AIDA Questionnaire on the Corporate Governance of Insurers

World Congress, Rio, 2018

AUSTRALIAN CHAPTER RESPONSE

Mark Radford Principal Radford Lawyers

mark@radfordlawyers.com.au

Current as at 1 February 2018

General reporter: Professor JJ Lin (AIDA Taiwan)

Corporate Governance – General and Life Insurers

Part I - General

Question 1: In your jurisdiction, what corporate governance models are available to insurance companies? In case multiple models are available, describe the main differences and the allocation of management and monitoring powers among the relevant bodies/committees and which model is generally or ideally adopted by insurance companies.

What is corporate governance as a concept in Australia?

The phrase 'corporate governance' can be usefully described as *"the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled within corporations. It encompasses the mechanisms by which companies, and those in control, are held to account."*[1]

In a similar vein, the Australian Prudential Regulation Authority (APRA), who is the authority responsible for licensing and prudential regulation of authorised insurers and Lloyd's underwriters in Australia, describes its objectives regarding good governance as being:

> "to ensure that an institution and group is managed soundly and prudently by a competent Board (or equivalent), which can make reasonable and impartial business judgements in the best interests of the institution and group and which duly considers the impact of its decisions on depositors and/or policyholders[2]."

The According to the OECD, corporate governance involves 3 key elements:[3]

---

[1] Justice Owen in the HIH Royal Commission, The Failure of HIH Insurance Volume 1: A Corporate Collapse and Its Lessons, Commonwealth of Australia, April 2003 at page xxxiv.

[2] http://www.apra.gov.au/CrossIndustry/Documents/Prudential%20Standard%20CPS%20510%20Governance.pdf

[3] G20/OECD Principles of Corporate Governance pg 9.

- a set of relationships between a company's management, board of directors ('board'), shareholders and other stakeholders;
- a structure through which the company's objectives are set; and
- the means of achieving those objectives and monitoring performance.

Australia's corporate governance model emphasises the interests of shareholders and, in the case of insurers, policyholders.

These interests are upheld by the board, who oversee the organisation's strategy, risk and budget through the audit, risk management, remuneration, actuarial and reinsurance functions within the company/insurance group and ensure compliance with accepted procedures for each.

In this system of corporate governance, directors take on a 'gatekeeper' function where they pledge their reputation to protect the interests of investors that are often unable to do so on their own.

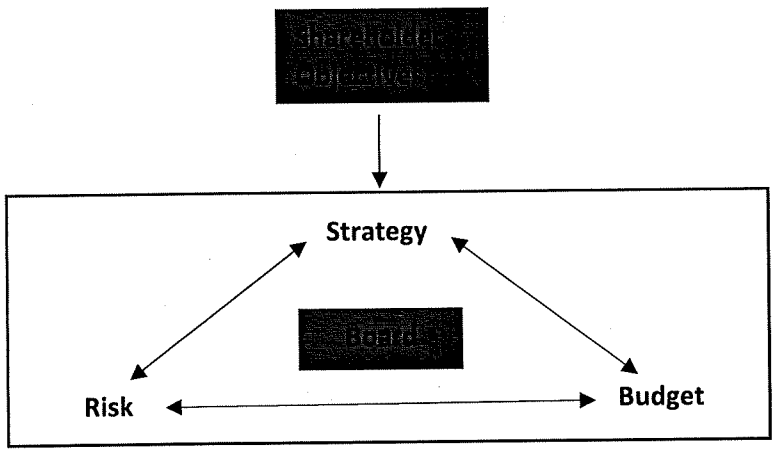
Given that the board is unable to fully engage in the day-to-day operations of an institution, management is designed to give effect to the board's wishes and assist them in meeting their obligations, the majority of which are laid out in the *Corporations Act 2001 (Cth)* (Corporations Act).

Under s12 of the *Insurance Act 1973 (Cth)* (Insurance Act) (general insurers) and s21 of the *Life Insurance Act 1995 (Cth)* (Life Insurance Act) (life insurers) (separate arrangements are in place for authorisation of Lloyd's underwriters under the Insurance Act), insurers are required to obtain authorisation from APRA in order to conduct insurance business, meaning that they will be subject to regulation by APRA.

Section 32 of the Insurance Act states that APRA can determine prudential standards that must be complied with by general insurers, the same concept applies to life insurers under s230A of the Life Insurance Act.

In Australia, corporate governance therefore entails compliance with APRA's Prudential Standards as well as Corporations Act and other general legislative requirements.

Board Function



Composition of a Board

An APRA regulated institution that is incorporated in Australia must have a minimum of 5 directors at all times, the majority of whom must be independent, unless an exception applies.[4] Board composition will be discussed in more detail in Part II, Question 1.

Risk Management Function and the Presence of a Risk Committee

Risk management involves a set of coordinated activities to direct and control an organisation regarding risk.[5]

At a high level, adequate risk management requires a board-approved risk management policy, which links the entity's risk management framework to the board's strategic objectives.

This involves defining an entity's risk appetite, risk culture and risk tolerance, all of which must be considered under APRA's prudential standard CPS 220 - Risk Management

- Risk appetite: the degree of risk an organisation is prepared to accept in pursuit of its strategic objectives and business plans, giving consideration to the interests of policyholders.
- Risk tolerance: for each material risk, the maximum level of risk that an organisation is willing to operate within based on its risk appetite, risk profile and capital strength.
- Risk culture: norms and behavior within an organisation that determine the way they identify, understand, discuss and act on risks that the organisation confronts or takes.[6]

The board is also responsible for the risk management framework, which provides the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity.[7]

This risk management framework is implemented as part of the overall risk management policy, which links the framework to shareholder objectives.

Senior management is responsible for the monitoring and management of material risks that have been identified by the board. CPS 510 requires the board to be satisfied that the senior managers have the full range of skills needed for the effective oversight and prudent management, respectively, of the entity.

It also requires directors to constructively challenge senior management proposals and decisions on all aspects of risk management arising from the institution's activities. As part of their risk management framework, CPS 220[8] requires that all insurers have:

- a risk appetite statement detailing an insurer's risk appetite and risk tolerance, as well as the process by which both are defined and compliance is monitored;
- a risk management strategy, which describes identified risks and how they are managed through policies/procedures and roles/responsibilities within the risk management function. The relationship between the board, board committees and senior management must be detailed, as well as the way in which these groups promote an appropriate risk culture;[9]
- a business plan;
- policies and procedures supporting clearly defined and documented roles, responsibilities

---

[4] CPS 510 – Corporate Governance pg 9
[5] AS/NZS ISO31000:2009, Risk Management Principles and Guidelines, pg 2
[6] APRA Information Paper: Risk culture, pg 7
[7] Commonwealth Risk Management Policy pg 13
[8] CPS 220, paragraph 23
[9] CPS 220, paragraph 30

and formal reporting structures for the management of material risks throughout the institution;

- a designated risk management function that assists the board/risk committee, is operationally independent, has necessary authority and reporting lines to the board, is resourced with appropriate staff and notifies the board of any breach or deviations from the risk management framework;
- an Internal Capital Adequacy Assessment Process (ICAAP), ensuring that enough capital is maintained over time to ensure solvency in the face of identified risks. Controls to manage capital risks, specific capital targets, procedures to monitor and act on risks as well as stress testing and scenario analysis are all required as part of this process;[10]
- a management information system (MIS) that is adequate, both under normal circumstances and in periods of stress, for measuring, assessing and reporting on all material risks across the institution; and
- a review process to ensure that the risk management framework is effective in identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks.

Although the ultimate responsibility for risk management (i.e. risk identification, assessment and treatment) lies with the board of an insurer, aspects of this function can be delegated to the risk committee, the presence of which is compulsory for an APRA regulated institution.[11]

The risk committee takes on an advisory role, which involves reviewing the insurer's risk management strategy (framework, policy and objectives), investigation of any internal risk control failures and any insurable risks.

The chairperson of the risk committee must be an independent director. Furthermore, there must be at least 3 members, all of whom are non-executive directors and the majority of which must be independent. They are responsible for:

- advising the board on the institution's overall current and future risk appetite and risk management strategy;
- oversight of an institution-wide view of the institution's current and future risk position relative to its risk appetite and capital strength;
- oversight of senior management's implementation of the risk management strategy;
- constructive challenge of senior management's proposals and decisions on all aspects of risk management arising from the institution's activities;
- reviewing the performance and setting the objectives of the institution's Chief Risk Officer (CRO), whilst also ensuring that the CRO has free access to the board and the Committee; and
- oversight of the appointment and removal of the CRO.

The board of an insurer must submit a risk management declaration to APRA that has been signed by both the chairperson of the board and the risk committee. This involves the following assertions:[12]

- the institution has systems in place for ensuring compliance with all prudential requirements;

---

[10] GPS 110

[11] CPS 510 – Corporate Governance

[12] CPS 220 – Risk Management Attachment A.

- the systems and resources that are in place for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks, and the risk management framework, are appropriate to the institution, having regard to the size, business mix and complexity of the institution;
- the risk management and internal control systems in place are operating effectively and are adequate having regard to the risks of the institution they are designed to control;
- the institution has a risk management strategy that is compliant with Prudential Standard CPS 220, and the institution has complied with each measure and control described in the risk management strategy;
- where it is a general insurer, the institution's Reinsurance Management Strategy complies with Prudential Standard GPS 230 Reinsurance Management, for selecting and monitoring reinsurance programs (discussed ahead); and
- the APRA-regulated institution is satisfied with the efficacy of the processes and systems surrounding the production of financial information at the institution.

An insurer's risk management framework will also involve reinsurance in order to spread liability to other insurers in the event of a catastrophe, allowing them to remain solvent. A general insurer must lodge a reinsurance arrangements statement with APRA on an annual basis that details schematics, reinsurers, parameters, effectiveness, monitoring and other factors detailed in GPS 230. Additionally, general insurers are required to maintain a reinsurance management strategy,[13] review it on an annual basis.

Where there are material changes to the operations of a regulated institution, the regulated institution must review and amend its reinsurance management framework and its reinsurance management strategy to take into account the changes which must then be approved by the board and submitted to APRA within 10 business days thereafter.

Life insurers are also required to annually report to APRA on their reinsurance arrangements, which includes schematics, reinsurers, parameters, effectiveness, monitoring as well as any other factors detailed in LPS 230. Additionally, they are not permitted to enter into certain categories of reinsurance arrangements unless approved by APRA.

Presence of a Compliance Function

As part of effective risk management, insurers are also required to have a designated compliance function that assists senior management with compliance risks.[14] These compliance issues typically revolve around laws, regulations and regulatory guidelines. The compliance function requires a reporting line independent from other business lines.[15]

Presence of an Audit Function and Committee

At a high level, the audit function involves an objective examination and evaluation of an organisation's financial statements/records to ensure that they are accurate. This involves providing a reasonable assurance (an audit of the company) that the financial statements present a true/fair view of the company's financial affairs and are in accordance with Australian accounting standards and legislation where appropriate.[16]

---

[13] compliant with paragraphs 19-27 of GPS 230
[14] CPS 220 paragraph 43.
[15] Ibid.
[16] CPA Australia – A Guide to Understanding Auditing and Assurance: Listed Companies, pg 7.

Auditors provide significant value to the board as they can identify weaknesses in internal controls such as complex and inconsistent reporting, which can otherwise make it difficult for a board to provide effective risk oversight. They can provide targeted advice to improve the business processes to reduce the risk of misreporting financial data where risk functions are not integrated, or where there are gaps in risk coverage. As such, both financial and risk audits can take place and can be internal or external to a company, where:[17]

- internal audit is an appraisal activity established within an entity and functions under the direction of the company's management and board. It is a management tool and forms part of the company's internal control structure. Internal audit is generally responsible for the evaluation of the adequacy of the company's internal controls. This can include evaluation of risk management controls and governance, the scope and adequacy of the internal audit work plan and the objectivity and performance of the internal audit function. Internal audit must also assess:[18]
    - the control environment – whether management, with the oversight of those charged with governance, has created a culture of honesty and ethical behaviour and that the strengths in the control environment are not undermined by any control environment weaknesses;
    - the entity risk assessment process – whether an entity has a process for identifying business risks relevant to financial reporting objectives, estimating the significance of risks, assessing the likelihood of their occurrence and deciding on actions to address those risks;
        - where an entity has such a process, and the auditor identifies material risks that management have failed to identify, evaluate whether there are any deficiencies in the process or internal controls;
        - if the entity doesn't have this process or has an ad hoc undocumented process, the auditor will discuss with management whether business risks relevant to financial reporting objectives have been identified and how they are addressed; and
    - the entity's information systems – inclusive of the related business processes relevant to financial reporting as well as methods of communication.
- Conversely, an external audit is undertaken by an auditor who is independent from the entity and has been appointed to express an opinion on the financial statements or other specified accountability matter[19]. External auditors act and report in accordance with objectives dictated by legislation such as the Corporations Act, regulations such as the APRA prudential standards or those established in a contract.

  The use of an external auditor has the obvious benefit of added objectivity and independence in the assessment of risk and financial records. Insurers are required to appoint an auditor under s 39 of the Insurance Act for general insurers and s 83(1) of the Life Insurance Act for life insurers. The appointed auditor must meet any specified eligibility criteria prior to such appointment, and perform functions, as set out in prudential standards.

Section 49J of the Insurance Act states that the principal auditor of a general insurer must give the insurer a certificate relating to the yearly statutory accounts. An auditor of a life insurer must also

[17] Ibid pg 13.
[18] ASA 315 – paragraphs 14-18.
[19] Ibid, pg 13

prepare a report that the company's annual returns are reliable and meet specified requirements under LPS 310.

The certificate must contain statements of the auditor's opinion on the matters required by the prudential standards to be dealt with in the certificate.

For general insurers, as required by GPS 310, the certificate must specify whether, in the Appointed Auditor's opinion, the yearly statutory accounts of the insurer present a true and fair view of the results of the insurer's operations for the year and financial position at year end, in accordance with:

- the provisions of the Insurance Act and prudential standards, the *Financial Sector (Collection of Data) Act 2001* (Collection of Data Act) and reporting standards;
- to the extent that they do not specify any requirements that conflict with the above mentioned Acts, the:
    - Australian Accounting Standards; and
    - other mandatory professional reporting requirements in Australia

Additionally, an appointed auditor must conduct a yearly review of the insurer's systems, processes and controls, including actuarial data integrity, compliance with risk management and reinsurance management strategies, all of which are designed to address compliance with prudential requirements and enable the reporting of correct financial information to APRA (s 49J Insurance Act).

The appointed auditor's findings must be summarised in a report that also addresses whether: [20]

- systems, procedures and controls exist that are kept up-to-date and address compliance with all prudential requirements;
- systems, procedures and controls relating to actuarial data integrity and financial reporting risks (the risks that incorrect source data will be used in completing returns to APRA in accordance with the Collection of Data Act) are adequate and effective;
- during the testing of the insurer's systems, procedures and controls, instances of non-compliance with prudential requirements have been identified. If so, details are to be provided;
- compliance with its Risk Management Strategy and Reinsurance Management Strategy has been achieved;
- the insurer has systems, procedures and controls in place to ensure that reliable statistical and financial data are provided to APRA in the quarterly returns required by reporting standards made under the Collection of Data Act; and
- there are matters that have come to the Appointed Auditor's attention that will, or are likely to, adversely affect the interests of policyholders of the insurer.

For life insurers, LPS 310[21] provides the Auditor must prepare a report that provides reasonable assurance on the life company's annual returns to APRA, as specified in Attachment A to the standard. In particular, the report must specify whether, in the Auditor's opinion, the annual returns are reliable and in accordance with the relevant prudential requirements including those in relation to accounting for statutory funds have been met. The Auditor must prepare a report that provides limited assurance that the life company has systems, procedures and internal controls that are designed to ensure that the life company:

---

[20] GPS 310 pg 8.

[21] LPS 310, paragraphs 19-22 and Attachment A

- has complied with all applicable prudential requirements; and

- has provided reliable data to APRA in the reporting forms prepared under the Collection of Data Act (including those provided quarterly).

The report must also provide limited assurance that these internal controls have operated effectively throughout the financial year of the life company and that the life company's systems, procedures and internal controls relating to actuarial data integrity and financial reporting risks (the risks that incorrect source data will be used in completing the reporting forms under the Colleciton of Data Act) are adequate and effective.

The audit function of both general and life insurers is also required to review the risk management framework on at least an annual basis, the results of which are to be reported to the insurer's audit committee (discussed ahead) or other specified senior officers.[22] In assessing risks, the following procedures must be used:[23]

- enquiries for information, which can be directed towards:
    - those charged with governance, which may help the auditor understand the environment in which the financial report is prepared;
    - employees involved in initiating, processing or recording complex or unusual transactions, which may help the auditor to evaluate the appropriateness of the selection and application of certain accounting policies;
    - in-house legal counsel on matters such as litigation, legal/regulatory compliance and fraud;
    - marketing/sales personnel about contractual arrangements with customers, sales trends and marketing strategies;
    - risk management function, who can provide information about operational/regulatory risks that may affect financial reporting;
    - information systems personnel on matters such as system changes, system/control failures or other information system related risks;
- analytical procedures;[24]
    - analytical procedures performed as risk assessment procedures may identify aspects of the entity of which the auditor was unaware and may assist in assessing the risks of material misstatement in order to provide a basis for designing and implementing responses to the assessed risks. The use of such procedures may help identify unusual transactions/events as well as other factors that may hold audit implications;;
- observation and inspection;[25]
    - this involves looking at an entity's operations (i.e. how business is conducted), whilst also going through their documents, records and internal control manuals; and
    - any reports prepared by the board/management such as minutes of board meetings,

[22] CPS 220 – paragraph 44
[23] ASA 315 – A7.

[24] Ibid – A14-15.
[25] Ibid – A18.

quarterly management reports and interim financial reports.

Any reports prepared by the auditor must have an auditor independence declaration attached in accordance with s307C of the Corporations Act.

Audit Committee

An insurance entity is required by APRA Standard CPS 510[26] to have an audit committee, which must contain at least 3 members. All of its members must be non-executive directors of the insurer, with an independent majority and the chairman also being an independent director. The committee must have a written charter that outlines its roles, responsibilities and terms of operation, including oversight of::

- all APRA statutory reporting requirements;
- other financial reporting requirements;
- professional accounting requirements;
- internal and external audit;
- the appointment and removal of the head of internal audit;
- the appointment and removal of the external auditor;
- the adequacy and independence of the both the internal and external audit plans ensuring that they cover all material risks and financial reporting requirements of the institution; and
- the independence and performance of the external auditor.

