



Discussion Paper

Management of IT security risk

8 May 2009

Disclaimer and copyright

While APRA endeavours to ensure the quality of this Publication, APRA does not accept any responsibility for the accuracy, completeness or currency of the material included in this Publication, and will not be liable for any loss or damage arising out of any use of, or reliance on, this Publication.

© Commonwealth of Australia

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. All other rights are reserved.

Requests and inquiries concerning reproduction and rights should be addressed to:

Commonwealth Copyright Administration
Copyright Law Branch
Attorney-General's Department
Robert Garran Offices
National Circuit
Barton ACT 2600
Fax: (02) 6250 5989

or submitted via the copyright request form on the website <http://www.ag.gov.au/cca>

Preamble

This discussion paper provides a brief overview of proposed guidance on the management of information technology security risk. It outlines measures that APRA regards as being representative of sound practice for the purpose of managing the security risks associated with information technology. Application of the practices and principles in the prudential practice guide should assist in safeguarding information technology assets by effectively managing risk and implementing a sound control framework.

The draft guide is available on the APRA website at www.apra.gov.au/policy.

Written submissions on these proposals should be forwarded not later than 5 June 2009 to:

Mr David Rush
General Manager
Policy Development
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001

or email: itsecureppg@apra.gov.au

Important

Submissions will be treated as public unless clearly marked as confidential and the confidential information contained in the submission is identified.

Submissions may be the subject of a request for access made under the Freedom of Information Act 1982 (FOIA). APRA will determine such requests, if any, in accordance with the provisions of the FOIA.

Overview of proposed prudential practice guide

The compromising of an APRA-regulated institution's information technology (IT) assets (including software, hardware and data) could have a significant detrimental impact on the institution's reputation and could result in a failure to meet key business objectives, including compliance requirements.

The proposed prudential practice guide (PPG) seeks to address those areas of IT security that APRA has identified, through its ongoing supervision, as the main areas of potential weakness. It provides a set of principles that are considered to represent better practice for safeguarding IT assets through sound risk management and control frameworks. The PPG aims to cover the key areas necessary to adequately secure a regulated institution's IT assets, with specific coverage of:

- the security management framework;
- acceptable usage and user awareness;
- identification, access and authorisation;
- life-cycle management controls;
- monitoring and incident management;
- security reporting and metrics; and
- security assurance.

The PPG is intended to have wide application for use by senior management, risk management and security specialists (management and operational). The broad array of identified users reflects the pervasive nature of IT security management, and the need for sound risk management practices and business understanding in order to evaluate and effectively manage an institution's security risk profile. Additionally, effective management of IT security risk will assist with compliance of other regulatory requirements (e.g. privacy and anti-money laundering).

Relation to risk management

In APRA's view, IT security risk represents the intersection of IT risk and security risk which, in turn, are subsets of operational risk.

IT risk includes the broader set of risks stemming from projects, outsourcing, software and IT infrastructure, whereas security risk relates to the potential compromise of confidentiality, integrity, availability and accountability of an institution's IT resources.

While IT risks are a subset of the broader set of operational risks, there are distinct practices and disciplines employed by financial institutions to manage these separate risk sets.

Development of the guide and the consultation process

APRA has consulted with a number of industry and professional associations in preparing this draft PPG and now seeks submissions from industry and other interested parties.

Once submissions from this current consultation have been considered, APRA proposes to issue a final version of the PPG later in 2009.



Telephone
1300 13 10 60

Email
contactapra@apra.gov.au

Website
www.apra.gov.au

Mail
GPO Box 9836
in all capital cities
(except Hobart and Darwin)