Prudential Practice Guide

GPG 230 – Operational Risk

February 2006

www.apra.gov.au

Australian Prudential Regulation Authority

Disclaimer and copyright

This prudential practice guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or prudential standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this guide.

APRA disclaims any liability for any loss or damage arising out of any use of this prudential practice guide.

This prudential practice guide is copyright. You may use and reproduce this material in an unaltered form only for your personal non-commercial use or non-commercial use within your organisation. Apart from any use permitted under the *Copyright Act 1968*, all other rights are reserved. Requests for other types of use should be directed to APRA.

About this guide

Prudential Standard GPS 220 Risk Management (GPS 220) sets out APRA's requirements of general insurers (insurers) in relation to risk management. This prudential practice guide aims to assist insurers in complying with those requirements in relation to operational risk and, more generally, to outline prudent practices in relation to operational risk management.

Subject to the requirements of GPS 220, insurers have the flexibility to configure their operational risk management framework in the way most suited to achieving their business objectives.

Not all the practices outlined in this prudential practice guide will be relevant for every insurer and some aspects may vary depending upon the size, complexity and risk profile of the insurer.

Operational risk

1. Operational risk is the risk of financial loss resulting from inadequate or failed internal processes, people and systems or from external events. An insurer may determine a definition of operational risk appropriate to the size, business mix and complexity of its activities and operating environment. APRA envisages that this definition of operational risk would be clearly understood throughout the insurer in order to effectively identify and manage this risk.
2. The management of operational risk would typically include (but is not limited to) the risks associated with outsourcing, business continuity[1], inadequate human resources, internal and external fraud, project management, underwriting and claims, business processes and the introduction of new products.

Human resources

3. In relation to human resources, the risk management framework may include the following elements or such elements as the insurer deems relevant to its circumstances:
   (a) risk identification and assessment of the insurer's human resource needs; and
   (b) monitoring and supervision of staff.

Fraud

4. APRA envisages that the risk management framework would address fraud risk. Fraud risk relates to the risk associated with intentional acts, undertaken with the objective of personal benefit, to tamper with or manipulate the financial or operational aspects of the business.
5. Fraudulent activity can arise from internal sources (e.g. premium redirection) or external sources (e.g. fictitious claims) and exposes the insurer to risk of financial loss if not managed appropriately.
6. In relation to fraud, the risk management framework would typically include (but is not limited to) the following elements:
   (a) risk identification and assessment;
   (b) internal controls and mitigation strategies;
   (c) segregation of duties at both an operational level and in relation to functional reporting lines;
   (d) financial accounting controls; and
   (e) staff training and awareness.

Project management

7. An insurer could consider addressing project management risk in its risk management framework. Project management risk is the risk that projects will not achieve the desired objectives or will have a negative impact on resource levels of the insurer.
8. In relation to project management, the risk management framework would typically include (but is not limited to) the following elements:
   (a) a formal project methodology for the promulgation of project initiatives including:
      (i) setting a business case for the project;
      (ii) cost/benefit analysis;
      (iii) risk identification and assessment; and
      (iv) stakeholder sign-offs;
   (b) clearly defined and appropriate levels of delegations of authority;
   (c) ongoing monitoring of project objectives and timeframes; and
   (d) post-implementation review.

[1] Requirements in relation to business continuity management are set out in *Prudential Standard GPS 222 Business Continuity Management*.

Telephone
1300 13 10 60

Email
contactapra@apra.gov.au

Web site
www.apra.gov.au

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