Presence of a Remuneration Committee

Conceptually a remuneration policy forms part of an insurance entity's risk management framework. The boards of all insurers are required to maintain and approve a documented remuneration policy outlining remuneration objectives and structure, including but not limited to performance based components of remuneration to align remuneration with prudent risk-taking.[27] This might include disclosure (for example in the case of listed companies through a remuneration report at a company's annual general meeting)[28] of:[29]

- primary benefits such as:
    - cash salary, fees and any commissions;
    - profit sharing and other bonuses (separately identifying those that are part of a long term incentive plan); and
    - non-monetary benefits;
- post-employment benefits, including retirement benefits broken into the following categories:
    - pension and superannuation benefits;

[26] CPS 510, paragraphs 73 to 89.
[27] CPS 510 - pg 13
[28] https://www.legislation.gov.au/Details/C2017C00328 Corporations Act – s300A
[29] AASB 1046 – 5.2.

- prescribed benefits (being those which must be approved by members under the Corporations Act s200B*); and*
- any other post-employment benefit;

- equity compensation, including:
  - the value of shares and units;
  - the value of options and rights;
  - any alteration to terms of vested options to rights during the reporting period which result in any increase in value; and
  - the value of other equity compensation; and
- other benefits:
  - termination benefits;
  - prescribed benefits (being benefits that are required by the Corporations Act (e.g. s200C) to be approved by members and are not post-employment benefits); and
  - all other benefits, separately identifying significant items..

Under CPS 510 an insurer's remuneration policy should:

- ensure that performance-based components of remuneration are designed to align remuneration with prudent risk-taking, including:
  - the outcomes of business activities;
  - the risks related to the business activities taking account, where relevant, of the cost of the associated capital; and
  - the time necessary for the outcomes of those business activities to be reliably measured;
- provide for the board, senior officer outside Australia or compliance committee to adjust performance-based components of remuneration downwards if necessary to protect financial stability of the institution or respond to significant unforeseen consequences; and
- set out who is covered by the policy, including persons whose primary role is risk management, compliance, internal audit, financial control or actuarial control and persons for whom a significant portion of remuneration is performance-based whose activities may affect the financial soundness of the institution and all responsible persons aside from:
  - non-executive directors;
  - appointed auditors or responsible auditors;
  - for general insurers, external appointed actuaries and the reviewing actuary;
  - for Category C insurers (discussed ahead), the senior officer outside Australia, and non-executive directors of the Category C insurer's agent in Australia where the agent in Australia is a corporate agent;
  - for life companies, external appointed actuaries; and
  - in the case of an eligible foreign life insurance company (discussed ahead), members of the compliance committee.

In addition to a remuneration policy, the presence of a remuneration committee is compulsory under CPS 510 – Corporate Governance and is responsible for:

- conducting regular reviews of, and making recommendations to the board on, the remuneration policy. This must include an assessment of the remuneration policy's effectiveness and compliance with the requirements of CPS 510;
- making annual recommendations to the board on the remuneration of the CEO, direct reports of the CEO, other persons whose activities may, in the board remuneration committee's opinion, affect the financial soundness of the institution and any other person specified by APRA; and
- making annual recommendations to the board on the remuneration of the categories of other persons covered by the remuneration policy.

Insurers who are listed on the Australian stock Exchange (ASX) should also have a remuneration committee in accordance with any ASX guidelines. The role of the remuneration committee is usually to review and make recommendations to the board in relation to:[30]

- the entity's remuneration framework for directors;
- the remuneration packages to be awarded to senior executives;
- equity-based remuneration plans for senior executives and other employees;
- superannuation arrangements for directors, senior executives and other employees; and
- whether there is any gender or other inappropriate bias in remuneration for directors, senior executives or other employees.

Actuarial Function

Section 39 of the *Insurance Act* for general insurers and s 93(1) of the *Life Insurance Act* for life insurers requires the insurers to have an actuary appointed. The actuarial function is essential for an insurer as they estimate the probability and likely cost of claims losses, including in cases where there is an occurrence of a disaster or an event such as death, sickness, injury, disability, or loss of property. This is done through the use of valuations in order to measure risk and uncertainty, which allows actuaries to provide impartial advice regarding operations, financial condition and insurance liabilities of an insurer. This advice is encapsulated through the preparation and provision of compulsory reports in accordance with prudential standards which the actuary must comply with in accordance with s49K of the *Insurance Act* and s97 of the *Life Insurance Act*, as applicable.

Under prudential standard GPS 320, the actuary of a general insurer is required to provide both a Financial Condition Report (FCR) and an Insurance Liability Valuation Report (ILVR) on an annual basis. For life insurers, only a Financial Condition Report is necessary under LPS 320 as at the end of each financial year.

Additionally, the actuary must lodge specified reports with or provide information to APRA in accordance with s49L of the *Insurance Act* or s98B of the *Life Insurance Act*, as applicable.

The annual FCR focuses on the solvency condition of an insurance company and considers both the current financial status, as reflected in the balance sheet, and a risk management assessment

[30] ASX Corporate Governance Principles and Recommendations – pg 32

involving the ability of the company to survive future risk scenarios such as natural disasters or poor economic conditions. For a general insurer, it must include:[31]

- a business overview including the background, structure and operations of the insurer;
- a summary of the ILVR's key results;
- an assessment of the adequacy of past estimates for insurance liabilities;
- an assessment of pricing, including adequacy of premiums;
- an assessment of the insurer's recent experience and profitability, including the current year and prior year performance of its insurance portfolios and analysis of any changes in business volumes, exposures, mix of business and pricing during the year ending on the valuation date;
- an assessment of asset and liability management, including the insurer's investment strategy;
- an assessment of current and future capital adequacy, and a review of the insurer's Internal Capital Adequacy Assessment Process (ICAAP), including any assumptions made and methodologies used in calculating the insurer's prescribed capital amount and capital base;
- an assessment of the adequacy of the calculation of the Insurer's Insurance Concentration Risk Charge (ICRC), including an assessment of the impact of multiple events in a year for an insurer with exposures to other accumulations as defined in GPS 116;
    - at a high-level the ICRC is the minimum amount of capital to be held against insurance concentration risks and relates to the risk of an adverse movement of the insurer's capital base due to a single large loss or series of losses;[32]
- an assessment of the suitability and adequacy of reinsurance arrangements, including the documentation of reinsurance arrangements and the existence and impact of any limited risk transfer arrangements, and whether the reinsurance arrangements are sufficient to cover the Probable Maximum Loss defined in GPS 116; and
- an assessment of the suitability and adequacy of the risk management framework.

Additionally, a general insurer must annually prepare an Insurance Liability Valuation Report (ILVR) and ensure that it is peer reviewed by another actuary. The ILVR should include:[33]

- the value of insurance liabilities;
- assumptions (estimates of uncertain variables) used in the valuation process, including the extent to which the assumptions used are based on the experience of the insurer;
- availability and appropriateness of the data;
- significant aspects of recent experience;
- the methodologies used to model the central estimates of outstanding claims liabilities and premiums liabilities;
- an assessment of the uncertainty in the gross and net central estimates;
- the sensitivity analyses undertaken;
    - a sensitivity analysis describes how the uncertain outcome from a mathematical model

[31] GPS 320 – Attachment B
[32] GPS 116
[33] GPS 320 – Attachment A, paragraph 55

can be attributed to different sources of uncertainty in its inputs;

- a description of probability distributions and parameters, or approaches adopted to estimate uncertainty if these are not specifically determined;
- risk margins (both stand-alone and diversified for each class of business) that relate to the inherent uncertainty in the central estimate values for outstanding claims liabilities and premiums liabilities, including any relevant statistics used to derive the risk margins including standard deviations and correlations;
- a reconciliation on an accident year basis of the change since the previous valuation of the net outstanding claims liabilities, including, where possible and relevant, separate measurement of the impact of:
    - significant differences between actual and expected claims experience;
    - significant differences caused by valuation basis and/or methodology change; and
    - additional liability associated with new claims incurred since the previous valuation; and
- any other matters required to be included in the ILVR under GPS 320.

In specified circumstances the ILVR must also be subject to a separate review by a reviewing actuary before submission to APRA.

Life insurers are also required to produce a FCR. This involves an investigation into the financial condition as at the end of the financial year of the company of each of its statutory funds, the general fund and the company as a whole. This investigation includes:[34]

- advice to the life company regarding the valuation of the life company's policy liabilities, and the calculation of the capital base and prescribed capital amount;
- an assessment of whether, over the financial year concerned, the life company has had in place systems and processes to ensure that the payment of surrender values results in payment of at least the amount calculated under Prudential Standard LPS 360 Termination Values, Minimum Surrender Values and Paid-up Values and that the requirements in respect of paid-up values have been complied with;
- an assessment of the cost of any investment performance guarantees within the meaning of Prudential Standard LPS 370 Cost of Investment Performance Guarantees and whether the life company has complied with that Prudential Standard in respect of each relevant statutory fund during the financial year concerned;
- an assessment, in relation to:
    - each statutory fund;
    - the general fund; and
    - the life company as a whole

    of the extent to which the life company has complied, during the financial year concerned, with:
    - the requirements of the capital adequacy standards; and
    - any directions or conditions of registration applicable to the life company under the Life Insurance Act;

[34] LPS 320 paragraph 12

- an assessment of the life company's Internal Capital Adequacy Assessment Process; and
- an assessment of the suitability and adequacy of the risk management framework.

Once completed, a copy of the FCR must be given to APRA within three months after the end of the period to which the report relates.[35]

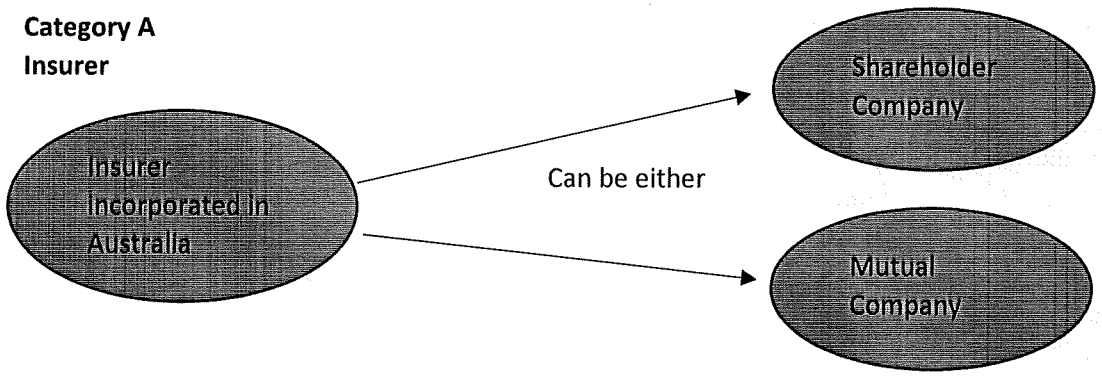
Life insurers must also prepare a valuation of policy liabilities in accordance with Prudential Standard LPS 340 – Valuation of Policy Liabilities.. This requires contracts to be classified into either life investment contracts or life insurance contracts in accordance with relevant accounting standards, unless otherwise specified. For life investment contracts, life insurers must comply with the requirements of the relevant accounting standards in the valuation of the policy liabilities. For life insurance contracts, a life insurer must value the policy liabilities in accordance with the principles and methodology set out in LPS 340.

Category C Insurers and Eligible Foreign Life Insurance Companies (EFLICs)

These types of insurers are subject to different governance models, which will be discussed ahead in Question 4.

Categories of General Insurers

In GPS 001 , APRA specifies 5 separate categories of general insurer.



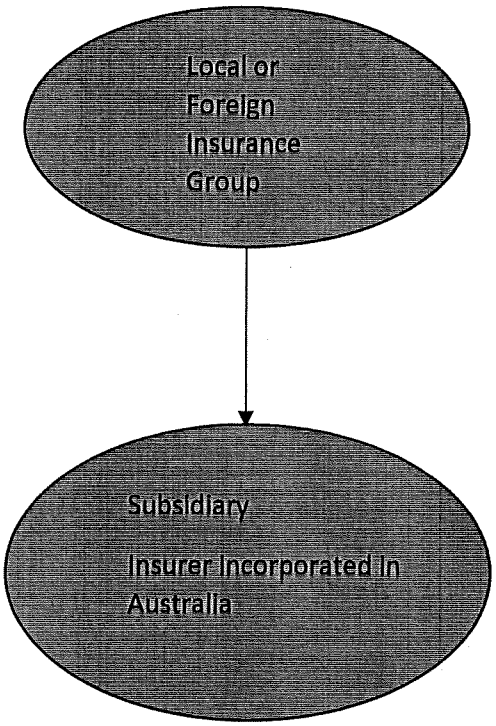
Section 124 of the Corporations Act specifies that companies can issue shares to shareholders (also known as members). A shareholder in a company must be a person, body corporate or a body politic.[36] The board of directors is liable to the shareholders, and must give effect to their interests.

Mutual companies can have two different legal forms: a cooperative or a mutual. A cooperative is an entity whose shares must be held by its employees or customers (policyholders in the insurance context). A mutual is an entity without shares or shareholders. Additionally, mutuals have no specific owner and they are managed collectively by their policyholders.

[35] Ibid, paragraph 17.

[36] http://asic.gov.au/for-business/running-a-company/company-shareholders/

Category B Insurer



Note: insurance group captives do not fall into this category.

Category B insurers are

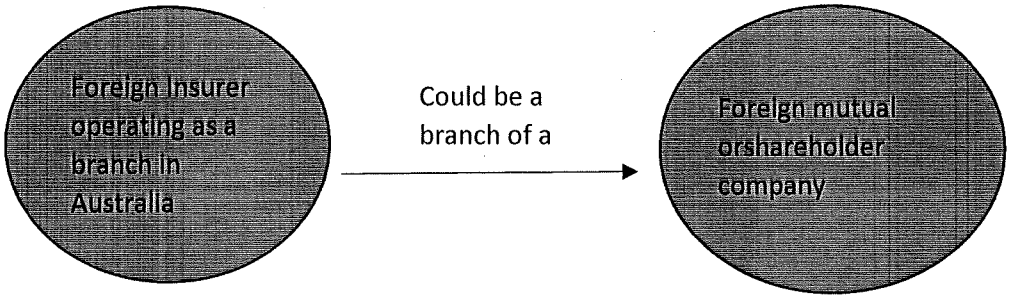
- incorporated in Australia; and
- a subsidiary of a local or a foreign insurance group.

Category B insurers are part of a local or foreign insurance group. They could be subsidiaries of mutual or shareholder companies. An insurance group captive is not a Category B insurer.

An insurance group captive is an insurer that:

- is a subsidiary of an insurer or an authorised non operating holding company (NOHC); and
- exists for the purpose of reinsuring the risks of the insurer or members of the insurance group, which may include the risks of joint venture partners of the members of the insurance group.

Category C Insurer

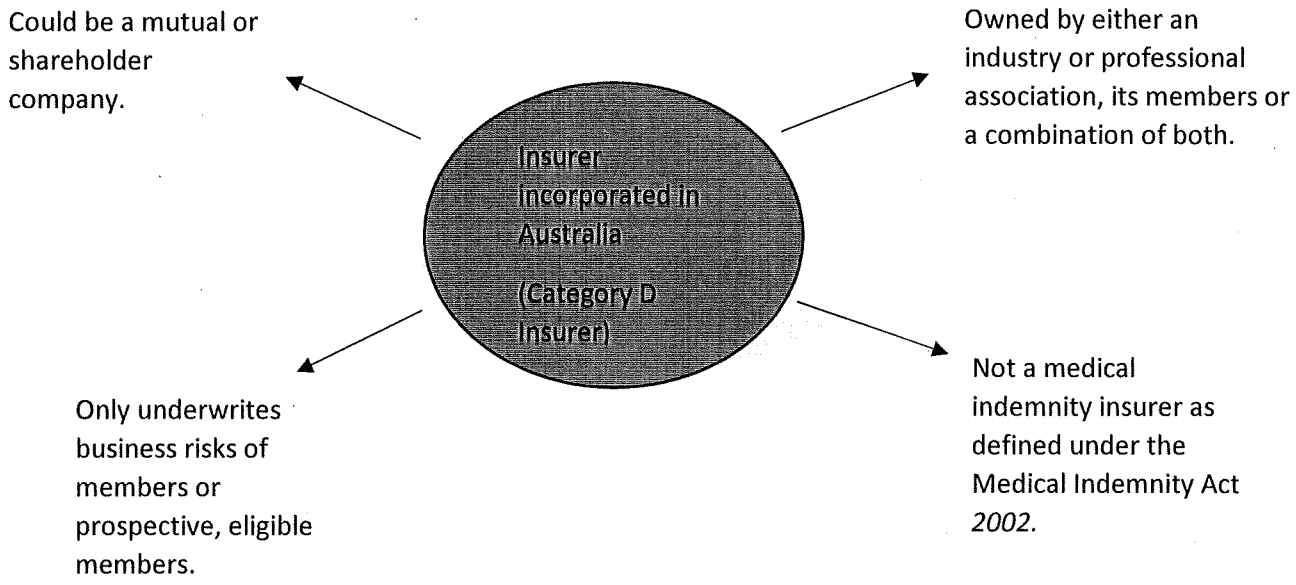


A Category C insurer is a foreign general insurer as defined in s3(1) of the Insurance Act. This means a body corporate that:

- is a foreign corporation within the meaning of paragraph 51(xx) of the Constitution; and
- is authorised to carry on insurance business in a foreign country; and
- is authorised under s12 to carry on insurance business in Australia.

A Category C insurer is a foreign insurer operating as a foreign branch in Australia and could be a branch of a foreign mutual or shareholder company.

