corporations found guilty of bribing a foreign or Commonwealth public official may be subject to even more onerous pecuniary penalties. Under the Bill, the maximum penalty for a corporation will be the greatest of the following:

- ⊃ A\$11,000,000;
- ⊃ three times the value of any benefit that the corporation has directly or indirectly obtained that is reasonably attributable to the conduct constituting the offence (including the conduct of any related corporation);
- ⊃ if the court cannot determine the value of that benefit, 10 per cent of the annual turnover of the corporation during the 12 months preceding the offence.

Source

Explanatory Memorandum, Crimes Legislation Amendment (Serious and Organised Crime) Bill (No. 2) 2009.



CGT Rollover relief

On 26 November 2009 the Senate referred the Tax Laws Amendment (2009 Measures No. 6) Bill 2009 for inquiry and report: http://www.aph.gov.au/senate/committee/economics_ctte/TLAB_6_09/index.htm.

The bill contains six schedules.

Schedule 2 contains amendments that will remove potential impediments to superannuation fund consolidation by allowing eligible entities to roll over capital and revenue losses and transfer previously realised losses when merging. These measures will apply from 24 December 2008 to 30 June 2010.

Submissions have been received and the reporting date is 25 February 2010.

Source

Parliament of Australia, Inquiry into the Tax Laws Amendment (2009 Measures No. 6) Bill 2009.

aonmastertrust.com.au

The information in this factsheet is general in nature. Your personal objectives, financial situation or needs were not taken into account when preparing this information. You may want to seek independent advice before making any decisions about your super. This factsheet was prepared by Aon Consulting Pty Limited (ABN 48 002 288 646, AFSL 236667) and issued by Aon Superannuation Pty Limited (ABN 83 057 982 822, AFSL 237465) as trustee for the Aon Master Trust (ABN 68 964 712 340). © 2010 This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part may be reproduced by any process nor may any other exclusive right be exercised without the permission of Aon Consulting Pty Limited.