Category D Insurer

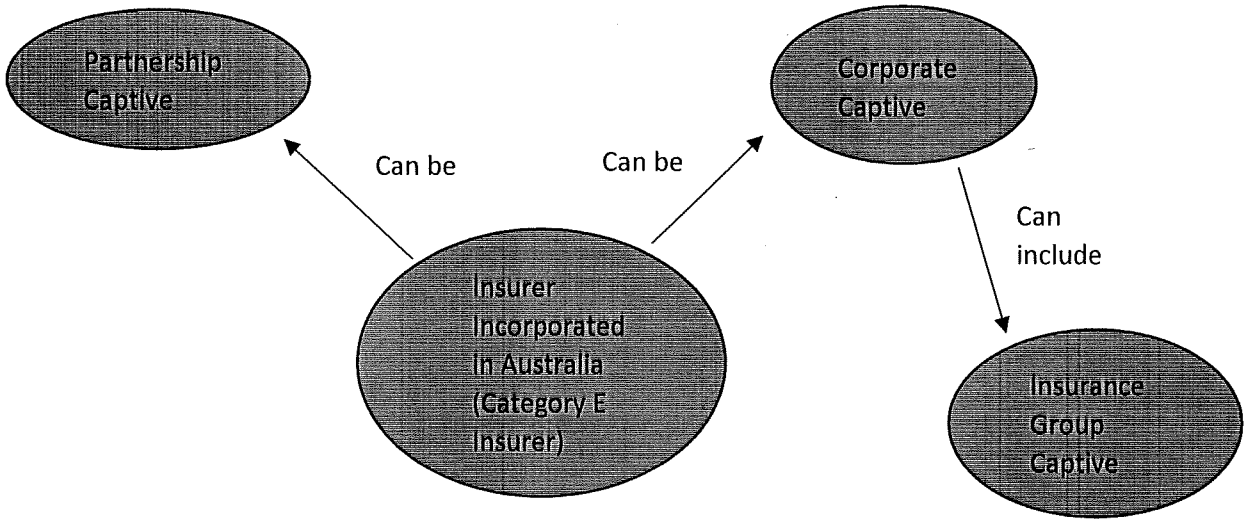


A Category D insurer is an insurer incorporated in Australia that:

- is owned by an industry or a professional association, or by the members of the industry or professional association or a combination of both; and
- only underwrites business risks of the members of the association or those who are eligible, under the articles of association or constitution of the association, to become members of the association; but
- is not a medical indemnity insurer as defined under the Medical Indemnity Act 2002.

Category D insurers are often referred to as 'association captives' and could be mutual companies or shareholder companies.

Category E
Insurer



A Category E insurer is an insurer incorporated in Australia that is a:

- corporate captive; or
- partnership captive.

Category E insurers, often referred to as 'sole parent captives', are generally shareholder companies.

A corporate captive is an insurer that:

- is owned by a single company or a group of related bodies corporate; and
- exists for the purpose of underwriting risks of the parent company or members of a group of related companies, which may include the risks of joint venture partners and contractors of members of the group of companies.

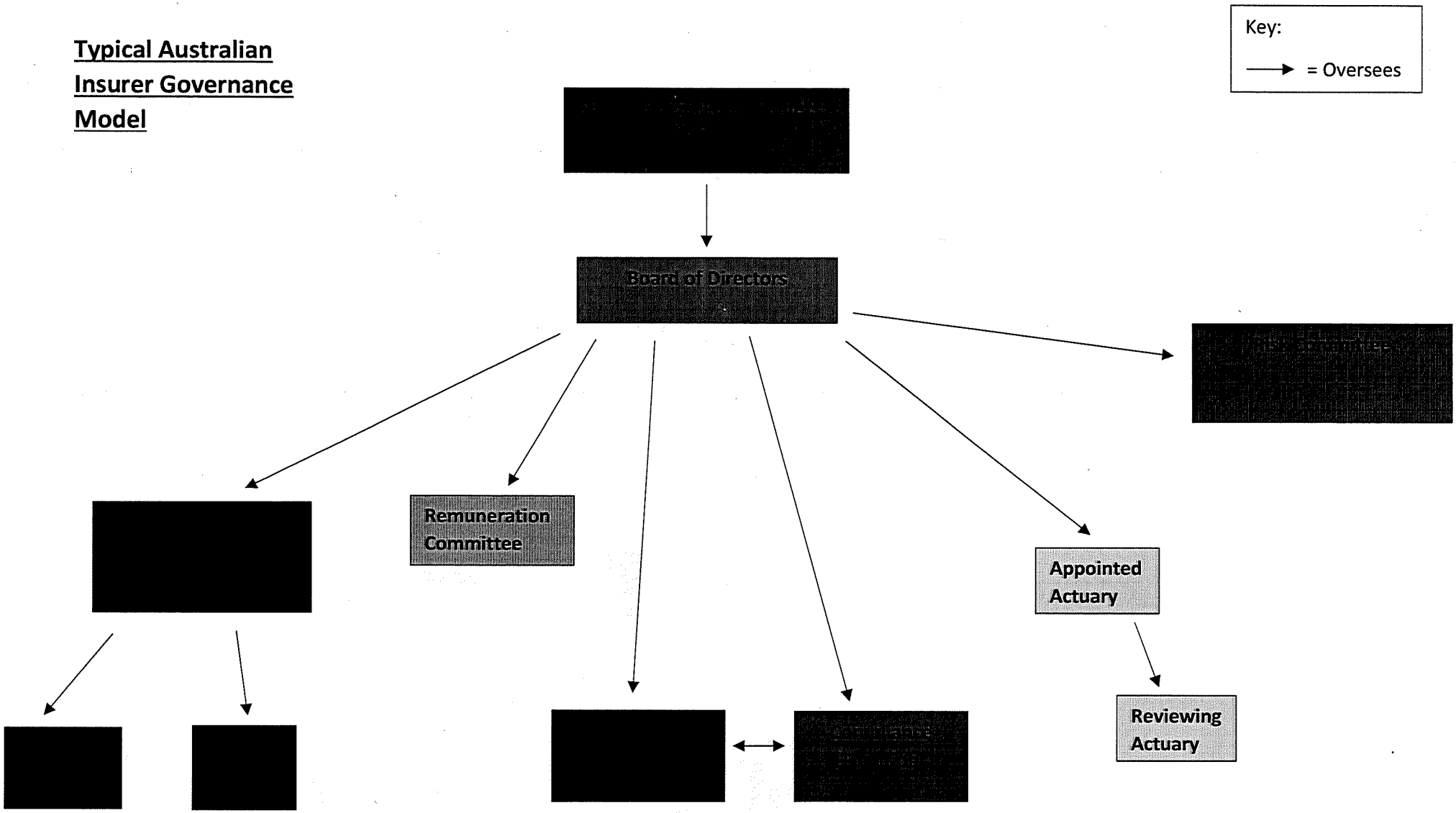
Corporate captives also include insurance group captives.

A partnership captive means an insurer that:

(a) is owned by a partnership; and

(b) exists for the purpose of underwriting the business risks of the partners and/or the partnership.

Typical Australian Insurer Governance Model



Question 2: What are the main sources of regulation addressing corporate governance of companies (and in particular of insurance companies)? *e.g.*, statutes, regulations, other rules/recommendations issued by national and supranational supervisors/regulators, self-regulation, codes of best practice, codes of ethics.

Relevant sections will be referred to throughout this paper. In Australia, corporate governance is regulated by the following:

Corporations

- *Corporations Act 2001*
- *Corporations Regulations 2001*

Insurers

- *Insurance Act 1973*
- *Insurance Regulations 2002*
- *Life Insurance Act 1995*
- *Life Insurance Regulations 1995*
- *Insurance Contracts Act 1984*
- *Insurance Contracts Regulations 1985* (will be replaced with the *Insurance Contracts Regulations 2017* on 1 April 2018)
- General Insurance Code of Practice
- Life Insurance Code of Practice

Standards, Guidelines and Codes of Practice

- ASX Corporate Governance Principles and Recommendations
- Aus/NZ Risk Management Standards
- Commonwealth Risk Management Policy
- G20/OECD Principles of Corporate Governance

APRA Prudential Standards

- APRA list of General Insurance Prudential Standards
- APRA list of Life Insurance Prudential Standards
- APRA list of Cross Industry Prudential Standards

Australian Accounting Standards Board

- AASB 1023
- AASB 1046
- AASB 10

Auditing and Assurance Standards Board

- ASA 315

Question 3: In your jurisdiction, are you aware of any insolvency or distress of an insurer directly attributable to poor corporate governance standards or practices or failure to adequately implement and apply such principles? If so, please identify the main triggers of the insolvency.

The Collapse of HIH Insurance Limited

HIH Insurance Limited (HIH Insurance) was the second largest insurer in Australia prior to their unprecedented collapse, with catastrophic effects both nationally and internationally. HIH Insurance was the holding company of the HIH group, which was comprised of several separate government–licensed insurance companies, including but not limited to HIH Casualty and General Insurance Limited, FAI General Insurance Company Limited (FAI Insurance), CIC Insurance Limited and World Marine and General Insurances Limited.

Following poor corporate governance, falling profits and APRA's proposition to increase capital adequacy requirements for insurers in 2000, HIH Insurance was declared insolvent and placed into provisional liquidation on 15 March 2001. In August 2001, Australian liquidators publicised an estimate for the total deficiency of the HIH Group of companies as being between $3.6 billion and $5.3 billion (based on a 75% confidence level for claims reserves). The gross value of claims against HIH at the time was in excess of $8 billion. The HIH Group still has outstanding liabilities and a compensation scheme administered by McGrathNicol has been in place since their collapse, with creditor reports being published at the end of each financial year.[37] To date, McGrathNicol have successfully finalised in excess of 35,000 individual creditors' claims, with an agreed creditor value of $6.7 billion across the eight licensed HIH insurers.[38]

A Royal Commission was established to prepare a report on the reasons for and the circumstances surrounding the failure of the HIH insurance group. As stated in the Royal Commission report[39] into the failure of HIH Insurance, their collapse of HIH was caused by a series of failures, including a number of which related to poor corporate governance and risk management issues. These included the following:

- the acquisition of FAI Insurance in Australia in 1999, which caused unexpected losses to HIH as a result of under-provisioning in FAI;
- losses stemming from its operations in the US and UK operations;
- the under-provisioning for claims, this is a major failure of risk management, which was not conducted in accordance with relevant accounting or actuarial standards at the time (such as of AASB 1023 and PS 300)and would be a consideration under today's Internal Capital Adequacy Assessment Process. This was also attributed to poor communication between the directors and the actuary;
- a poor governance culture, where no questioning of leadership decisions took place. It is imperative that an organisation's governance processes are transparent and inclusive for all stakeholders involved;
- HIH had a corporate governance model, but failed to assess its suitability for changing circumstances in the insurance industry. This is a blatant failure of their risk governance, as there has been minimal risk identification, analysis or evaluation;
- the audit function focused exclusively on HIH's finances rather than HIH's overall risk profile, which is a terrible governance practice as audit should also take on the additional role of

[37] http://www.hih.com.au/creditor-reports.html
[38] http://www.mcgrathnicol.com/case-studies/hih-insurance-limited/
[39] The Failure of HIH, April 2003

overall risk identification and assessment;

- the independence of the audit committee was also compromised as management was usually present at meetings between the committee and the directors. There was also a lack of independence within the external audit process compromising the integrity of financial reporting;
- operating below the minimum solvency requirements stipulated by APRA and the Insurance Act, which at the time meant that the value of the insurer's assets must exceed liabilities by the greater of $2 million, 20% of annual premium income or 15% of outstanding claims provisions;
- there was improper documentation of reinsurance arrangements on the reinsurance slips – much of the reinsurance documentation did not come to the attention of the board or the auditors, which in turn affected the accounting that took place within the company and created misstatements in financial reports;
- HIH had inadequate information systems, which deprived it of timely and reliable information that could form the basis of management decisions. This was exacerbated by the unsustainable expansion of the company's operations and a complex corporate structure:
    - being unable to access reliable data on claims can cause an insurer to underprice its products and engage in unprofitable trading;
    - company ledgers were compromised by inaccurate information;
    - poor information systems also led to budgeting failure, which in turn caused poor expenditure management and an inaccurate assessment of performance; and

  The Royal Commission identified 56 possible breaches of the Corporations Act, Insurance Act and the NSW Crimes Act, most of which were caused by poor governance practices.

Following HIH Insurance's collapse, APRA's powers were strengthened, building the foundations for their current regulatory framework and prudential standards. The Royal Commission recommended that APRA develop *"a more sceptical, questioning and, where necessary, aggressive approach to its prudential supervision of general insurers."*[40]

Minimum entry-level capital requirements for general insurers were substantially increased and reforms were introduced to enable APRA to make prudential standards for general insurance. The new prudential standards imposed stricter obligations on general insurers for fit and proper persons, governance, liability valuation, reinsurance and risk management.

APRA also introduced new risk assessment and supervisory response tools known as the Probability and Impact Rating System (PAIRS) and the Supervisory Oversight and Response System (SOARS) in October 2002.

PAIRS is APRA's risk assessment model, which focuses on the probability and the impact of a failure of an APRA-regulated entity. It introduced:

- a common set of rating components for inherent risk, management and control, and capital support;
- a structured process for combining these component ratings into a probability of failure rating; and
- an impact rating scale.

The PAIRS model was enhanced in early 2008 and now considers management and control aspects by risk type to better reflect the manner in which APRA conducts supervisory activities. It allows supervisors to view the net risk position of key risk types including board, management, risk

[40] Justice Owen in the HIH Royal Commission, The Failure of HIH Insurance, April 2003, Recommendation 26.

governance, strategy and planning, liquidity, operational, market and investment, credit, and insurance risks.

This enhanced PAIRS model applies to all entities capable of receiving a PAIRS rating by APRA, regardless of their size. These include authorised deposit-taking institutions, general insurers, life insurers, private health insurers and registrable superannuation entities and their licensees.[41]

SOARS is used to determine how supervisory concerns that have arisen from PAIRS risk assessments should be acted upon in a targeted and timely manner.

Any entity subject to a PAIRS assessment will also be assigned a SOARS stance, which will affect the level of response to a supervisory concern identified by APRA. Supervisory stances encompassed by SOARS include normal, oversight, mandated improvement and restructure. The following is notable:[42]

- entities with a normal supervisory stance are expected to remain able in meeting obligations to beneficiaries under reasonably foreseeable circumstances. Supervision activities generally include prudential consultations/reviews, analysis of data received on a monthly/quarterly/annual basis and contact with home regulators for foreign entities;

- entities with an oversight supervisory stance are expected to remain able in meeting obligations to beneficiaries over the short to medium term, but there are aspects of their risk position that may create vulnerabilities in extremely adverse circumstances, requiring more extensive examination by APRA with a close monitoring of key areas;

- mandated improvement entities are assessed by APRA as being conducted in a way that puts beneficiaries and/or the financial system at risk. These entities require more active intervention by APRA; and

- restructure entities are deemed by APRA as being an unacceptable risk to the financial system/beneficiaries due to imminent failure based on an inability to rectify serious weaknesses. Restructure entities require new capital, management, operations or ownership, possibly all four.

The introduction of enhanced capital requirements, risk management and corporate governance procedures and improved APRA oversight of insurers as a result of the HIH collapse is expected to provide a stronger and more stable insurance environment to avoid future collapses of this nature and protect policyholders in future.

The Collapse of United Medical Protection

United Medical Protection (UMP) was a mutual company and a medical defence organisation that provided discretionary indemnity protection to its membership of medical practitioners, which included roughly 60% of doctors Australia-wide. On 3 May 2002, UMP and its subsidiary Australasian Medical Insurance Limited were placed into provisional liquidation. This situation had catastrophic consequences, as it resulted in the possible withdrawal of medical services, particularly in high risk specialties, as practitioners were unprepared to risk incidents occurring for which they may not have had indemnity cover.

---

[41] APRA Probability and Impact Rating System – April 2017, pg 6.
[42] APRA Supervisory Oversight and Response System – April 2017, pg 5-9.

The collapse was attributed to numerous factors, including:

- changes to NSW health care legislation in 2001, causing a significant spike in claims in 2001;
- investment losses and rising reinsurance costs in the aftermath of the September 11 terrorist attacks;
- the insufficient provision for incurred but not reported claims, where medical defence organisations were unable to properly assess the amount of money that needed to be held in reserve to meet these claims;
- the collapse of HIH Insurance, who provided them with reinsurance; and
- a withdrawal of reinsurance capacity in global markets.

Although UMP eventually recovered from liquidation due to a Government bail out package, significant reform of the medical indemnity insurance industry took place in the aftermath of the collapse.

The *Medical Indemnity Act 2002* was introduced with a commencement date of 1 January 2003. This Act was designed to contribute towards the availability of medical services in Australia by providing Commonwealth assistance that supports access by medical practitioners to arrangements that indemnify them for claims arising in relation to the practice of their medical professions.[43]

Additionally, the *Medical Indemnity (Prudential Supervision and Product Standards) Act 2003* (Medical Indemnity Product Act) was introduced with a commencement date of 1 July 2003. This legislation prohibits institutions from providing medical indemnity cover unless the institution is an authorised general insurer under the Insurance Act 1973 (and in effect did away with the earlier medical indemnity mutual schemes that were discretionary in nature).

The Medical Indemnity Product Act also makes provision for minimum product standards for medical indemnity contracts – the Australian Securities and Investments Commission (ASIC) is responsible for the supervision of these contracts. Modern medical indemnity cover can now only be provided by general insurers through contracts of insurance, meaning that these policies also became subject to the strengthened prudential framework that arose after the HIH collapse. Medical indemnity insurance is no longer provided by mutual organisations in Australia given the heavier regulations imposed after the UMP collapse and the risks associated with unregulated insurance-like operations.

On a supplementary note, following the UMP collapse and introduction of the enhanced arrangements for medical indemnity insurance, a further enquiry was undertaken into the activities of both discretionary mutual funds (which due to their discretionary nature are not viewed as underwriting contracts of insurance at common law) and unauthorised foreign insurers in Australia and with effect from 1 July 2008 there are only limited circumstances in which insurance risks can be placed with unauthorised foreign insurers that are not authorised under the Insurance Act 1973 to carry on insurance business in Australia. Discretionary mutual funds can still operate in Australia but may need an AFSL in order to do so and as noted above cannot underwrite medical indemnity insurance risks.

[43] *Medical Indemnity Act 2002* s 3

Question 4: In your jurisdiction, is corporate governance regulation applied according to the nature, scale and complexity of an insurer's business? If yes, please describe any significant differences and rationale for the differences.

APRA applies some of their prudential standards to general insurers and life companies collectively. However, some only apply to general insurers or life insurers specifically. As previously stated, the requirements imposed upon a general insurance actuary[44] will require the production of both a financial condition report as well as an insurance liability valuation report. However, the APRA requirements for a life insurance actuary[45] do not require the production of an insurance liability valuation report, as they are more focused on individual policy liabilities, which can be included in the financial condition report. The requirements of general insurers and life insurers will differ based on the nature, scale and complexity of their business, and so APRA's prudential standards have been designed to accommodate this.

The scale of an institution may also determine whether it includes the presence of non-compulsory committees such as the nomination committee, however, all authorised life and general insurers are required to have a remuneration, risk and audit committee regardless of their size.[46] In practice most insurers also have a separate Compliance Committee as well.

Prudential regulation is also applied differently depending on the organisational structure of the insurer, such as Australian branches of foreign insurers incorporated overseas (i.e. Category C Insurers), level 2 insurance groups and eligible foreign life insurance companies.

For level 2 insurance groups, APRA's prudential standards generally apply to the parent entities of level 2 insurance groups, the structure of which is discussed in Part II, question 7. This makes compliance with the prudential standards easier for complicated insurance group structures such as that of Insurance Australia Group, where it would otherwise be cumbersome to impose the regulatory compliance obligations at the individual entity level within the group. Additionally, making the parent entity responsible for the conduct of the group forces a robust risk management and governance framework, with information systems and communication coordinated across all levels and functions. The head (i.e. parent) of a Level 2 insurance group must therefore maintain a group board remuneration committee, a group board audit committee and a group board risk committee, whilst also ensuring that management is capable of effectively managing the group in line with the board's directions.[47]

On the other hand, legislation such as the Corporations Act, Insurance Act and the Life Insurance Act will apply to all entities within the group independently, not just the parent entity.

For Category C insurers and eligible foreign life insurance companies, APRA's prudential standards only apply to the Australian branch of an entity's operations and are not binding on foreign boards. APRA is unable to regulate the conduct of foreign insurers that are incorporated overseas, and it would be extremely difficult to do so, although there are a number of Memorandums of understanding in place with overseas regulators to assist in sharing of information regarding regulated entities.

Ultimately the responsibility of a Category C insurer lies with its board. However, the entity must elect a senior officer outside of Australia that has been delegated authority from the board. The senior officer will be responsible for overseeing the operations of the Australian branch in

---

[44] GPS 320
[45] LPS 320
[46] CPS 510 – pg 2
[47] Ibid.

conjunction with a senior manager, who must be ordinarily resident in Australia and will meet with APRA on request.[48] Additionally, Category C insurers are not required to have a board audit, remuneration or risk committee.

For an eligible foreign life insurance company, the board is responsible for its overall activity. However, given the difficulty and risk profile that comes with entrance into a foreign market, the Australian branch must establish a compliance committee to operate in accordance with any prudential standards as per s16ZF of the Life Insurance Act. This committee is designed to ensure that the foreign life insurer complies with the requirements under the Life Insurance Act and must be delegated the requisite authority to do so. It should be noted that this committee serves an advisory role – it is still the ultimate responsibility of the foreign life insurer's board to ensure compliance with the Life Insurance Act. This committee must be headed by the Principal Executive Officer (PEO), the nomination of whom is to be included in any application for registration of the life insurers in accordance with s20(2) of the Life Insurance Act. Including the PEO, there must be five members (who fulfill the criteria under CPS 520), one of whom is a director of the foreign insurer's board and at least another two independent members (all of whom must be separate individuals). The PEO and at least one independent member must be resident in Australia in order to effectively operate the committee. Furthermore, the chairperson of this committee must be a non-executive member. Although the compliance committee fulfils the function of a remuneration committee, an EFLIC is still required to have an audit and risk committee and must also establish a compliance committee.

Question 5: Please provide specific examples of corporate governance structures and practices that are better implemented through self-regulation rather than through legal or supervisory requirements.

Self regulation enables industry to address a range of issues, from establishing industry standards, to developing and applying codes of professional ethics, to ensuring consumer confidence through industry-level regulation (such as a trade association or a professional society), as opposed to a governmental level. Self regulation can assist to set industry best practice and reduce the costs of legislative compliance for organisations.

In Australia, the General Insurance Code of Practice, the ASX Corporate Governance Principles and Recommendations and the Australian Institute of Company Directors' Corporate Governance Framework are all examples of corporate governance structures and practices that are implemented through self-regulation.

The General Insurance Code of Practice

The General Insurance Code of Practice (the Code) is a voluntary, self-regulatory code that binds all general insurers who are signatories to it. It applies to all general insurance products, excluding reinsurance, worker's compensation, marine insurance, medical indemnity insurance and motor vehicle injury insurance. Signatories are tasked with reporting their compliance with this code to the Code Governance Committee (CGC), who are the body responsible for its administration alongside the Insurance Ccouncil of Australia. The code contains standards for topics such as claims handling, internal/external dispute resolution and monitoring/enforcement.

The aim of the code is to:

[48] Ibid pg 12.

- commit insurers to high standards of service;
- promote better, more informed relations between insurers and policyholders;
- maintain and promote trust and confidence in the general insurance industry;
- provide fair and effective mechanisms for the resolution of cComplaints and disputes between insurers and policyholder; and
- to promote continuous improvement of the general insurance industry through education and training.

The objectives of the code will be pursued having regard to the law, and acknowledging that a contract of insurance is a contract based on the utmost good faith.

Insurers that are signatories to the code must therefore ensure that:

- the retail insurance sales process as well as the services provided by employees and authorised representatives are conducted in an efficient, honest, fair and transparent manner;
- employees and authorised representatives receive appropriate education and training to allow for the competent provision of services;
- claims and complaints handling are conducted in an honest, fair, transparent and timely manner;
- catastrophies are responded to in an efficient, professional and practical way; and
- a subscription to the independent external dispute resolution scheme administered by the Financial Ombudsman's Service takes place (soon to become the Australian Financial Complaints Authority).

Additionally, there must be systems and processes in place to enable the CGC to monitor compliance with the code. Compliance with the code must be detailed in an annual return to the CGC, while reports on compliance with the code must be given to directors or executive management. Given that subscription to the code is voluntary, these reporting requirements are not as formal as the APRA reporting obligations However, the board of directors still needs to ensure that code compliance is being met through self-regulation, in addition to both legal and APRA's prudential requirements.

The ASX Corporate Governance Principles/Recommendations

Rule 4.10.3 of the ASX Listing rules states that listed companies need to disclose how they fulfil the ASX Corporate Governance Recommendations in their annual report. If the entity has not followed a recommendation for any part of the reporting period, its annual report must contain a corporate governance statement which separately identifies that recommendation and the period during which it was not followed and state its reasons for not following the recommendation and what (if any) alternative governance practices it adopted in lieu of the recommendation during that period. This process of self-regulation is known as the "if not, why not" approach.[49] For insurers, it is worth noting that many of these recommendations are mandatory as they overlap with APRA's prudential framework. For instance, Recommendation 4.1 requires corporations to have an audit committee, which is a requirement under CPS 510.

Australian Institute of Company Directors' Corporate Governance Framework

[49] ASX Corporate Governance Principles/Recommendations, pg 3

The Australian Institute of Company Directors' Corporate Governance Framework (the Framework) outlines skills, attributes and expertise that comprises good director practice. Given that these serve as guidelines as opposed to binding rules, the Framework is best implemented through self-regulation.

The purpose behind this is for directors to identify areas of improvement and mentor others who are seeking to improve in certain areas. The Framework is designed as a "wheel" with four quadrants depicting the four areas of focus and engagement applying to board and director practice:

- the individual quadrant, which reflects the practices every director brings as an individual to his or her director role – for example, the responsibilities he or she has in relation to leadership both as a director and as a chairman;

- the board quadrant, which reflects the practices of individual directors in relation to the whole board, their commitment to the successful functioning of the board and collegiate responsibilities;

- the organisational quadrant, which focuses on the responsibilities of directors in relation to the performance of the organisation, including those of senior executives. There is a focus on relationships and critical areas of organisational functioning that should be led by directors as individuals within the whole board. This quadrant also identifies the director level operations necessary for the functioning of an entity, including governance, risk, strategy, finance and management relations; and

- the stakeholder quadrant, which focuses on the essential interaction between directors and stakeholders. This is the outward focus directors need to consider in carrying out directorship responsibilities, looking beyond shareholders to a broader range of stakeholders.

The process of self-assessment that comes with the implementation of this framework is ideal for ensuring that the board of directors maintains the strengths and skills needed to ensure the proper functioning of an entity, as well as compliance with previously mentioned laws and APRA regulations as applicable to directors.

Question 6: In case your jurisdiction was recently requested to implement domestically certain corporate governance principles set forth by supranational regulations, describe the main obstacles and problems (if any) that resulted from such process.

Following Australia's entry into the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and the 2009 recommendations, the OECD Working Group on Bribery (working group) released its phase 4 report (the report) in December 2017. This report states that whilst Australia has undertaken a number of legislative and institutional reforms to strengthen its fight against foreign bribery, it has not properly implemented recommendation 9, which requires that Australia has a clear framework for voluntary reporting.

This includes matters such as:

- the nature and degree of co-operation expected of a company;
- whether and how a company is expected to reform its compliance system and culture;
- the credit given to the company's co-operation;
- measures to monitor the company's compliance with a plea agreement; and
- the prosecution of natural persons related to the company.

Additionally, the report states that Australia has still not properly implemented recommendation 13, which requires that further awareness should be raised toward foreign bribery as a predicate offence to money laundering, and that Australia should provide additional guidance to reporting entities regarding the detection of foreign bribery, including through case studies and typologies.

Recommendation 9

In late 2016, the Australia Federal Police and Commonwealth Director of Public Prosecutions (CDPP) released a draft Best Practice Guideline on Self-Reporting of Foreign Bribery and Related Offending by Corporations. At the time the phase 4 report was written, these guidelines had not been finalised. However, this is no longer the case as the finalised guidelines have now been released, which state that the CDPP will assess an entity's corporate governance framework in accordance with international standards. To fully comply with recommendation 9, awareness will need to be raised regarding the finalised guidelines and the success of the self-reporting framework will need to be assessed through future developments.

Recommendation 13

There is still minimal guidance for businesses in the area of anti-corruption as compliance is largely left in the hands of the private sector. The working group has stated that Australia still needs to introduce more methods of encouraging companies to adopt adequate means to prevent foreign bribery in their corporate governance structure through internal controls, compliance programs and codes of ethics. Anti-corruption is a serious factor in the establishment of an entity's corporate governance. However, the seriousness of corporate anti-corruption has not been supported by the government's failure to proactively pursue criminal charges in this area, which could serve the dual purposes of punishment and deterrence.

The main obstacle to Australia's implementation of recommendation 13 is the fact that existing anti-corruption systems do not provide adequate information about foreign bribery methodologies, and focus too heavily on illicit flows related to bribe payments and too little on the incoming flows that represent the proceeds of bribing foreign public officials. The Fraud and Anti-Corruption Centre was established in 2013 and is composed of 13 Commonwealth agencies, including AUSTRAC. This is a promising development that is continuing to improve its information exchange capabilities regarding the illicit flow of bribery proceeds. Additionally, Australia established the Fintel Alliance on 3 March 2017, which is a public-private sector partnership that aims to increase collaboration between the two sectors. The working group has stated that this should help to provide good examples of corporate governance practice, which can then be implemented in future regulatory efforts.

Whistleblower Protections

The introduction of the Treasury Laws Amendment (Whistleblowers) Bill 2017 is a development that will strengthen Australia's whistleblower regime if passed. The Bill is currently the subject of inquiry by the Economics Legislation Committee which is expected to issue its report by 16 March 2018. However, there is much work to do as the Joint Parliamentary Committee on Corporations and Financial Services recommended in September 2017 that the Government examine options for ensuring ongoing alignment between public and private sector whistleblower frameworks, including the possibility of combining the private sector protections in a single Act and harmonising Commonwealth, States, and Territories' whistleblowing legislation. This would ensure greater regulation and impose corporate governance requirements on entities – namely a whistleblower protection program that is integrated into their risk management framework and compliant with

future regulatory efforts. The Australian Government has considered this recommendation and will respond at a later date. The OECD report praises the introduction of this legislation and will continue to monitor the development of Australia's whistleblower framework in line with our need to enhance whistleblower protections in the private sector.

Question 7: Are there any significant differences between general corporate governance rules and the specific rules governing insurance companies?

The following table sets out a summary of some of the significant differences between general corporate governance requirements and those applicable to insurers.

Legislation/Rule/ Standard and Section	Obligation/Right	Difference between insurers and other corporations
Corporations Act 2001 s 201A	Proprietary companies must have at least 1 director and public companies must have at least 3.	The board of an APRA regulated institution is required to have a minimum of 5 directors (CPS 510 pg 9). Insurers are therefore subject to a higher standard in this regard.
Corporations Act 2001 s 911A	Need for a financial services licence to carry on financial services business. Some insurers are exempt from this requirement if they are APRA regulated and only conduct "wholesale" insurance business.	Corporations that do not carry on financial services business are not required to hold a financial services licence.
Corporations Act 2001 s 912A	(1) A financial services licensee must: (a) do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly; and (aa) have in place adequate arrangements for the management of conflicts of interest that may arise wholly, or partially, in relation to activities undertaken by the licensee or a representative of the licensee in the provision of financial services as part of the financial services business of the licensee or the representative; and (b) comply with the conditions on the licence; and (c) comply with the financial services laws; and (ca) take reasonable steps to ensure that its representatives comply with the financial services laws; and (d) subject to subsection (4)----have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence and to carry out supervisory arrangements; and (e) maintain the competence to provide those financial services; and (f) ensure that its representatives are adequately trained (including by complying with section 921D),	Those who do not hold a financial services licence are not subject to these requirements.

Legislation/Rule/ Standard and Section	Obligation/Right	Difference between insurers and other corporations
	and are competent, to provide those financial services; and (g) if those financial services are provided to persons as retail clients--have a dispute resolution system complying with subsection (2); and (h) subject to subsection (5)--have adequate risk management systems; and (j) comply with any other obligations that are prescribed by regulations made for the purposes of this paragraph.	
Corporations Act 2001 Pt 7.7A Division 4	Financial services licensees must ensure that no conflicted remuneration is being distributed or accepted by their employees and representatives.	This requirement only applies to financial services licensees and they must ensure that it is incorporated into their compliance function. However, general insurance products are exempted from this requirement, meaning that the conflicted remuneration ban is more applicable to life insurers.
Corporations Act 2001 Chapter 7	Requirement of financial services entities to provide a Product Disclosure Statement, Financial Services Guide and Statement of Advice (SoA mainly applies to personal advice provided in relation to life insurance) to retail clients in a format that complies with the requirements set out in Chapter 7.	Insurers and all other financial services institutions are required to ensure the preparation of various disclosure documents that comply with Chapter 7. This should be approved by an insurer's risk/compliance function.
Insurance Contracts Act 1984 s 13	Insurance contracts are based on a duty of utmost good faith and there is an implied provision in such contracts requiring that each party involved will act with the utmost good faith towards the other party.	Unlike other organisations, insurers should include controls in their risk management framework to ensure that this duty is complied with.
Insurance Contracts Act 1984 s 14A	Failure to comply with the duty of utmost good faith will be treated as a breach of financial services law and the Australian Securities and Investments Commission (ASIC) has the power to take action.	As above.
Insurance Act 1973 s 12, *Life Insurance Act 1995* s 21	A body corporate needs to apply in writing to APRA for an authorisation to carry on insurance business in Australia.	Entities that are not insurers do not require an authorisation from APRA to conduct business. In addition, this section subjects insurers to APRA's prudential standards.
Insurance Act 1973 s 25A, *Life Insurance Act 1995* s 245A	APRA can apply to the court to disqualify a director or senior manager of an insurer.	All company directors may be disqualified under the general Corporations Act requirements by ASIC or a Court in specified circumstances. For example under s206F when a corporation has been wound up.
Insurance Act 1973 s 27	APRA is able to remove a director of a general insurer, authorised NOHC or a general agent if they are a "disqualified person" or do not meet fitness and propriety tests.	General disqualification principles apply to all corporations under the Corporations Act for directors in specified circumstances. E.g.

Legislation/Rule/ Standard and Section	Obligation/Right	Difference between insurers and other corporations
		bankruptcy.
Life Insurance Act 1995, s 31, s 48	S 31(a) a life company must at all times have at least one statutory fund in respect of its life insurance business but may have more statutory funds if it chooses to do so. S 41(1) A director of a life company has a duty to the owners of policies referable to a statutory fund of the company. (2) The director's duty is a duty to take reasonable care, and use due diligence, to see that, in the investment, administration and management of the assets of the fund, the life company: (a) complies with this Part; and (b) gives priority to the interests of owners and prospective owners of policies referable to the fund.	Life insurance are required to hold statutory funds, whilst other corporations generally are not required to do so. This imposes different corporate governance obligations on life insurers in relation to the management of these funds.
Insurance Act 1973 s 28	A general insurer is required to hold assets in Australia that are greater than or equal to the total amount of its liabilities, unless otherwise authorised by APRA.	This cannot be applied as a blanket rule to corporations generally. However, given the nature of the insurance business, it is imperative that this is a statutory requirement. This is also expanded upon in GPS 110 – Capital Adequacy, where a general insurer is required to: • have an Internal Capital Adequacy Assessment Process; • maintain required levels of capital; • determine its prescribed capital amount having regard to a range of risk factors that may adversely impact a general insurer or Level 2 insurance group's ability to meet its obligations. These factors include insurance risk, insurance concentration risk, asset risk, asset concentration risk and operational risk; • comply with any supervisory adjustment to capital imposed by APRA; • make certain public disclosures about the capital adequacy position of the general insurer or Level 2 insurance group; • seek APRA's consent for certain

Legislation/Rule/ Standard and Section	Obligation/Right	Difference between insurers and other corporations
		planned capital reductions of the general insurer or Level 2 insurance group; and • inform APRA of any significant adverse changes in the general insurer or Level 2 insurance group's capital position. The *Life Insurance Act 1995* requires life insurers to have statutory funds in Australia (unless otherwise approved by APRA) to record their assets and liabilities (refer above). In addition to this similar requirements are imposed upon life insurers in LPS 110, which states that a life company must: • have an Internal Capital Adequacy Assessment Process; • maintain required levels of capital within each of its funds and for the company as a whole; • determine each fund's prescribed capital amount having regard to a range of risk factors that may adversely impact the company's ability to meet its obligations. These factors include insurance risk, asset risk, asset concentration risk and operational risk; • comply with any supervisory adjustment to capital imposed by APRA; • make certain public disclosures about the capital adequacy position of each fund and the company as a whole; • seek APRA's consent for certain planned capital reductions of the company; and • inform APRA of any significant adverse changes in the capital position of the company as a whole or any of its funds.
Insurance Act 1973 s 35, *Life Insurance Act 1995* s 83B	General Insurers are required to comply with APRA's General Insurance Prudential Standards. Life insurers are required to comply with APRA's Life Insurance Prudential Standards.	General corporate governance rules do not require compliance with APRA prudential standards.

Legislation/Rule/ Standard and Section	Obligation/Right	Difference between insurers and other corporations
Insurance Act 1973 s 39, *Life Insurance Act 1995* s 93(1)	Insurers are required to appoint an actuary that fulfils the requirements of GPS 320 and LPS 320 respectively. Small general insurers are exempt from appointing an actuary under this prudential standard.	Given the nature of the insurance industry, the appointment of an actuary is imperative. Other industries generally do not always require an actuary.
Insurance Act 1973 s 40, *Life Insurance Act 1995* s 83A	APRA may require an insurer to appoint an additional auditor through a written notice. For instance, APRA may require the appointment of an auditor for a special purpose review.	General corporate governance would not dictate that APRA is entitled to require appointment of an additional auditor, as they only regulate insurance companies, ADIs and members of the superannuation industry.
Insurance Act 1973 s 49, *Life Insurance Act 1995* s 88B, 98B	Auditors and actuaries must give information when required.	Not all organisations are regulated by APRA and would therefore not have such an obligation.
Insurance Act 1973 s 49J, *Life Insurance Act 1995* s 83	S49J: (1) For each general insurer: (a) the principal auditor of the insurer must audit the insurer's yearly statutory accounts; and (b) an auditor of the insurer must perform for the insurer the functions of an auditor set out in the prudential standards; and (c) an auditor of the insurer must prepare, and give to the insurer, the reports (if any) required by the prudential standards to be prepared by the auditor. (2) The general insurer must make the arrangements that are necessary to enable an auditor to do those things. (3) The principal auditor of a general insurer must give the insurer a certificate relating to the yearly statutory accounts. The certificate must contain statements of the auditor's opinion on the matters required by the prudential standards to be dealt with in the certificate. (4) The reports that the prudential standards require an auditor to prepare must deal with all of the matters required by the prudential standards to be dealt with in the reports.	Generally speaking, most companies (other than small proprietary companies or some companies limited by guarantee) are required to have their financial statements audited and an auditor appointed in accordance with the *Corporations Act 2001*. However, the auditors for general insurers are subject to the further requirements under GPS 310. For life insurers, LPS 310 sets out the role of the auditor in addition to the requirements under the *Corporations Act 2001*.
Insurance Act 1973 s 49K, *Life Insurance Act 1995* s 97	The actuary of an insurer must perform the functions required by the prudential standards.	Insurers have specific corporate governance requirements in relation to actuaries that are contained in GPS 320 and LPS 320. Notably, actuaries are required to produce financial condition reports and general insurance actuaries also create Insurance Liability Valuation reports.
GPS 110 – Capital Adequacy LPS 110 – Capital	The board must ensure that the insurer/Level 2 insurance group/life company maintains an adequate level and quality of capital commensurate with the	Although all corporations must meet solvency standards, insurers are required to maintain a minimum level

Legislation/Rule/ Standard and Section	Obligation/Right	Difference between insurers and other corporations
Adequacy	scale, nature and complexity of its business and risk profile, such that it is able to meet its obligations under a wide range of circumstances	of capital for regulatory purposes known as the prudential capital requirement. This is subject to supervisory adjustments by APRA.
GPS 116 - Capital Adequacy: Insurance Concentration Risk Charge	General insurers are required to hold a minimum amount of capital against insurance concentration risks – i.e. the adverse impact on a general insurer's/level 2 insurance group's capital base due to a large loss or series of losses.	Although events may happen to corporations that could have a severe impact on their capital base, insurance companies have obligations to policyholders to pay out claims which can be multiplied in the face of catastrophic events and as such it is a key responsibility of an insurer's board, to maintain adequate levels of capital and/or reinsurance support to meet the insurers obligations to policyholders at all times.
LPS 115 - Capital Adequacy: Insurance Risk Charge	Life insurers are required to hold a minimum amount of capital against insurance risks. The Insurance Risk Charge relates to the risk of adverse impacts on a life insurer's capital base due to movements in future mortality, morbidity, longevity, servicing expenses and lapses.	
GPS 230 – Reinsurance Management	GPS 230 states that a general insurer must: • have in its reinsurance management framework a documented Reinsurance Management Strategy, sound reinsurance management policies and procedures, and clearly defined managerial responsibilities and controls; • submit its Reinsurance Management Strategy to APRA when any material changes are made; • submit a Reinsurance Arrangements Statement detailing its reinsurance arrangements to APRA at least annually; and • make an annual reinsurance declaration based on the 'two-month rule' and 'six-month rule' specified in GPS 230, and submit the declaration to APRA at the same time as the Reinsurance Arrangements Statement. • The two-month rule is where within 2 months of the reinsurance arrangement's inception, one of the following must be achieved: o a regulated institution must have a placing slip which has been signed/stamped by participating reinsurers and contains finalised terms/conditions with agreed wording on the regulated institution's behalf; o no agreed wording, but has been signed/stamped and has no outstanding terms and conditions; or o no placing slip but there's a cover note issued by the participating reinsurers. The	Reinsurance is a key feature of the insurance industry and it is imperative that reinsurance documentation is included in an insurer's risk management framework. General corporate governance rules, regulations and laws do not impose reinsurance obligations as it is exclusive to the insurance industry.

Legislation/Rule/ Standard and Section	Obligation/Right	Difference between insurers and other corporations
	regulated institution must also have systems to verify that the content of the cover note is the same as the placing slips agreed between the regulated institution and the reinsurers. • The six-month rule is where within 6 months of the reinsurance arrangement's inception, one of the following must be achieved: o compliance with the first option in the two month rule; or o a full treaty contract wording that has been agreed upon by the participating parties. • If there is no compliance with either rule, a declaration must be made that sets out what alternative documentation is in place. If there's none, then the reasons for this must be set out alongside the actions that the insurer is taking to rectify this.	
LPS 230 – Reinsurance Management (soon to be replaced by a new version)	LPS 230 states that a life company: • must report on its reinsurance arrangements annually; and • must not enter into reinsurance arrangements of a certain type unless approval has been granted by APRA.	As above.
GPS 310 - Audit and Related Matters	In addition to performing their ordinary requirements, the auditor for a general insurer must check for compliance with insurer-specific documents such as a reinsurance management strategy. They must then report back to the board. Additionally, the auditor must ensure that the insurer has complied with all prudential requirements.	Non-insurance entities do not have a reinsurance management strategy or other insurer-specific documents. Furthermore, non-APRA regulated entities do not need to comply with the prudential standards.
LPS 310 - Audit and Related Matters	Life insurance auditors are required to monitor compliance with APRA's prudential standards.	Non-APRA regulated entities do not need to comply with the prudential standards.
CPS 520 – Fit and Proper	All APRA-regulated institutions are required to ensure that responsible persons meet the fit and proper criteria specified in this prudential standard (discussed in detail ahead).	Non-APRA regulated entities/responsible persons are only subject to other standards – ie. the director's duties in the *Corporations Act 2001*

Part II - Fitness and Propriety of Board Directors

Question 1: Are there any laws or regulations already adopted or any proposals in your jurisdiction, relating to the qualification and composition of board directors in an insurance company? If so, please explain.

Qualification of Board Directors

In Australia, directors are held to a high moral standard and must act with care and diligence, in good faith and cannot take improper advantage of their position. .[50] As such, the Corporations Act sets out primary obligations of directors and imposes some restrictions on those who may be ineligible to be appointed as a director.

In terms of these general directors duties, section 180(1) of the Corporations Act imposes a duty upon a director to exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise if they:

- were a director or officer of a corporation in the corporation's circumstances; and
- occupied the office held by, and had the same responsibilities within the corporation as, the director or officer.

Additionally, s181(1) requires a director to exercise their powers and discharge their duties:

- in good faith in the best interests of the corporation; and
- for a proper purpose.

The duty of good faith requires the director/officer to act in the best interests of the shareholders as opposed to their own interests.

Section 184 also sets out criminal offences for directors who are reckless or intentionally dishonest in failing to act in good faith in the interests of the company, or use information to their advantage dishonestly

Section 182 also provides a director must not improperly use their position to:

- gain an advantage for themselves or someone else; or
- cause detriment to the corporation.

Section 183 imposes an additional duty to not misuse information obtained whilst acting as a director.

The appointment of a director should therefore involve considerations regarding their ability to comply with these general obligations.

The Corporations Act also includes some restrictions on who can be appointed as a director.

---

[50] *Corporations Act 2001*s180-182

Section 201B provides only a person who is at least 18 may be a director and any person who is disqualified from managing a director may only be appointed if permission is granted by ASIC or a Court. Section 206B includes some automatic disqualification criteria such as:

- those convicted of an offence which concerns the making of decisions that affect the whole or substantial part of the business of the corporation or its financial standing;
- those convicted of offences punishable by imprisonment of greater than 12 months, including in a foreign country; and
- persons who are undischarged bankrupt or who have entered into a personal insolvency agreement.

Specific to insurers, sections of the Insurance Act and the Life Insurance Act are relevant when appointing directors and broaden the range of persons who cannot be appointed as a director of an insurer.

Section 24 of the Insurance Act states that it is an offence to appoint a disqualified person as the director of a corporation. A disqualified person is defined under s25 of the Insurance Act as someone that at any time:

- has been convicted of an offence against or arising out of the Insurance Act, the *Financial Sector (Collection of Data) Act 2001*, the *Corporations Act 2001* and any Corporations Law that was previously in force, or any law of a foreign country that corresponds to that Act or to that Corporations Law;
- has been convicted of an offence against or arising out of a law in force in Australia, or the law of a foreign country, if the offence concerns dishonest conduct or conduct relating to a financial sector company;
- where a person is an individual, has been or becomes bankrupt, taken the benefit of a law for the relief of bankrupt or insolvent debtors, or compounded with creditors; and
- where a person is a corporate agent, the corporate agent knows, or has reasonable grounds to suspect, that a person who is, or is acting as, a director or senior manager of the corporate agent is a disqualified person; or a receiver, or a receiver and manager, has been appointed in respect of property owned by the corporate agent; or an administrator has been appointed in respect of the corporate agent; or a provisional liquidator has been appointed in respect of the corporate agent; or the corporate agent has begun to be wound up; or
- the Federal Court of Australia has disqualified the person under s 25A of the Insurance Act.

The equivalent provision for life insurers is s245 of the Life Insurance Act, which states that a person is disqualified if:

- the person has been convicted of an offence against the Life Insurance Act or its predecessor, the Life Insurance Act 1945;
- the person has been convicted of an offence against any other law of the Commonwealth or a law of a State, a Territory or a foreign country, being an offence in respect of:
    - conduct relating to insurance; or
    - dishonest conduct; or
- the person has:
    - become bankrupt; or
    - applied to take the benefit of a law for the relief of bankrupt or insolvent debtors; or

- compounded with his or her creditors; or
- the Federal Court of Australia has disqualified the person under s 245A of the Life Insurance Act.

Composition of Board

As previously stated, the board of a locally incorporated APRA-regulated institution must have a minimum of five directors, the majority of whom are ordinarily resident in Australia (if foreign owned at least two directors must be ordinarily resident in Australia).[51] Additionally, a majority of directors present and eligible to vote at all board meetings must be non-executive directors. The chairperson of the board must be independent and cannot have been the CEO of the institution in the previous three years.

APRA also impose restrictions on board representation based on shareholdings. For example, where a shareholding constitutes not more than 15 per cent of the APRA-regulated institution's voting shares, there should not be more than one board member who is an associate of the shareholder where the Board has up to six directors, and not more than two Board members who are associates of the shareholder where the Board has seven or more directors.

The key actions of an independent director involve:

- approaching the issues before them with an open mind;
- seeking to be as well informed as they reasonably can; and
- applying an independent (rather than a dependent) mind to their decision making.

The board must have a majority of independent directors at all times, with the exception of locally incorporated subsidiaries, who only need a majority of non-executive directors regardless of independence. For a locally incorporated APRA-regulated institution that is a subsidiary of a non-prudentially regulated parent company, there must still be an independent majority, but the parent company directors can sit on the board of the subsidiary.

A director is not independent if they:[52]

- are a substantial shareholder[53] of the APRA-regulated institution or an officer of, or otherwise associated directly with, a substantial shareholder of the institution;
- are employed, or have previously been employed in an executive capacity by the APRA-regulated institution or another member of the group, and there has not been a period of at least three years between ceasing such employment and serving on the board;
- have within the last three years been a principal of a material professional adviser or a material consultant to the APRA-regulated institution or another member of the group, or an employee materially associated with the service provided;
- are a material supplier or customer of the APRA-regulated institution or another member of the group, or an officer of or otherwise associated directly or indirectly with a material supplier or customer; or
- have a material contractual relationship with the APRA-regulated institution or another member of the group other than as a director.

The ASX corporate governance principles which may apply to insurers that are listed on the

[51] CPS 510 pgs 9 and 10
[52] Ibid, Attachment A pg 24
[53] As defined under the *Corporations Act 2001*s 9

Australian stock exchange, provide further guidance and state that independence may be questioned if the director:

- has close family ties with any person who falls within any of the categories described above; or
- has been a director of the entity for such a period that his or her independence may have been compromised.

The presence of such factors needs to be assessed to determine whether they will affect the director's capacity to bring an independent judgement.

Directors of insurance companies also need to meet "fit and proper" standards in accordance with APRA requirements. These are discussed in further detail at Question 3. below.

Question 2: In your opinion, what factors, conditions, or incentives might weaken the independence of the board of directors or individual members of the board?

Association with the Executive

As seen in the collapse of HIH Insurance, it is important to conduct proper due diligence over executive actions. Here, there was a culture of executive leadership not being questioned, as seen in the risky acquisition of FAI insurance which was not questioned by the HIH board. The failure to challenge the CEO's decision on the basis of his status as founder and his large influence over the board was one of the many factors that triggered HIH's collapse, a clear example of a failure to provide independent scrutiny of management proposals.

Independence should be questioned if a director or board member:

- is or has been employed in an executive capacity by the entity or any of its subsidiaries and there has not been a period of at least three years between ceasing such employment and serving on the board;
- is, or has within the last three years been, a partner, director or senior employee of a provider of material professional services (for example as an auditor or other professional advisory capacity) to the entity or any of its related entities; and
- is, or has been within the last three years, in a material business relationship (e.g. as a major supplier or customer) with the entity or any of its related entities, or an officer of, or otherwise associated with, someone with such a relationship.

The rationale behind this is that a recent relationship with an entity, whether through employment or other means, may cause a director to be overly sympathetic to management and weaken their ability to provide an independent oversight of the executive. In the US context it has been argued that despite the appointment of directors who fit these criteria, many are still overly sympathetic to management.[54] Regardless, a director is more likely to provide an objective oversight of management's actions if they have not worked with them in executive capacity or material capacity in the past.

Large Shareholdings

Independence may be compromised where directors have a large shareholding in a company. For instance, the Suncorp group announced in 2014 that all directors must own at least $200,000 of

[54] Hiring Cheerleaders: Board Appointments of "Independent" Directors

company shares.[55] It could be argued that a material conflict of interest arises where an individual that holds a large package of shares is also responsible for signing off on financial statements and making strategic and transactional decisions. This is due to the fact that remuneration is largely based on the company's performance, meaning that they could be acting in their own interests as well as the company's, with a consequential weakening of independence.

CPS 510 states that a substantial shareholder is not an independent director, which means that an independent director cannot hold more than 5% of the total number of votes attached to shares.[56] This provides some additional risk management from a governance perspective to ensure that independent directors are truly that.

Although the Suncorp directors are unlikely to have more than 5% of the number of votes attached to shares, it is arguable that having a $200,000 investment in the company is a large investment, which may give rise to concerns regarding conflicts of interest.

Remuneration

If not managed correctly by an entity's corporate governance framework, remuneration is a key factor that can weaken the independence of directors and the board as a collective. APRA recognises this, as an entity is required to maintain a documented remuneration policy that is subject to the Board's approval.[57]

In other areas of financial services regulated by APRA the Australian Government has taken a tough stance on remuneration through the recent introduction of the Banking Executive Accountability Regime Bill, which imposes a variety of statutory obligations on banks and their subsidiaries. Notably, a new deferred remuneration obligation is proposed, where companies must defer a percentage of a director's variable remuneration in order to ensure that directors make decisions that are in the long-term interests of the entity as opposed to short-term profits. A reduction in this remuneration will take place if directors fail to comply with their accountability obligations (i.e. meeting the director's duties, cooperating with APRA and acting in the company's long-term interests). Flaws and merits of this Bill aside, making decisions for an entity that are in the long-term interests of the shareholders is inexplicably tied with remuneration and this is recognised by the Australian Government. A director that is encouraging the creation of high profits at the expense of shareholder interests is not bringing an independent mind to the board.

Personal Characteristics

In order to comply with the director's duties in ss 181-184 of the Corporations Act, it is important that the requisite characteristics of honesty, integrity, due skill and diligence are met by directors and other potential board candidates. As previously stated, a major criterion for an independent director is that they are able to act in the best interests of the company as opposed to their own. Without these personal characteristics, it is impossible for a director to be truly independent. Naturally, it is difficult for individuals outside of the board to make such a character determination, which is why it is important that an entity has sufficient internal controls to ensure that the right candidate is appointed to a director position.

---

[55] Suncorp directors forced to invest under new rules, positives and negatives with policy
[56] Corporations Act s9
[57] CPS 510, pg 13

Question 3: How does an insurance company ensure that individual board members and the board collectively have enough knowledge to monitor and oversee the activities of the insurer appropriately, particularly where specific expertise is needed?

In Australia, insurance companies are regulated by both APRA and ASIC in order to ensure that directors and the board as a collective have the necessary knowledge/skills. Insurers are expected to comply with relevant legislation as well as the standards of these regulators, particularly regarding key licenses (if applicable) such as an Australian Financial Services Licence (AFSL).

An imperative for any director or board member is to ensure they understand the extent and limitations of their own knowledge base and seek appropriate advice from those with expert knowledge where required, such as an actuary, accountant and legal advisor.

For an APRA regulated insurer whether a director is considered a 'responsible person' for the purposes of the commentary ahead regarding "fit and proper persons" will largely depend on the size and nature of the organisation.

A responsible person is any person that is:

- a director of an APRA-regulated institution;
- a senior manager of an APRA-regulated institution;
- the Appointed Auditor;
- an Appointed/Reviewing Actuary;
- the Responsible Auditor; and
- performs activities for the APRA-regulated institution that may impact on the financial standing of an institution or its business (directly or indirectly).

The ability of other responsible persons to properly perform their role is crucial, as this will impact on the knowledge of the board and their ability to oversee insurer activities. As such, all responsible persons are subject to APRA's fit and proper criteria specified ahead.

Corporations Act Obligations

The general obligation of due care and diligence includes the business judgement rule,[58] which requires a director of a corporation to inform themselves appropriately about the subject matter of a judgement to the extent that they reasonably believe to be appropriate. As part of due diligence, this requires a director to ensure that they are knowledgeable by making proper inquiries as part of their role.

In Australia, entities providing a financial service are required to hold an AFSL, unless an exemption applies (in some cases an APRA regulated insurer may be exempt from this requirements if it only issues "wholesale" insurance business). Notably, there is a duty placed upon AFSL holders to maintain the competence necessary for the provision of financial services.[59] This obligation therefore extends to the directors, where they must oversee insurer activities and ensure that necessary competencies are being maintained.

APRA

Prudential standard CPS 510 states that there is a requirement for directors, collectively, to have the necessary skills, knowledge and experience to understand the risks of the institution, including its

[58] *Corporations Act 2001*, s180(2)
[59] Ibid, s 912A(1)(e)

legal and prudential obligations, and to ensure that the institution is managed in an appropriate way taking into account these risks. This does not preclude the board from supplementing its skills and knowledge by engaging external consultants and experts where specific expertise is needed.

APRA also imposes an obligation on the board to ensure that its members are fit and proper for their position. Insurers are required to have a fit and proper policy approved by the board for the appointment of directors and responsible persons, using the following assessment criteria specified in CPS 520:

- insurers must clearly define and document the competencies required for each responsible person position;
- it would be prudent for an APRA-regulated institution to conclude that the person possesses the competence, character, diligence, honesty, integrity and judgement to perform properly the duties of the responsible person position;
- the person is not disqualified under an applicable Prudential Act from holding the position;
- the person either:
    - has no conflict of interest in performing the duties of the responsible person position; or
    - if the person has a conflict of interest, it would be prudent for an APRA-regulated institution to conclude that the conflict will not create a material risk that the person will fail to perform properly the duties of the position.

The Fit and Proper Policy must form part of the institution's risk management framework,

It is also worth noting that the above criteria as well as additional criteria apply to appointed auditors and actuaries as specified in CPS 520.[60]

If an insurer complies with these criteria, then APRA will assume that the board members, appointed auditors and actuaries collectively have enough knowledge to monitor and oversee the activities of the insurer appropriately. Additionally, the fit and proper policy must include the process by which the insurer assessed whether a person was fit and proper. This process needs to include details of:[61]

- a statement of who will conduct fit and proper assessments on behalf of the APRA-regulated institution;
- the information to be obtained and how it will be obtained;
- the matters that will be considered before determining if a person is fit and proper for a responsible person position; and
- the decision-making processes that will be followed.

This must be given to any candidates for directorship for the purposes of determining whether they comply. An assessment must then take place before any director positions are filled. Insurers are therefore required to be proactive in their assessments of fitness and propriety, and cannot rely on APRA to make such assessments for them.

[60] CPS 520 – paragraph 32 for auditors, 35-39 for actuaries.
[61] CPS 520 pg 14

The Fit and Proper Policy must require annual fit and proper assessments (or as close to annual as is practicable) for each responsible person position ensuring that such persons remain appropriate for their roles.

Where an APRA-regulated institution has assessed that a person is not fit and proper, or a reasonable person in the APRA-regulated institution's position would make that assessment, the APRA-regulated institution must take all steps it reasonably can to ensure that the person:

- is not appointed to; or
- for an existing responsible person, does not continue to hold,

the responsible person position.

In addition, those who fail to meet the relevant fit and proper person standards may be removed from their position either by the board, APRA or a Court in accordance with ss 25A(3)(b), 27(2)(b), 43(2)(b), 44(1)(a) and 44(3)(b) of the Insurance Act or s245A(3)(b) of the Life Insurance Act (as applicable).

ASIC

In Australia, entities providing a financial service are required to hold an AFSL, unless an exemption applies (in some cases an APRA regulated insurer may be exempt from this requirements if it only issues "wholesale" insurance business). Notably, there is a duty placed upon AFSL holders to maintain the competence necessary for the provision of financial services.[62] This obligation therefore extends to the directors, where they must oversee insurer activities and ensure that necessary competencies are being maintained. ASIC normally assesses competence by looking at the knowledge and skills of responsible managers, although given that insurers are regulated by APRA, ASIC would usually include those who are 'responsible persons' for the purposes of APRA's 'fit and proper' standard as persons with direct responsibility for the AFSL (called responsible managers).[63]

Under an AFSL responsible managers need to have experience and qualifications or training that are relevant to their role. This means that their experience and qualifications or training need to be relevant to the financial services and products that their role relates to. ASIC will assess the skills and knowledge of a responsible manager through one of 5 options. They are as follows:

1. meet widely adopted and relevant industry standards or relevant standards set by APRA and have 3 years relevant experience over the past 5 years;
2. be individually assessed by an authorised assessor as having relevant knowledge equivalent to a diploma and have 5 years relevant experience over the past 8 years;
3. hold a university degree in a relevant discipline and complete a relevant short industry course and have 3 years relevant experience over the past 5 years;
4. hold a relevant industry- or product-specific qualification equivalent to a diploma (or higher) and have 3 years relevant experience over the past 5 years; and
5. if not relying on Options 1–4, you need to provide a written submission that satisfies ASIC that the responsible manager has appropriate knowledge and skills for their role. The submission must cover all of the information in RG 105.[64]

[62] *Corporations Act 2001*, s 912A(1)(e)
[63] RG 105 pg 8
[64] Ibid, paragraph 105.71.

For an insurer, it is most likely that option 1 is the ground on which a responsible manager will be assessed by ASIC. Together, all of the responsible managers in an organisation must have knowledge and skills that demonstrate they are capable of providing all of the financial services and products covered by an AFSL and understand the legal and compliance obligations relating to those services and products.

Question 4: Are there significant differences in terms of requirements and duties between executive and non-executive members of the board of directors of an insurer?

The recent Victorian decision of *AIG Australia Ltd v Jaques* [2014] VSCA 332 summarises some of the key legal differences between an executive and non-executive director :

The Court held that generally a non-executive director will not be a full time operative of the company, and someone is not otherwise employed by it or is delegated by it to act in its affairs.

The role of the non-executive director is generally considered to be the role of an independent overseer of the board and the company, but without operational or administrative control, which is generally left to the executive directors.

How a director is held out to the public, including the investing public, for example in company publications or corporate lodgings is not determinate.

The subjective views of the board or its individual directors as to their roles is also unlikely to be determinative.

All directors will owe a duty to exercise independent judgment and supervision as a board member. There is no different duty owed between the two roles. However the standard of care owed may vary between executive and non-executive directors.

The actual duties performed by the director is determinative of the issue. The role of a non-executive director is fundamentally different from an executive director due to their lack of involvement in the day to day management of the company.

Executive directors therefore play a more active role in insurer management. Given that they work with management on a daily basis, they will keep the rest of the board updated on the insurer's activities in this regard. Where there's an insurance group, the executive director often has a management role in another entity within the group. Given the nature of the insurance industry, the executive director will have a more direct role in areas such as risk management and reinsurance.

Given that non-executive directors are mostly independent, their role is more advisory in nature and focuses on providing an independent, objective oversight over management as opposed to participation within its function. This can be seen in CPS 510, which states that the board remuneration, audit and risk committees must all be composed of non-executive directors. By allowing these committees to be made up of non-executive directors, a more objective view of the insurer's management is established. Additionally, the majority of the board is made up of non-executive directors with the rationale that this will allow the board to remain independent from management. Another advantage of this is that non-executive directors in insurance companies are chosen for their high caliber of experience, knowledge and skills, which can be used to provide high quality advice to an executive director whenever he/she attends board meetings without compromising the independence requirements of the board.

Differences aside, both executive and non-executive directors are still subject to the director's duties contained in the Corporations Act and are expected to comply with APRA's prudential standards.

Question 5: In your jurisdiction are there any black letter rules or general principles that enable directors to rely upon external opinions when addressing issues or aspects where specific expertise when needed?

Prudential standard CPS 510 states that the board is able to supplement its skills and knowledge by engaging external consultants and experts where specific expertise is needed.

Section 189 of the Corporations Act provides that if a director relies on information, or professional or expert advice, given or prepared by:

- an employee of the corporation whom the director believes on reasonable grounds to be reliable and competent in relation to the matters concerned; or
- a professional adviser or expert in relation to matters that the director believes on reasonable grounds to be within the person's professional or expert competence; or
- another director or officer in relation to matters within the director's or officer's authority; or
- a committee of directors on which the director did not serve in relation to matters within the committee's authority; and

the reliance was made:

- in good faith; and
- after making an independent assessment of the information or advice, having regard to the director's knowledge of the corporation and the complexity of the structure and operations of the corporation; and

the director's reliance on the information or advice is taken to be reasonable unless the contrary is proved.

This provides a legal principle allowing directors to rely on external options or specific advice when fulfilling their director's duties of due care and diligence and acting in good faith in specified circumstances.

In addition to this, if a major business functions of the insurers are to be outsourced APRA requires insurers to comply with the requirements relating to outsourcing of business activities outlined in CPS 231 (if applicable).

The board of an insurer is ultimately responsible for overseeing any outsourcing arrangements, whether they are offshore or not. This involves identifying, assessing, managing, mitigating and reporting on any risks associated with an outsourcing arrangement through a risk management strategy. When assessing the options for outsourcing arrangements, communication with APRA is key and an entity must demonstrate that it has:[65]

- prepared a business case for outsourcing the material business activity;
- undertaken a tender or other selection process for selecting the service provider;
- undertaken a due diligence review of the chosen service provider, including the ability of the service provider to conduct the business activity on an ongoing basis;
- involved the board of the APRA-regulated institution, board committee of the APRA-regulated institution, or senior manager of the institution with delegated authority from the board, in approving the agreement;
- considered all the matters outlined below, that must, at a minimum, be included in the outsourcing agreement itself;
- established procedures for monitoring performance under the outsourcing agreement on a continuing basis;

[65] CPS 231 pg 7.

- addressed the renewal process for outsourcing agreements and how the renewal will be conducted; and
- developed contingency plans that would enable the outsourced business activity to be provided by an alternative service provider or brought inhouse if required.

When outsourcing to a related body corporate the insurers must be able to demonstrate it has:

- assessed the changes to the risk profile of the business activity that arise from outsourcing the activity to a related body corporate and how this changed risk profile is addressed within the institution's risk management framework;
- confirmed that the related body corporate has the ability to conduct the business activity on an ongoing basis;
- taken into account the required monitoring procedures to ensure that the related body corporate is performing effectively and how potential inadequate performance would be addressed;
- looked at contingency issues in accordance with business continuity management standard CPS 232 should the outsourced activity need to be brought in-house; and
- assessed the relevance of these above mentioned requirements to the extent they are relevant to outsourcing arrangements with a related body corporate.

Outsourcing arrangements should be evidenced by a legally binding outsourcing agreement that must be signed by all relevant parties. This agreement must include:[66]

- the scope of the arrangement and services to be supplied;
- commencement and end dates;
- review provisions;
- pricing and fee structure;
- service levels and performance requirements;
- the form in which data is to be kept and clear provisions identifying ownership and control of data;
- reporting requirements, including content and frequency of reporting;
- audit and monitoring procedures;
- business continuity management;
- confidentiality, privacy and security of information;
- default arrangements and termination provisions;
- dispute resolution arrangements;
- liability and indemnity;
- sub-contracting;
- insurance; and
- to the extent applicable, offshoring arrangements (including through subcontracting).

These requirements do not apply to an arrangement with a related body corporate unless APRA requests a documented arrangement, another prudential arrangement requires an arrangement or the arrangement is between a category D insurer and a related body corporate.

Should a documented arrangement be necessary, an entity is required to include a clause that allows APRA access to documentation and information related to this agreement, which may include on-site visits to a service provider. There is also a notification requirement, where an entity needs to

[66] Ibid pg 8.

notify APRA within 20 business days after the outsourcing arrangement is executed. The notification must include a risk assessment, which includes the key risks involved in the arrangement and any risk mitigation strategies.[67] The notification process is accompanied by a consultation phase, where APRA must satisfy itself that the impacts surrounding the arrangement have been encompassed in the entity's risk management framework. Insurers are required to ensure that sufficient resources are allocated to the management of the outsourcing relationship, which includes maintaining regular contact with the service provider, as well as some criteria for monitoring performance.[68]

Audit also plays a role in outsourcing, where there must be regular reviewing and reporting to the board on compliance with the outsourcing policy. APRA may also request an external auditor or other expert to provide an assessment.

These outsourcing requirements provide a prudential standard to ensure outsourcing of business activities and reliance on third party service providers is undertaken with due care and diligence in line with general directors duties.

Question 6: Describe the extent and scope of supervisors'/regulators' intervention with reference to the qualifications and to the activities of the board of an insurer.

As discussed in Part II, Question 3, APRA must be satisfied that a director or other responsible person fulfils requirements of fitness and propriety outlined in CPS 520. A failure to comply with this prudential standard should be notified to APRA and could also be a matter that is required to be reported to ASIC under s912D of the Corporations Act if the insurer holds an AFSL. Additionally, ASIC has powers of investigation for any breaches of the *Corporations Act 2001*such as the director duties mentioned in Part II, Question 1.

Under the *Insurance Act 1973* s25A, APRA may apply to the Court to disqualify a director or senior manager of a general insurer if the person is not fit and proper and the disqualification is justified. Additionally, if the director or senior management is responsible for any activities in contravention of APRA's prudential standards or breach of director duties, then a disqualification will also take place on this basis. Pursuant to s 27 of the Insurance Act, APRA is able to remove the director of a general insurer, authorised NOHC or a general agent. Under this provision, APRA may direct (in writing) that the general insurer, authorised NOHC or corporate agent remove the person from the position if the person is disqualified or does not meet one or more of the criteria for fitness and propriety set out in the prudential standards. The corresponding provision for life insurers can be found in s 245A of the *Life Insurance Act 1995*.

Question 7: Are there any special rules and regimes applicable to the governance of subsidiaries belonging to an insurance group, also in terms of information flows?

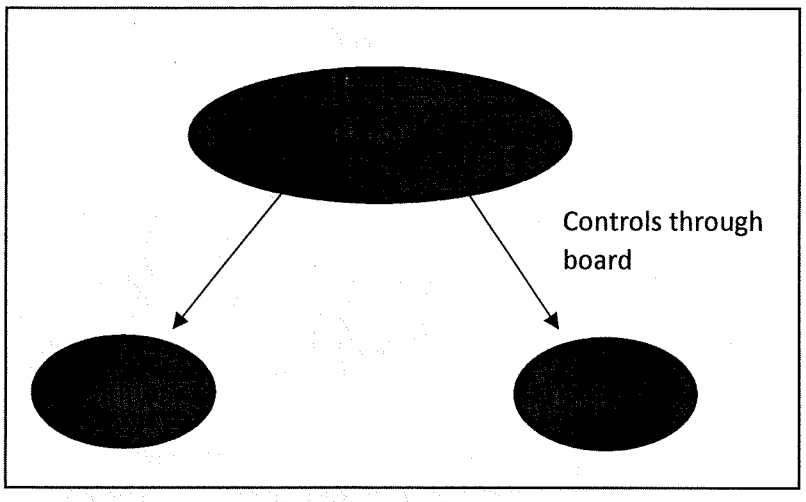
General Insurers

Level 2 Insurance Groups:

In Australia, general insurers may form part of a level 2 insurance group, which are regulated by similar prudential standards to those of individual insurers with some minor exceptions. It is worth noting that a Level 1 insurer refers to an individual insurer that is authorised under s 12 of the Insurance Act and part of a Level 2 insurance group. A level 2 insurance group can take the following forms:

[67] Ibid pg 10.
[68] Ibid pg 11.

Option (a):

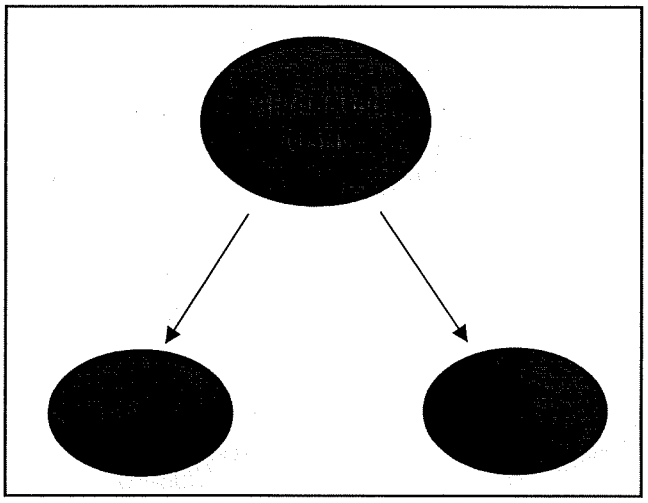


No authorised NOHC (Non-Operating Holding Company

Consolidated

(a) where there is no authorised non operating holding company NOHC and an insurer has controlled entities, the consolidation of the insurer and its controlled entities; or

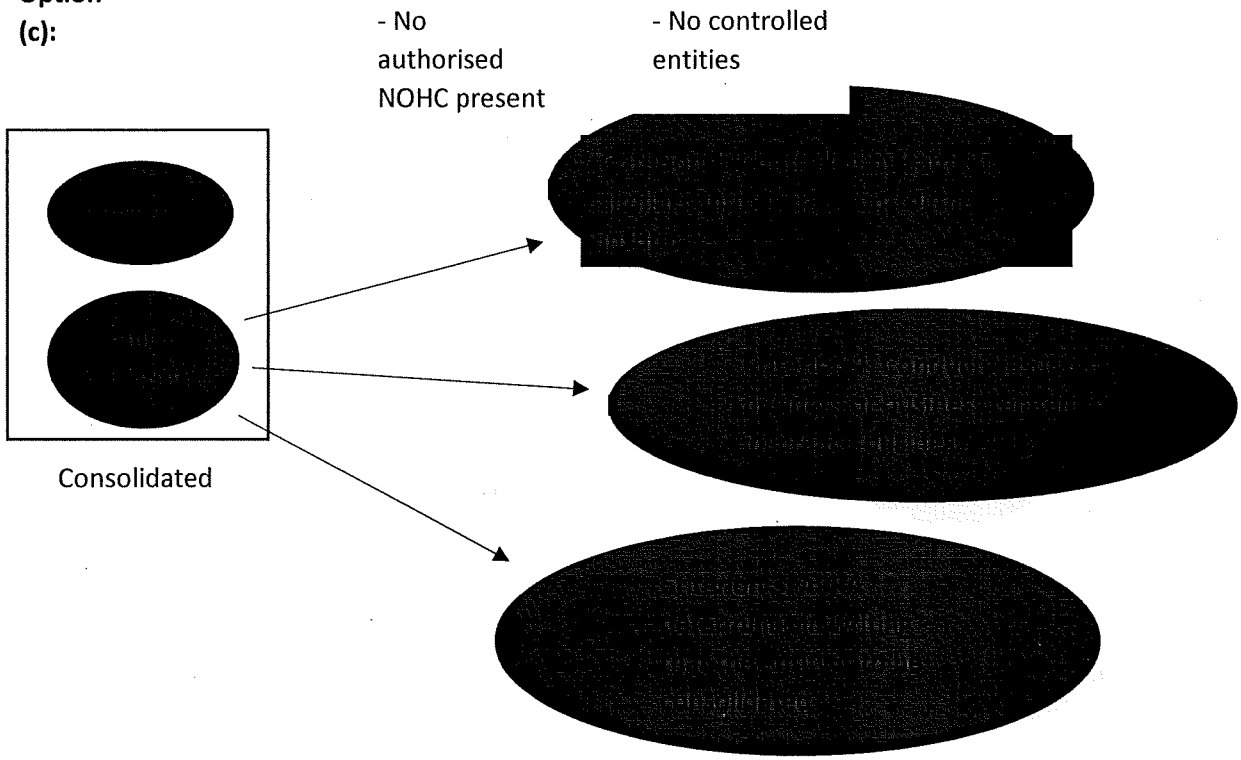
Option (b):



Consolidated group

(b) where there is an authorised NOHC, the consolidation of the authorised NOHC and its controlled entities; or

Option (c):



(c) where there is no authorised NOHC and an insurer does not have controlled entities, the consolidation of the insurer and any entity that meets the following criteria:

- the entity is subject to control by an entity or group of related entities that are the same or very similar to the entity or group of related entities that control the insurer; and
- the entity conducts insurance business or business related to insurance business; and
- APRA determines, in writing, that the entity is to be consolidated.

APRA may also determine that the entity is not to be consolidated despite meeting requirements 1 and 2.

All entities conducting insurance business (regulated and unregulated)[69] within a Level 2 insurance group must be consolidated. Consolidation must be in accordance with the requirements of Accounting Standards including AASB 10 for the production of consolidated financial statements.

APRA may, in writing, determine that an entity is to be consolidated, despite that entity not being a controlled entity of the insurer or authorised NOHC, if:

- the entity is controlled by an entity or group of related entities that are the same or very similar to the controlling entity/group of related entities in control of other Level 2 members; and
- it conducts insurance business or business related to insurance business.

Although APRA has the discretion to determine the parent/head of an insurance group (an insurer, authorised NOHC or a subsidiary of either), generally the parent entity is:

[69] As defined in s 3 of the Insurance Act 1973.

- where the Level 2 insurance group is headed by an authorised NOHC, the authorised NOHC; and
- where the Level 2 insurance group is headed by an insurer, the insurer.

Group Requirements

Given the difficulty and complexity associated with governance of insurance groups, the head of an insurance group must maintain governance arrangements in accordance with CPS 510.[70] This involves the approval of the head of the group's board (head board) for a documented group remuneration policy as well as a group internal audit function. . A group actuarial function is also required pursuant to Attachment C of GPS 320.

An insurance group's remuneration policy is subject to the same requirements as an individual insurer, as detailed in Part 1, Question 1. and must outline:

- Performance-based components of remuneration must be designed to align remuneration with prudent risk-taking, including:
    - the outcomes of business activities;
    - the risks related to the business activities taking account, where relevant, of the cost of the associated capital; and
    - the time necessary for the outcomes of those business activities to be reliably measured.
- Performance-based components for the board, senior officer or compliance committee as relevant should be adjusted downwards if necessary to protect financial stability of the institution or respond to significant unforeseen consequences.
- Policy needs to set out who is covered by the policy, including, risk and financial control personnel, significant personnel with performance-based remuneration and all responsible persons aside from:
    - Non-executive directors;
    - Appointed auditors or responsible auditors;
    - For general insurers, external Appointed Actuaries and the Reviewing Actuary;
    - For Category C insurers, the senior officer outside Australia, and nonexecutive directors of the Category C insurer's agent in Australia where the agent in Australia is a corporate agent;
    - For life companies, external Appointed Actuaries; and
    - In the case of an EFLIC, members of the Compliance Committee

The group internal audit function is subject to the same requirements as an individual entity's audit function. The internal audit function must still include evaluation of the adequacy and effectiveness of the financial and risk management framework of the group. To fulfil its functions, the internal auditor must, at all times, have unfettered access to the group's business lines and support functions, meaning access to all entities within the group.

[70] CPS 510 pg 7

The head board is ultimately responsible for the prudent governance of the insurance group and is required to have group remuneration, audit and risk committees that are all subject to the same requirements specified in Part I, Question 1. The function of these group committees is the same, except the scale of their activities will be larger given the larger number of entities.

The head board is tasked with ensuring that directors and senior management within the group have the characteristics and skills necessary for the group's effective oversight and prudent management.

Regarding risk management and outsourcing, the standards in CPS 220 and CPS 231 must be applied on a group basis and ensure that the standards are applied appropriately to each entity. As part of risk management, the head of the level 2 insurance group is required to make sure that the group collectively maintains sufficient capital, has a group ICAAP, and inform APRA of any changes in the group's actual or anticipated capital adequacy.

Group Auditor Requirement

The parent entity of a level 2 insurance group is required to appoint a group auditor in addition to individual auditors for each entity. As stated in GPS 310, the group auditor of a Level 2 insurance group must fulfil the fit and proper criteria and be one of the following persons:

- the Appointed Auditor of the parent entity where the parent entity is an insurer;
- the Appointed Auditor of an APRA-authorised insurer within the group; or
- a responsible auditor of the parent entity where the parent entity is an authorised NOHC.

The group auditor cannot be:

- the group actuary (as discussed ahead);
- the actuary of an entity within the group carrying on insurance business;
- an employee or director of the entity of which a person referred to in the sub- paragraphs above is an employee or director; or
- a partner of a person referred to in the sub-paragraphs above.

The group auditor's role involves providing an independent and objective view of the truth and fairness of the group's annual accounts required by reporting standards, whilst also assessing the group's systems, procedures and controls used to address compliance with prudential requirements and for the purposes of producing reliable financial data. Their responsibilities also include:

- conducting a limited assurance review of the annual accounts of the group, whilst providing a report on the findings of this review, which must address whether:
    - the returns provided to APRA give a fair view of the level 2 insurance group's financial position;
    - systems, procedures and controls exist in accordance with the prudential requirements, which also extend to actuarial data and financial reporting;
    - any details of non-compliance with the prudential requirements have been identified;
    - the group has complied with its risk management strategy and reinsurance management strategy;
    - the group has systems, procedures and controls in place to ensure that reliable statistical and financial data are provided to APRA in the semi-annual returns required by reporting standards made under the Collection of Data Act; and
    - there are matters which have come to the Group Auditor's attention that will, or are likely to, adversely affect the interests of policyholders of the group.
- on an annual basis, reviewing and testing the group's systems, processes and controls

designed to:
    - address compliance with all prudential requirements;
    - enable the group to report reliable financial information to APRA; and
- undertaking a special purpose review of matters specified by APRA that relate to the Level 2 insurance group's operations, risk management or financial affairs, whilst also preparing a report in respect of that review.

Group Actuary Requirement

Level 2 insurance groups must appoint a group actuary,[71] who must meet the fit and proper requirements specified in CPS 520, be a member of a recognised professional body for actuaries, hold appropriate qualifications and have a minimum of 5 years post-qualification experience with an insurer. The group actuary cannot be:

- the Group Auditor;
- the auditor of an entity within the Level 2 insurance group carrying on insurance business;
- an employee or director of an entity of which a person referred to above is an employee or director;
- a partner of a person referred to above; or
- the Chief Executive or a director of any entity within the Level 2 insurance group or its wider corporate group (where applicable).

The group actuary is still required to prepare Financial Condition Reports as well as Insurance Liability Valuation Reports (ILVRs) on a group basis. Similar to the requirements surrounding the group actuary, it is the responsibility of the level 2 insurance group to provide the actuary with any information provided by APRA or requested by the actuary in order to help them perform their duties. This will include access to all data, reports, staff and other information possessed by the board of the parent entity, the board committees, the board of any other group entities and the committees of these entities.

The role and responsibilities of the group actuary focus on providing advice on the valuation of the group's insurance liabilities. This is encompassed in an annual preparation of the ILVR and corresponding investigations necessary for its preparation. A group actuary must also conduct an actuarial assessment of the group's insurance liabilities for a half-yearly report that must be submitted to APRA in accordance with the requirements discussed in Part I, Question 1.

For a level 2 insurance group, it is important that another actuary reading the ILVR is able to gain an understanding of the suitability of any accounting figures for overseas business (as discussed ahead), consolidation adjustments, inherent limitations in the process for the design of the ILVR and risks associated with insurance liabilities.

In each ILVR, the group actuary must comment on the advice provided to the group in relation to the two half-yearly reports immediately preceding the date of the ILVR. Those comments should cover the extent to which the advice was accepted by the group in preparing its half-yearly reports and the extent to which the actuary has amended the valuation of insurance liabilities in the ILVR compared to the last advice given to the group for the half-yearly report at the group's balance date. The ILVR will also include the group's categories of insurance business for the purposes of GPS 001 and an assessment of the group's insurance concentration risk charge with regard to reinsurance arrangements and the business being undertaken.

[71] GPS 320 Attachment C, paragraph 1

APRA may also require the group actuary to conduct a special purpose review in a similar manner to the group auditor. This can also be subject to a special purpose external peer review.[72]

Given that level 2 insurance groups can comprise both international and Australian business, insurance liability valuations will need to take this into account. For Australian business, the insurance liability valuation will be conducted in accordance with the earlier specified criteria. This will be applied with relevant adjustments that take into account intra-group transactions. For the international business, any outstanding claims or premiums liabilities will need to be determined before creating the ILVR.

Reinsurance

Regarding reinsurance, the following apply to Level 2 insurance groups:

- given that level 2 insurance groups can contain international entities, it is important that their reinsurance management strategy covers international business;
- furthermore, the 2-month and 6-month rules (detailed in the Part I, Question 7 table) do not apply to the international business of a level 2 insurance group;
- level 2 insurance groups do not need to undertake reinsurance declarations; and
- APRA does not require submission of Limited Risk Transfer Arrangements that a non-insurer entity proposes to enter into. However, details of entrance into such arrangements must be provided.

Level 3 groups

APRA may determine a Level 3 group where:

- it considers that material activities are performed within the group across more than one prudentially regulated industry and/or in one or more non-prudentially regulated industries (ie. a conglomerate); and
- it wants to ensure that the ability of the group's prudentially regulated institutions to meet their obligations to depositors, policyholders is not adversely impacted by risks emanating from the group, including its non-prudentially regulated institutions.

As such, both general and life insurers can form part of a level 3 group. The level 2 insurance group requirements will also apply to level 3 insurers on a similar basis with some slight differences. For instance, the same requirements for a level 2 insurance group regarding an ICAAP apply, with the difference that a level 3 head is not required to have a group ICAAP.[73]

3PS 310 states that a level 3 head must appoint a group auditor, who complies with the fitness and propriety requirement in CPS 520 and satisfies the auditor independence requirements/functions in CPS 510. This auditor will report to the level 3 head's group audit committee established in accordance with CPS 510, which also requires the establishment of a group risk and remuneration committee. The head of a level 3 group is also in charge of ensuring that the group risk management framework incorporates the requirements of prudential standard CPS 220, discussed in Part I, question 1.

[72] GPS 320 Attachment C, paragraph 23.
[73] CPS 220 Footnote 6, paragraph 23(e)

Part III – Risk Management

Question 1: In your opinion, what is the biggest risk challenge (e.g. regulation, capital standard, pricing, interest rate, cyber, terrorism, etc.) facing the insurance industry today in your jurisdiction?

It has been accepted by both ASIC and APRA that cyber crime is a risk challenge that is at the forefront of the financial services industry, particularly insurance. The difficulty with cyber risk management is that it requires continual investment in sound governance practices as technology continues to develop. Cyber crime poses a major threat to the insurance industry given its dynamic nature and continually new methods of perpetration. This not only provides a challenge for the internal governance of insurers, but it also impacts on their ability to properly gauge risk and pricing for the sale of cyber insurance products.

This was noted in APRA's 2017-21 corporate plan, where it outlined the increasing prominence of cyber security risks as a result of technology's development. Being able to review how APRA-regulated institutions address these risks whilst also enhancing its own processes for mitigating cyber security risks is high on its list of priorities.

Additionally, APRA released Insight Issue 4 in December 2017, which discusses the high uptake of cyber insurance as a focus area. The results from APRA's 2017 Cyber Security Survey indicate that 74% of respondents have a cyber insurance policy, with a further 17% considering the purchase of cyber insurance. This highlights the growing concern surrounding the risk challenges associated with cyber security, as the main reasons for the increasing use of cyber insurance include:

- increased exposure to cyber risk;
- liability risk for third party data;
- better access to cyber response capabilities;
- new or maturing cyber insurance offerings; and
- the introduction of mandatory breach reporting requirements (for example in relation to Privacy Act breaches).

Given that this is a relatively new area of insurance, there is minimal actuarial data or claims history. As such, APRA expects insurers to engage in extensive initial and ongoing due diligence to assess and price for risk.

As outlined in the Cyber Security Survey, cyber-attacks on APRA-regulated institutions are increasing in prevalence and the following types were reported:

- ransomware and other malware: This was the most common incident reported, where malicious software has been used to encrypt essential data for ransom purposes. APRA has highlighted the need for institutions to have effective anti-malware solutions and the importance of back-up data that will not be affected by such an attack;
- distributed denial of service: The second most common incident, where users are unable to access digital services due to an overwhelming number of fake access requests. This is a risk that should be subject to internal controls;
- hacking of an internet-facing platform: Attackers were able to execute commands on servers to create and delete files. Hardened configurations, end-point protection and network segmentation prevented attackers from accessing sensitive customer data and this risk was largely mitigated;
- sensitive data leakage: Incidents included sensitive data being sent by an employee to a private (external) email address. This highlights the importance of data loss prevention

controls;

- phishing: The attempt to obtain sensitive information such as passwords or other credentials. This has been largely reduced through staff and customer education regarding cyber safety, yet it is still a material risk that insurers should consider; and
- website defacement: This was also reported as a minor issue, but the need for constant monitoring of websites to identify unauthorised changes should take place.

Another major area of concern for insurers is the currency of information hardware/software. Only 50% of respondents in the 2017 survey reported that their hardware/software was up to date. It is important to ensure that information assets are current and capable of being encompassed within mainstream IT support, as dated technology may not be able to address risks associated with cyber crime. APRA recommends that all institutions have an approach to information asset lifecycle management that is covered by an entity's risk management framework.

ASIC has also acknowledged the prevalence of cyber crime and provides guidance on cyber risk management in Report 429 – Cyber resilience: Health check. This has been accomplished through:

- increasing awareness of cyber risks;
- encouraging collaboration between industry and government and identifying opportunities for our regulated population to improve its cyber resilience; and
- identifying how cyber risks should be addressed as part of current legal and compliance obligations that are relevant to ASIC's jurisdiction.

Cyber crime has been identified as a systemic risk for all financial services institutions, meaning that any unmitigated risks in the financial system will have serious consequences for the economy. ASIC notes that there has been significant growth in the number and severity of cyber attacks globally – the total number of cybersecurity incidents detected in 2014 was 42.8 million, which was a 48% increase from 2013. Even more problematic was the estimate that 71% of cybersecurity incidents went undetected at the time this report was released (March 2015).

Question 2: What specific laws or regulations, actual or pending in your jurisdiction, will present significant implementation risk challenge toward the insurance industry?

From a corporate governance perspective, Australia recently commenced a Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry ('Royal Commission'). A financial services entity includes every general insurer, life insurer, reinsurer, AFSL holder and authorised representatives. The terms of reference for this inquiry have been released, which can be found within the Letters Patent. The key elements are as follows:

Misconduct

Whether any conduct amounts to misconduct, or whether any conduct falls below community standards and expectations. Misconduct includes conduct that constitutes an offence, is misleading or deceptive, is a breach of trust, breach of duty or unconscionable conduct, or is conduct that breaches a professional standard or a recognized and widely adopted benchmark for conduct.

Culture and remuneration

Whether any misconduct or poor conduct is attributable to culture and governance practices in a financial services entity, or in the relevant industry or industry sector. This also extends to whether the misconduct or poor conduct results from other practices, including recruitment and remuneration practices, of a financial services entity or the relevant industry or industry sector.

Redress

This element focuses on the effectiveness and adequacy of existing redress mechanisms for consumers who have suffered detriment resulting from the misconduct of financial services entities. This could include civil claims for damages for breach of statutory or common law duties to the client, or external dispute resolution processes (such as the Financial Ombudsman Service, which is soon to become part of the Australian Financial Complaints Authority).

Regulatory framework

The adequacy of existing laws, forms of industry self-regulation (including industry codes of conduct) and internal systems within entities to identify, regulate and address misconduct (and conduct that does not meet community standards), in order to meet community standards and expectations and to provide redress to consumers.

Regulator effectiveness

The effectiveness and ability of regulators to identify and address misconduct (i.e. breaches of the law and/or legal duties).

The need for further reform

Taking into account law reforms already announced by the Federal Government, whether any further changes are necessary to minimise the likelihood of misconduct. Changes might include:

- the legal framework;
- practices within financial services entities; or
- the operations of financial regulators.

Although the Royal Commission is in its early stages, there is potential for new laws and regulations to arise from any findings that may occur. Should such laws and regulations come into existence, there may be significant implementation risk challenge to the insurance industry and a need to update governance practices.

For life insurers, an Inquiry into the life insurance industry began in September 2016. One of its main terms of reference was the need for further reform and improved oversight of the life insurance industry. APRA has noted the need for continually high supervisory intensity of individual life insurers. For instance, APRA recently engaged with the board and senior management of CommInsure to gain assurance over the robustness and completeness of the independent reviews commissioned to investigate the allegations of poor claims handling practices and unethical

behaviour and to ensure a focus on stakeholder and community expectations throughout the review process.[74]

Although no report will be released until 31 March 2018, this could pave the way for new legislation/regulations that may impact on life insurer governance and present significant implementation risk.

The Treasury Laws Amendment (Design And Distribution Obligations And Product Intervention Powers) Bill 2018 is also currently under consultation and is intended to introduce:

- design and distribution obligations for financial products to ensure that products are targeted at the right people; and
- a temporary product intervention power for the ASIC when there is a risk of significant consumer detriment.

The Bill (if passed) will amend the Corporations Act to include the following Design and distribution obligations related changes that apply to general and life insurance products issued to retail clients and other risk management products (e.g discretionary mutuals) for which a PDS is required:

- four new design obligations (apply to issuer/insurer):
    - to make a target market determination in relation to the product;
    - to review the target market determination as required to ensure it remains appropriate;
    - keep records of the person's decisions in relation to the new regime; and
    - to notify ASIC of any significant dealings in a product that are not consistent with the product's target market determination;
- five new distribution obligations (can apply to issuer and distributors, including insurer agents and brokers (when acting for insurers or not)):
    - not to deal, or provide financial product advice, in relation to a product unless a target market determination has been made;
    - not to deal, or provide financial product advice, where a target market determination may no longer be appropriate;
    - to take reasonable steps to ensure that products are distributed in accordance with the target market determination;
    - to collect information related to the distribution of a product; and
    - to notify the issuer of a product of any significant dealings in the product that are not consistent with the products target market determination.

- new content in s1018A advertising notices regarding the target market;
- new ASIC powers to request information relevant to its regulatory role; issue stop orders in relation to suspected contraventions of the new regime; and make exemptions and modifications to the new regime;
- provide ASIC with a new broad product intervention power – new product intervention power to regulate, or if necessary, ban issue of harmful financial products (including insurance and discretionary mutuals) to retail clients where there is a risk of significant consumer detriment.

[74] APRA submission - Parliamentary Joint Committee on Corporations and Financial Services - Inquiry into the life insurance industry pg 19

The estimated increase in annual compliance costs for the industry as a whole will amount to – $232.1 million for the design and distribution changes and $7.7 million for the product intervention power changes. Industry believes it will be significantly more and consultation continues.

Part IV – Ethics and Corporate Social Responsibility

Question 1: Please provide any concrete examples where business ethical standards and/or corporate social responsibility standards have been applied and have changed the behaviors of the insurance company.

In Australia, ASIC regularly issues enforceable undertakings against companies that have breached their obligations, both ethical and legal. These ensure that insurers are behaving in a manner that does not detriment consumers. The following examples directly relate to the conflicted remuneration provisions in the Corporations Act,[75] where benefits given to financial services licensees/representatives directly influence the choice of financial product recommended to a retail client, as well as the resulting advice.

A recent example involves Youi Insurance, where ASIC was concerned that Youi's remuneration and bonus structures incentivised sales staff to prioritise sales ahead of consumer interests.

Youi has refunded 102 consumers approximately $14,000 in total, and will pay $150,000 as a community benefit payment to the Financial Rights Legal Centre's Insurance Law Service, after ASIC raised concerns about its home and car insurance sales practices.

Additionally, Youi engaged an independent firm to conduct a review of sales practices in response to concerns that "some sales staff were charging consumers for insurance policies without their consent to purchase. This included where consumers only made an inquiry to get an insurance quote".

Since this review, ASIC reports that Youi has altered its behaviour by:

- changing its remuneration structure and reduced the incentives provided to sales staff based on sales volumes;
- reviewing sales scripts and staff training;
- introducing new controls and monitoring of sales staff; and
- making significant changes to its legal, risk and compliance capability.

ASIC has released three reports covering its review of the sale of add-on insurance through car dealers, which found that the insurance is expensive, of poor value and provides consumers very little or no benefit (refer REP 470, REP 471, REP 492).

These reviews have had the effect of changing its behaviour by insurers and have resulted in action being taken by ASIC against a number of insurers, including for example an enforceable undertaking entered into between ASIC and Swann Insurance. Following ASIC's concerns that Swann Insurance offered add-on insurance products bought through car and motorbike dealerships that were of minimal value, a $39 million refund to 67,960 customers will take place. Swann will offer to:

[75] Pt 7.7A, Division 4.

- refund the premium paid by customers who claimed on their Swann comprehensive car insurance and obtained a replacement vehicle;

- partially refund customers who were sold excessive cover;

- refund the premium paid by customers for policies with little or negative value; and

- for customers who paid their loan off early, partially refund the insurance premium from the date the loan was paid off.

ASIC has also taken similar action against other insurers in this add on insurance space as per the examples below and remains focused on improving consumer outcomes from insurers in the add on insurance market:

- Virginia Surety to refund over $330,000 to add-on insurance customers (refer: 17-189MR);
- QBE refunds $15.9 million in add-on insurance premiums (refer: 17-258MR).

Question 2: In your jurisdiction, are there any specific laws or regulations already adopted or any proposals, or any arrangements in place in the governance system, relating to the protection of policyholders' and/or financial consumers' interests?

As stated in Part II, Question 1, there are numerous director duties contained in the Corporations Act that are required to be upheld. These involve sections 180(1) (duty of due care and diligence), 181(1) (duty of good faith) and 182 (improper use of position). The director's duties ensure that board members act in the best interests of shareholders by ensuring that the company is run in a sustainable manner. If a breach of these duties takes place, company directors will be guilty of an offence under s 1311, where a penalty will be pursued to protect the interests of the public.

As previously mentioned, there is also a requirement for those conducting financial services business to hold an AFSL (s 911A). The AFSL obligations protect policyholders/financial services consumers by ensuring that all licence holders are competent in the provision of their services, whilst also complying with all relevant legislation, regulations and standards. Given that a corporate entity can hold an AFSL, internal corporate governance must ensure that the entity:[76]

- does all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly;
- has in place adequate arrangements for the management of conflicts of interest that may arise wholly, or partially, in relation to activities undertaken by the licensee or a representative of the licensee in the provision of financial services as part of the financial services business of the licensee or the representative;
- complies with the conditions on the licence;
    - conditions can be imposed by ASIC (s 914A), which can be done for the protection of policyholder and consumer interests;
- complies with the financial services laws;
- takes reasonable steps to ensure that its representatives comply with the financial services laws;

[76] Corporations Act s 912A.

- has available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence and to carry out supervisory arrangements;
- maintains the competence to provide those financial services;
- ensures that its representatives are adequately trained and are competent, to provide those financial services;
- if those financial services are provided to persons as retail clients--have a dispute resolution system;
    - this involves compulsory membership of an ASIC approved external dispute resolution scheme (such as the Financial Ombudsman Service);[77] and
- has adequate risk management systems.

If there is a breach of these AFSL obligations, the licensee must have adequate arrangements (approved by ASIC) in place to compensate the retail consumers/clients (s 912B). These arrangements include a mandatory obligation to hold professional indemnity insurance to compensate retail clients for losses they suffer as a result of a breach by the licensee or its representatives of their obligations in Ch 7 of the Corporations Act. Such insurance requirements must meet the guidelines specified by ASIC in RG 126.

In addition, the Australian government has established the Financial Claims Scheme (FCS) that protects depositors of authorised deposit-taking institutions (banks, building societies and credit unions) and policyholders of general insurance companies from potential loss due to the failure of these institutions. For general insurers, the FGS provides compensation to eligible policyholders with valid claims against a failed general insurer. Under the FCS, most policyholders with the affected general insurer are covered for valid claims up to $5,000. For any valid claims of $5,000 and over, the policyholder or claimant must be eligible under certain criteria.

Question 3: In your jurisdiction, is an insurance company required to produce an annual Corporate Social Responsibility (CSR) report or a Global Sustainability Initiative (GSI) report? If so, what context needed to be disclosed in these reports?

Although there is no specific requirement to produce an annual CSR or GSI report, listed insurance companies are still expected to make disclosures that cover similar topics. As stated in the ASX Corporate Governance Recommendations, a listed entity should disclose whether it has any material exposure to economic, environmental and social sustainability risks and, if it does, how it manages or intends to manage those risks.[78] The rationale behind this is to aid investors in properly assessing the risk associated with an insurance company. Meeting this recommendation does not require the publishing of a sustainability report, though a company can choose to do so in order to meet this recommendation.

Rule 4.10.3 of the ASX Listing rules states that listed companies need to disclose how they fulfil the ASX Corporate Governance Recommendations in their annual report. As such, listed insurance companies will generally include information on how they manage economic, environmental and social sustainability risks in their annual reports as opposed to a separate CSR or GSI report.

[77] Ibid 912A(2)(b).
[78] ASX Corporate Governance Recommendations pg 30

Part V - Disclosure

Question 1: In your opinion, what mechanisms shall be in place or considered in an insurance company to ensure the transparency of its governance structure? (e.g., the articles of association, the organization chart, any existing committees, the major shareholders, the ethical standard, corporate social responsibility, etc.)

The risk, audit and remuneration committees are all important mechanisms for ensuring independent oversight of an insurer's governance in these areas. As stated in CPS 510, insurers are required to have a written charter that outlines each Committee's roles, responsibilities and terms of operation. In practice, these charters will also disclose the composition of the committees, as well as the qualifications/experience of each committee member. Additionally, the ASX corporate governance recommendations suggest that listed corporate entities disclose the charter of each committee. By providing such information on each committee, both shareholders and the general public are able to access invaluable information that can aid their understanding of an insurer's internal governance structure and how a board intends to uphold shareholder objectives.

In conjunction with board charters, listed companies in Australia are subject to compulsory annual reporting requirements by publishing an annual report.[79] These compulsory reporting requirements are a key mechanism of ensuring corporate governance transparency within insurance organisations by including the following material:

- directors' report (including the remuneration report),[80] which contains the following information:
    - the operations of the company;
    - the financial position of the company;
    - the business strategies of the company and its prospects for future financial years (unless their inclusion would be unreasonably prejudicial);
    - significant changes in the company's state of affairs;
    - the company's principal activities and any significant changes in the nature of those activities;
    - future activities; and
    - remuneration of directors and key management personnel.
- corporate governance report,[81] which discloses the extent to which they have followed the ASX Corporate Governance Recommendations;
- financial report[82] containing information on a company's financial performance through the inclusion of four primary financial statements:
    - a statement of comprehensive income;
    - a statement of financial position;
    - a statement of changes in equity; and
    - a statement of cash flows.
- the auditor's report[83] on the financial and remuneration reports, including an opinion on whether:
    - the financial report complies with the Corporations Act 2001, the Australian Accounting Standards and International Financial Reporting Standards; and
    - all information, explanations and assistance necessary for the audit has been given, whether sufficient financial records have been kept to enable the financial report to

[79] pursuant to ASX Listing Rules 4.3A-4.3B.
[80] required by *Corporations Act* s 298
[81] ASX Listing Rule 4.10.3
[82] *Corporations Act* s 292
[83] *Corporations Act* s 301

be prepared and audited, and whether other records and registers as required by the Corporations Act 2001 have been kept.

In conjunction with the annual reporting obligations, the annual general meeting[84] is an invaluable transparency mechanism for shareholders/members to gain valuable insights into an insurance company and its governance structure. This meeting considers topics such as the annual financial, remuneration, directors' and auditor's reports, the election of directors, the appointment of the auditor and the fixing of the auditor's remuneration. Voting takes place on the remuneration report, although any resolutions reached on this are advisory. Members can ask questions of an auditor (who must attend under s 250RA of the Corporations Act if the company is a listed company) on topics such as:

- the conduct of the audit;
- the preparation and content of the auditor's report;
- the accounting policies adopted by the company in relation to the preparation of the financial statements;
- the independence of the auditor in relation to the conduct of the audit; and
- any written questions that have been submitted.

Additionally, members are able to ask questions or make comments about company management.

In addition to the annual report, another important transparency mechanism is the establishment of a code of conduct,[85] which assures shareholders that corporate governance affairs are being managed in a responsible and ethical manner by directors that hold high personal integrity. A typical code of conduct might involve:

- a commitment to acting ethically and responsible in upholding its legal obligations;
- an expectation that all directors and staff will:
    - act in the entity's best interests;
    - act honestly and with high standards of personal integrity;
    - comply with the laws and regulations that apply to the entity and its operations;
    - not knowingly participate in illegal or unethical activities;
    - not enter into activities or arrangement that compromise the entity's reputation or best interests;
    - not take advantage of customers;
    - not take advantage of their position;
- describe the organisation's anti-bribery measures;
- process handling for conflicts of interest; and
- measures for reporting unethical behavior (i.e. whistleblowers).

In addition to the above mechanisms, insurers should disclose information to shareholders regarding the background of all directors (not just those within board committees) and why they fulfil the fit and proper criteria described in CPS 520. In combination with a code of conduct, this ensures full transparency regarding the ability of the directors to engage in sound corporate governance practices.

[84] *Corporations Act* s 250N
[85] ASX Corporate Governance Recommendations pg 19

Question 2: Are there any governance practices that, in your opinion, can best be achieved through disclosure rather than through specific supervisory requirements? Which governance practices should be mandatory for an insurance company?

Reporting obligations in any form are better achieved through disclosure as opposed to specific supervision, as they encourage good governance within entities whilst also aiding regulators in the effective performance of their role.

As stated in the previous question, all corporations in Australia are mandatorily required to make a number of disclosures through their annual report, which includes a directors' report, corporate governance report, financial report and an auditor's report.

Additionally, under the previously mentioned legislation/prudential standards throughout this paper, it is mandatory for insurers to lodge a number of documents with APRA. As detailed in Part I, Question 1, the audit function is responsible for the production of an audit certificate as well as a report detailing the auditor's annual review, both of which are submitted to APRA. The production of risk management declarations, reinsurance management statements and actuarial reports are also examples of mandatory governance practices that are best achieved through disclosure.

Question 3: What is the interplay between market abuse regulations and other disclosure/transparency rules applicable to listed insurers and industry specific rules applicable only to insurance companies?

In Australia, market misconduct is governed by part 7.10 of the Corporations Act, which is administered by ASIC. Of particular relevance to insurers are:

- s1041A which prohibits market manipulation through a transaction(s) that may create or maintain artificial share prices;
- s1041B which prohibits tales trading or market rigging transactions;
- s1014C which prohibits engaging in fictitious or artificial transactions;
- s1014E which prohibits the making of false or misleading statements which may induced a person to apply for, dispose of or increase or reduce and interest in a financial product or financial market;
- s1014G which provides a person must not in the course of carrying on a financial services business engage in dishonest conduct; and
- s 1041H, which states that a person must not engage in misleading or deceptive conduct in relation to a financial product or service.

Insurers are also subject to a duty of utmost good faith contained in s 13 of the Insurance Contracts Act. This duty is an implied term in all insurance contracts, where insurers are expected to act with honesty and fairness.

The risk of misleading/deceptive conduct being attributed to an entity or its representatives must also be accounted for in accordance with prudential standard CPS 220. In addition to this, the transparency/disclosure obligations discussed earlier in this paper (i.e. fit and proper persons specified in CPS 520, codes of conduct provided by listed corporations under ASX governance principles, etc.) are designed to ensure that responsible persons and other employees behave ethically and do not engage in market misconduct. For general insurers, any breach or anticipated breach of the prudential standards must be reported to APRA under s 38AA of the Insurance Act. Similarly, life insurers are required to do the same under s 132A of the Life Insurance Act. Both sections specify that the failure to inform APRA of a breach/potential breach is an offence.

For corporations in Australia, whistleblowers are entitled to protection under s 1317AA of the Corporations Act when a report is made to ASIC on the presence of market misconduct within an organisation. Disclosures can also be made to APRA, who will keep the whistleblower's identity confidential. Whistleblower protections will soon be enhanced in Australia should the Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2017 (Cth) be passed, where a single regime will be introduced that covers the financial and corporate sectors and includes a broadened definition of what constitutes a whistleblower. Currently, a whistleblower will qualify for protection if:

- the discloser is:
  - an officer of a company; or
  - an employee of a company; or
  - a person who has a contract for the supply of services or goods to a company; or
  - an employee of a person who has a contract for the supply of services or goods to a company; and
- the disclosure is made to:
  - ASIC; or
  - the company's auditor or a member of an audit team conducting an audit of the company; or
  - a director, secretary or senior manager of the company; or
  - a person authorised by the company to receive disclosures of that kind; and
- the discloser informs the person to whom the disclosure is made of the discloser's name before making the disclosure; and
- the discloser has reasonable grounds to suspect that the information indicates that:
  - the company has, or may have, contravened a provision of the Corporations legislation; or
  - an officer or employee of the company has, or may have, contravened a provision of the Corporations legislation; and
- the discloser makes the disclosure in good faith.

VI. Outlook

In respect of the corporate governance of insurers, please describe your criticisms on the system in your jurisdiction, any recommendations for the future, and/or the main challenges which insurance undertakings encountered.

The main challenges for insurers in Australia arise from the wide range of legislation and regulatory standards that they are required to comply with. This creates sometimes overlapping regulation and/or inconsistency in requirements across regulatory regimes. In general terms the regulators ASIC and APRA work cohesively to aim to minimise dual regulation of insurers, and this is often recognised in ASIC standards and the Corporations Act requirements which specify carve outs applicable to APRA regulated entities.

Industry and regulatory tensions can sometimes arise where one industry participant is the subject of a regulatory review and agree to reach a settlement with a regulator rather than challenge its legal obligations to comply with regulatory requests. This can at times create pressure on other industry participants to do the same (especially if faced with regulatory pressure) when the outcome

sought goes beyond a level that is legally required. This is an issue that we have seen in recent ASIC action in relation to add on insurance products where commercial negotiations are reached that may be beyond those legally required.

This dual regulation system at times creates a tension between managing the risks of potential consumer detriment (for example through lower commissions, reduced premiums or ASIC seeking to ensure insurers aim for better claims outcomes which may increase an insurers loss ratios) against APRA prudential management of the insurer which may seek to see improved profitability and reduced loss ratios and general obligations to shareholders to seek profitable returns. Increasingly we are seeing a trend to balance the interests of consumers above those of shareholders or profitability and financial stability which may in future be a challenge for insurers to strike the right balance between these competing interests and obligations.